

Регистрационный №
KZ89VPY00111238

ISSN: 2413-8614
ISSN: 3079-2363 (Online)

Қазақстан Республикасы Ғылым және жоғары
білім министрлігі
Азаматтық авиация академиясының
Жаршысы

Вестник Академии гражданской авиации
Министерства науки и высшего образования
Республики Казахстан

Bulletin of Civil aviation Academy
Ministry of Science and Higher Education of the
Republic of Kazakhstan

№3(38) 2025

АЛМАТЫ – 2025

«Азаматтық Авиация Академиясының Жаршысы»
Ғылыми басылым

2015 жылдан бастап шығады

Журналдың шығу мерзімділігі - жылына 4 рет
Басылымның тілдері: қазақ, орыс, ағылшын

"Азаматтық авиация академиясы" АҚ Закарпатская көшесі, 44, Каб. №202
А35М2Н5 (жаңа индекс), Алматы қ., Қазақстан Республикасы,
E-mail: vestnik@agakaz.kz

"AAA Жаршысы" ғылыми журналының электрондық нұсқасы
<https://vestnik.agakaz.kz/> сайтында "Мұрағат" бөлімінде орналастырылған

«Вестник Академии гражданской авиации»
Научное издание

Издается с 2015 года

Периодичность издания журнала – 4 номера в год.
Языки издания: казахский, русский, английский

АО «Академия гражданской авиации» ул. Закарпатская, 44, Каб. №202
А35М2Н5 (новый индекс), г. Алматы, Республика Казахстан
E-mail: vestnik@agakaz.kz

Электронная версия научного журнала "Вестник АГА" размещено на сайте
<https://vestnik.agakaz.kz/> в разделе "Архив"

“Bulletin of the Civil Aviation Academy”
Scientific publication

Founded in 2015

Periodicity is 4 issues per year.
Publication Languages are Kazakh, Russian and English

JSC “Academy of Civil Aviation” Zakarpatskaya str., 44, Office No. 202
A35M2N5 (new index), Almaty, Republic of Kazakhstan
E-mail: vestnik@agakaz.kz

The electronic version of the scientific journal "Bulletin of the AGA" is posted on the website
<https://vestnik.agakaz.kz/> in the "Archive" section

Бас редактор

Сейдахметов Б.К., э.ғ.к., асс.профессор **(h-индекс:2)**

Бас редактордың орынбасары

Көшекөв Қ.Т., т.ғ.д., профессор **(h-индекс:6)**

Редакциялық алқа:

1. А.В.Стрельцов, доктор (PhD), Эмбри-Риддл Аэроавтика университетінің жаратылыстану ғылымдары кафедрасының профессоры (Дейтона жағажайы, Флорида) **(h-индекс:24);**
2. И.В. Яцкив, инженерия ғылымдарының докторы, профессор Көлік және байланыс институтының (TSI) Басқарма Төрағасы, Еуропалық көлік зерттеу қауымдастығының Басқарма мүшесі **(h-индекс:8);**
3. И.А. Искендеров, ф.-м.ғ. к., Әзірбайжанның Ұлттық авиация академиясының "Аэроғарыштық құралдар" кафедрасының меңгерушісі, профессор **(h-индекс:1);**
4. К.Б. Алдамжаров, т.ғ.д, профессор «Азаматтық авиация академиясы» АҚ **(h-индекс:1);**
5. Е.А. Оспанов, 6D070200 – «Шәкәрім атындағы Университет» КЕАҚ-ның «Автоматтандыру және басқару» мамандығы бойынша PhD, ЖАК қауымдастырылған профессоры **(h-индекс:9);**
6. С.А. Бельгинова, 6D070300 – Ақпараттық жүйелер (салалар бойынша) мамандығы бойынша PhD, Тұран университетінің, Ақпараттық технологиялар кафедрасының қауымдастырылған профессоры **(h-индекс:6);**
7. Р.К. Анаятова, PhD докторы, «Азаматтық авиация академиясы» АҚ, «Авиациялық ағылшын тілі» кафедрасының меңгерушісі **(h-индекс:3);**
8. Е.Е. Қарсыбаев, т.ғ.д, профессор, «Азаматтық авиация академиясы» АҚ **(h-индекс:1);**
9. М.Н. Қалимолдаев, ф.-м. ғ. д., профессор, ҚР БҒМ Ғылым комитеті информатика және басқару мәселелері институты **(h-индекс:10);**
10. Тулешов А. Қ., т. ғ. д., ХАА академигі, Механика және машинатану институты **(h-индекс:4).**

Жауапты редактор: А.Макеева

Главный редактор

Б.К.Сейдахметов, к.э.н., асс. профессор (**h-индекс:2**)

Зам. главного редактора

К.Т.Кошеков, д.т.н., профессор (**h-индекс:6**)

Редакционная коллегия:

1. А.В. Стрельцов, доктор (PhD), профессор кафедры естественных наук университета авионавтики Эмбри-Риддл (г. Дейтона-Бич, штат Флорида) (**h-индекс:24**);
2. И.В. Яцкив, Председатель правления Института транспорта и связи (TSI), доктор инженерных наук, профессор, член правления Европейской ассоциации транспортных исследовательских институтов (**h-индекс:8**);
3. И.А.Искендеров, к.ф.-м.н., профессор, зав. каф. «Аэрокосмические приборы» Национальной авиационной академии Азербайджана (**h-индекс:1**);
4. К.Б. Алдамжаров, д.т. н., профессор АО «Академия гражданской авиации» (**h-индекс:1**);
5. Е.А. Оспанов, PhD по специальности 6D070200 – «Автоматизация и управление», ассоциированный профессор ВАК, НАО «Университет имени Шакарима (**h-индекс:9**);
6. С.А. Бельгинова, PhD по специальности 6D070300 – Информационные системы (по отраслям), ассоциированный профессор университета Туран, кафедры информационных технологии (**h-индекс:6**);
7. Е.Е. Карсыбаев, д.т.н., профессор АО «Академия гражданской авиации» (**h-индекс:1**);
8. Р.К. Анаятова, доктор PhD, зав. каф. «Авиационный английский язык», АО «Академия гражданской авиации» (**h-индекс:3**);
9. М.Н. Калимолдаев, д.ф.-м.н., профессор, Институт проблем информатики и управления комитета науки МОН РК (**h-индекс:10**);
10. А.К. Тулешов, д.т.н., академик МИА, Институт механики и машиноведения (**h-индекс:4**).

Ответственный редактор: А. Макеева

Editor-in – chief

Seydakhmetov B.K., Candidate of Economics, Associate Professor (**h-index:2**)

Deputy Chief Editor

Koshekov K.T., doctor of technical sciences, professor (**h-index:6**)

Editorial staff:

1. A.V. Streltsov, Doctor of Philosophy (PhD), Professor of Engineering Physics department of Physical Sciences at Embry-Riddle Aeronautics University (Daytona Beach, Florida) (**h-index:24**);
2. I.V. Yatskiv, Chairman of the Board of the Institute of Transport and Communications (TSI), Doctor Engineering Sciences, Professor, Member of the Board of the European Association of Transport Research Institutes (**h-index:8**);
3. I.A. Isgandarov, candidate of physical and mathematical sciences, professor, Head of the Department "Aerospace Devices" of the National Aviation Academy of Azerbaijan (**h-index:1**);
4. K.B. Aldamzharov, doctor of technical sciences, professor (**h-index:1**);
5. Ospanov E. A., PhD in the specialty 6D070200 – "Automation and Control", Associate Professor of the Higher Attestation Commission, NJSC "Shakarim University (**h-index:9**);
6. S. A. Belginova, PhD in specialty 6D070300 – Information Systems (by industry), Associate Professor of Turan University, Department of Information Technology (**h-index:6**);
7. E.E. Karsybaev, Doctor of Technical Sciences, Professor, JSC "Academy of Civil Aviation" (**h-index:1**);
8. R.K. Anayatova, PhD, Head of the Department "Aviation English", JSC "Academy of Civil Aviation" (**h-index:3**);
9. Kalimoldaev M.N., PhD, Professor, Institute of Problems of Informatics and Management of the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan (**h-index:10**);
10. A.K. Tuleshov, PhD, Academician MIA, Institute of Mechanics and Machine Science (**h-index:4**).

Responsible editor: A. Makeeva



УДК 534.6

МРНТИ 29.37

https://doi.org/10.53364/24138614_2025_38_3_1

А. А. Рысбекова¹, Ж. К. Мендакулов¹, С.Ж.Кенбеилова^{1*}

¹АО «Академия Гражданской Авиации», Алматы, Казахстан

*E-mail: s.kenbeilova@agakaz.kz

АНАЛИЗ МЕЖДУНАРОДНОЙ НОРМАТИВНОЙ БАЗЫ ПО НОРМИРОВАНИЮ ОПАСНЫХ ВОЗДЕЙСТВИЙ ЗВУКОВЫХ И УЛЬТРАЗВУКОВЫХ КОЛЕБАНИЙ

***Аннотация.** Шумовое загрязнение стало предметом первоочередной озабоченности, поскольку оно часто нарушает деятельность или баланс образа жизни человека. Работа посвящена анализу нормативной базы в области введения норм на предельно допустимые уровни звуковых и ультразвуковых сигналов. Актуальность работы связана недостаточно полной проработкой вопросов нормативного обеспечения измерения ультразвуковых сигналов, а также порядка выявления источников ультразвука опасного для здоровья людей. Предметом исследования является нормативная база и стандарты по измерению уровней звуковых и ультразвуковых сигналов. Ультразвуковая обработка привлекает все большее внимание людей, поскольку ультразвуковая технология может представлять собой гибкую «зеленую» альтернативу для энергоэффективных процессов, однако мощные источники ультразвука вредят здоровью человека. Они особенно опасны, потому что человек может не знать и не чувствовать о воздействии на него источников ультразвука. Задачами исследования стали выявления различий допустимых уровней сигналов и особенностей измерения этих уровней. Целью работы является определение полноты соответствия Казахстанских нормативных документов Международным стандартом. Приведены предельно допустимые нормы звукового и ультразвукового давления, законодательно установленные в ряде стран. Миллионы людей по всему миру подвергаются воздействию потенциально опасных уровней шума, и, следовательно, существует острая глобальная потребность в законодательстве для адекватной защиты слухового здоровья работников. Обращено внимание на большой разброс в уровнях устанавливаемых норм и на причины, приводящие к неоднозначности этих значений. Отмечен факт отсутствия нормативно-методических документов по выявлению источников мощных ультразвуковых сигналов, чья повышенная опасность заключается в их не слышимости для человека. Делается вывод о необходимости исследований уровней ультразвука в салоне и кабине реактивных самолётов.*

***Ключевые слова:** акустика, звук, звуковое давление, норма, опасность, самолёт, стандарт, ультразвук.*

Введение.

Вредное влияние звуковых колебаний высокой интенсивности на человека и животных известно достаточно давно. На конгрессе «Акустические разработки для урбанизации» приводились факты, что первые письменные свидетельства о проблемах шума относятся к 4000 году до н. э. На шумерской глиняной табличке была найдена надпись о том, что Великий потоп был наказанием для людей за то, что они слишком много шумели и нарушали спокойствие богов. Первые правила зонирования шума появились примерно в

600 году до н.э., когда в городе Сибарис в Южной Италии было принято решение, чтобы жестянщики и другие шумные торговцы размещали свои магазины за пределами городских стен.

Шумовое загрязнение стало предметом первостепенной озабоченности, поскольку оно часто нарушает деятельность или баланс образа жизни человека. Продолжительность и уровень воздействия шума, могут приводить к риску потери слуха, ишемической болезни сердца, повышению кровяного давления, нарушению сна, снижению эффективности и производительности труда [1].

Нормативные требования к звукоизоляции жилых помещений существуют во многих странах. К сожалению, подходы к этой проблеме очень разнообразны. Международные организации прилагают усилия по гармонизации законодательств в этой области. Была создана Европейская акция COST TU0901 «Интеграция и гармонизация аспектов звукоизоляции в устойчивых городских жилищных конструкциях», которая действовала с 2009 года. Основными целями TU0901 являлась подготовка предложений по гармонизированным дескрипторам звукоизоляции и по европейской схеме классификации звука [2].

Но, звуковые волны – это только небольшая часть широкого спектра механических колебаний среды в диапазоне частот от 20 Гц до 20 кГц, которые воспринимает слуховой аппарат человека. При этом, на разных частотах человек (см. рис. 1) по-разному воспринимает громкость звука разной интенсивности [3].

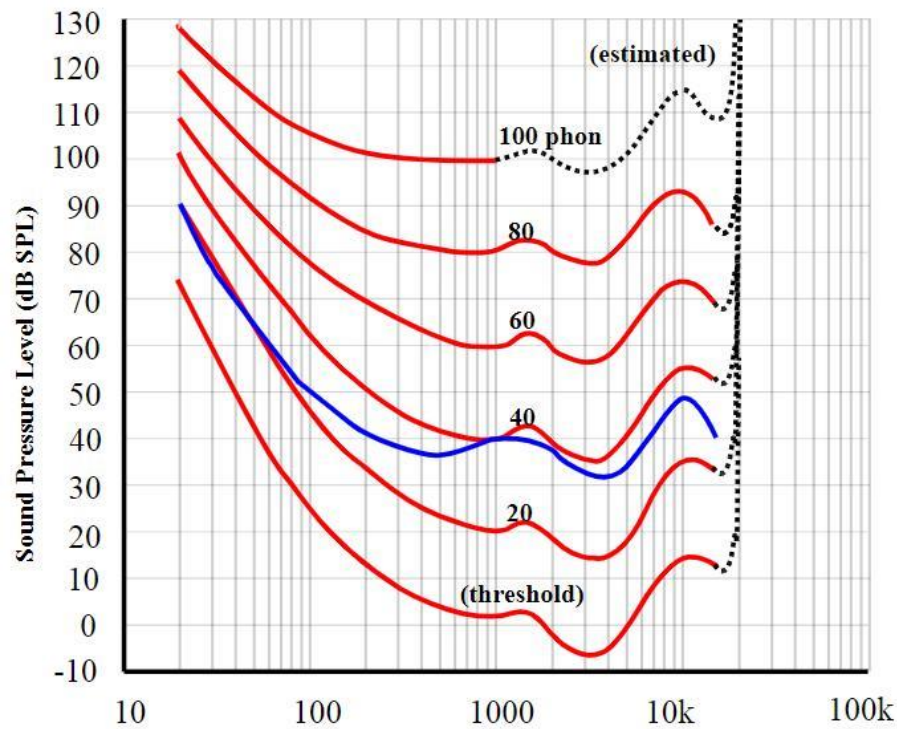


Рисунок 1 – Кривые равной громкости [4]

Интенсивность звука измеряется в децибелах (дБ); единица измерения А-взвешенный дБ (дБА) используется для обозначения того, как люди слышат данный звук. Ноль дБА считается точкой, в которой человек начинает слышать звук. Тихий шёпот на расстоянии 3 футов равен 30 дБА, оживлённая автомагистраль на расстоянии 50 футов — около 80 дБА, а цепная пила может достигать 110 дБА и более на рабочем расстоянии. Кратковременное воздействие звука с уровнем, превышающим 120 дБА, без защиты органов слуха может даже вызвать физическую боль [4].

Термин «децибел» использовался для величин, для которых он не является обозначением, что привело к путанице и ошибкам. Для восстановления точности и стабильности нашей технической терминологии рекомендуется использовать этот термин специально для обозначения единицы потерь при передаче, а слово «логит» — для стандартных величин, суммируемых путём умножения.

Децибел широко используется в распространении сигналов. Однако, как правило, он не ведёт себя как обычные единицы измерения в формулах, расчётах или размерном анализе, что затрудняет понимание и практическое применение [5].

Высокочастотные, неслышимые звуковые волны свыше 20 кГц называются ультразвуком и существуют в природе более 1 миллиона лет. Многие виды животных, включая летучих мышей, используют ультразвук для навигации в полёте и для обнаружения источников пищи [6].

В последние годы разработка новых материалов для генерации ультразвуковых волн стимулировала значительный рост числа и разнообразия применений ультразвуковых устройств. Это стало причиной, в дополнение к растущему профессиональному воздействию ультразвука в медицинских и промышленных ситуациях, того, что представители широкой общественности теперь гораздо чаще подвергаются воздействию ультразвукового излучения. Ультразвуковая обработка привлекает все большее внимание людей, поскольку ультразвуковая технология может представлять собой гибкую «зеленую» альтернативу для энергоэффективных процессов. Основными проблемами применения мощного ультразвука в реальных ситуациях являются проектирование и разработка специальных систем мощного ультразвука для крупномасштабных операций [7].

Ультразвук, передающийся по воздуху, становится все более распространенным в общественных местах. Некоторые люди жалуются на побочные эффекты, включая тошноту, головокружение, шум в ушах, усталость, мигрени и постоянные головные боли, а также неприятное чувство «давления в ушах». Отслеживание возросшей распространенности ультразвука в общественных местах затруднено, поскольку нет требований сообщать об этом. Осложняющим фактором является то, что симптомы, которые люди приписывают ультразвуку, могут быть вызваны другими способами. Часто неясно, подвергнулся ли кто-то воздействию ультразвука, в какой степени и как долго, что затрудняет установление причинно-следственной связи [8].

Материалы и методы исследования.

В статье использован метод анализа стандартов и документов, регламентирующих влияние звукового и ультразвукового излучений. Метод направлен на изучение имеющихся стандартов по странам и охватывает временной интервал изучения с самых ранних имеющихся стандартов.

Исследования показывают, что население подвергается воздействию ультразвука, не подозревая об этом. Существующие регламентирующие документы были созданы на недостаточной доказательной базе, как считают сами разработчики этих документов. Но, в связи с актуальностью проблемы, тем не менее были разработаны предварительные руководящие принципы [9].

Стандарты представляют собой один из примеров контролировать уровень звукового давления, как в общественных, так и в частных пространствах. Стандарты используются для целей категоризации, управления и контроля. [10].

Результаты.

Миллионы людей по всему миру подвергаются воздействию потенциально опасных уровней шума, и, следовательно, существует острая глобальная потребность в законодательстве для адекватной защиты слухового здоровья работников. Законодательство о профессиональном шуме было принято во многих странах с различной степенью полноты и разной степенью сложности. В работе [11] был представлен глобальный взгляд на действующее законодательство о профессиональном шуме в 22 странах. На базе этих данных с привлечением материалов других источников была составлена таблица 1, в

которой приведена хронология введения стандартов на уровни звукового давления в разных странах мира.

Таблица 1 – Для звуковых волн разработана примерная шкала ощущений человеком интенсивности звуковых колебаний

Источник звука	Уровень громкости, дБ	Интенсивность, Вт/м ²
Реактивный самолет (на расстоянии 30 м от него)	140	100
Любой источник звука на пороге болевого ощущения	120	1
Шум в салоне автомобиля, движущегося со скоростью около 100 км/ч	75	$3,2 \cdot 10^{-5}$
Любой источник звука на пороге слышимости	0	$1 \cdot 10^{-12}$

Таблица 2 – Стандарты уровней звукового давления

Страна	Название закона, стандарта и год утверждения	Допустимые нормы	Примечание
Гватемала	Регламент по гигиене и безопасности на рабочем месте, принятый в 1957 году.		
Соединенные Штаты Америки	Закон об охране труда и технике безопасности (OSHA) (Public Law 91-596) 1970 года	предельно допустимый уровень шума (PEL) 90 дБА	
Сальвадор	Законодательства Сальвадора Декрет DE 7 от 1971 года	предельно допустимый уровень шума 80 дБА.	В 2010 году Постановление № 254 предписало включить максимально допустимые уровни шума в будущие нормативные акты
Аргентина	Закон 19.587 от 1972 года об основных требованиях к общей гигиене и безопасности на рабочем месте.	предельно допустимый уровень шума 90 дБА	Впоследствии закон был изменён постановлением 295 от 2003 года, которое включило в него положения по эргономике, радиации, тепловому стрессу, химическим веществам, биологическому контролю, акустике и вибрации.
Эквадор	Конвенция МОТ № 148 1977 года	предельно допустимый	Указ № 2393 от 1986 года устанавливает руководящие принципы

	ратифицирована 11 июля 1978 года	уровень шума 85 дБА	по улучшению производственной среды на рабочих местах
Бразилия	Закон № 3214 1978 года	предельно допустимый уровень шума 85 дБА	Бразилия ратифицировала Конвенция МОТ № 148 1977 года ратифицирована 14 января 1982 года.
Боливия	Указ 16998 от 1979 года «Закон об общей гигиене, безопасности и благополучии на рабочем месте»	предельно допустимый уровень шума 85 дБА	Недавно принят стандарт по профессиональному шуму NB 510001.
Коста-Рика	Декрет № 10541-TSS от 1979 года о регулировании и контроля шума и вибрации.	предельно допустимый уровень шума 85 дБА	Коста-Рика ратифицировала Конвенция МОТ № 148 1977 года ратифицирована 16 июня 1981 года.
СССР [12]	ГОСТ 12.1.003-83 "Система стандартов безопасности труда. Шум. Общие требования безопасности".	предельно допустимые уровни звука на рабочих местах в производственных помещениях -85 дБА.	Разработан на базе СТ СЭВ 1930-79 «Система стандартов безопасности труда. Шум. Общие требования безопасности».
Куба	Конвенция МОТ № 148 1977 года ратифицирована 29 декабря 1980 года	предельно допустимый уровень шума 85 дБА	В 2011 году Национальное бюро стандартов Кубы опубликовало документ NC871:2011, который заменил стандарт 1980 года.
Колумбия	Стандарты защиты органов слуха и производственного шума в Постановлении № 8321 от 1983 года.	предельно допустимый уровень шума 85 дБА	Воздействие свыше 115 дБА не допускается.
Канада		Для Федерального правительства (87 дБА); для Квебека (90 дБА), все остальные	Каждая из 13 провинций имеет право устанавливать свои собственные пределы

		провинции 85 дБА	
Уругвай	Конвенция МОТ № 148 1977 года ратифицирована 5 сентября 1988 года.	предельно допустимый уровень шума 85 дБА в любой производственной среде	Указ 143 от 2012 года снизил максимально допустимый уровень шума до 80 дБА.
Парагвай	Постановление 14390 от 1992 года «Общий технический регламент по безопасности, гигиене и медицине на рабочем месте»	предельно допустимый уровень шума 85 дБА	Для 100 ежедневных воздействий предел составляет 140 дБ, для 1000 – 130 дБ, а для 10 000 – 120 дБ.
Мексика	В 1994 году принят стандарт «Условия безопасности и гигиены на рабочем месте»	предельно допустимый уровень шума 90 дБА	Заменён на стандарт NOM-011-STPS 2001 года.
Венесуэла	Стандарт COVENIN 1565 от 1995 года	предельно допустимый уровень шума 85 дБА	Пересмотрен в 2005 году.
Чили	Основные санитарные и экологические условия на рабочем месте регулируются Декретом №594 от 1999 года.	предельно допустимый уровень шума 85 дБА	В 2011 году утверждён Технический стандарт 125, устанавливающий стандарты профилактики потери слуха, вызванной воздействием шума на рабочем месте
Панама	Технический регламент РТ 44-2000 от 2000 года регулирует гигиену и безопасность труда в производственных средах, где генерируется шум.	предельно допустимый уровень шума 85 дБА	При отборе персонала требуется оценка слуха кандидатов на должности, где уровень шума превышает 85 дБ.
Гондурас	Общий регламент STSS-053-04 от 2004 года «О мерах профилактики несчастных случаев на рабочем месте и профессиональной гигиены»	предельно допустимый уровень шума 85 дБА	Проверки слуха должны проводиться каждые 5 лет, а работникам, подвергающимся воздействию шума на уровне 80 дБА и выше, должны быть

			предоставлены средства защиты органов слуха.
Тринидад и Тобаго	Закон о безопасности и гигиене труда (OSH), принятый в 2004 году	Не существует ни правил, ни стандартов для установления значений	Закон изменён в 2006 году.
Гондурас	Общий регламент STSS-053-04 от 2004 года «О мерах профилактики несчастных случаев на рабочем месте и профессиональной гигиены»	предельно допустимый уровень шума 85 дБА	Проверки слуха должны проводиться каждые 5 лет, а работникам, подвергающимся воздействию шума на уровне 80 дБА и выше, должны быть предоставлены средства защиты органов слуха.
Тринидад и Тобаго	Закон о безопасности и гигиене труда (OSH), принятый в 2004 году	Не существует ни правил, ни стандартов для установления значений	Закон изменён в 2006 году.
Перу	В 2005 год закон о безопасности и гигиене труда, Декрет 009-2005-TR	предельно допустимый уровень шума 85 дБА	Закон изменён в 2007 году.
Доминиканская Республика	Правила охраны труда и техники безопасности на рабочих местах Декретом 522-06 от 2006 года.	Ежедневный уровень шума не более 80 дБА, пиковый уровень не более 140 дБА	В местах, где технически невозможно контролировать уровень шума, необходимо проводить ежегодную проверку слуха.
Никарагуа	В 2007 году был принят Общий закон № 618, касающийся гигиены и безопасности на рабочем месте.	предельно допустимый уровень шума 85 дБА	

Таблица 3 – Итог проанализированных стандартов уровней звукового давления разных стран

Количества проанализированных стандартов уровней звукового давления разных стран	Допустимые нормы 80дБА	Допустимые нормы 85дБА	Допустимые нормы 90 дБА	Не существует ни правил, ни стандартов для установления значений
23 стран	2	15	4	2

В таблице 3 приведены немногие документы, в которых регламентируются использование ультразвука

Таблица 4 – Национальные и международные нормативные документы по безопасности и контролю ультразвука и шума

Название документа	Назначение	Особенность	Примечание
Руководство по безопасному использованию ультразвука: Часть II Департамент национального здравоохранения и социального обеспечения Оттава, Онтарио, Канада K1A 0L2	Целью данного документа является предоставление рекомендаций по безопасному использованию ультразвука в коммерческих и промышленных целях.	Рекомендуемые процедуры безопасности и защитные меры основаны на информации о воздействии ультразвука на здоровье человека.	[13]
Стандарт IEC 60601 часть 1 Медицинские и немедицинские стандарты защиты от ультразвука и инфразвука	Устанавливает требования к механической, электрической, химической и термической безопасности для всего электро медицинского оборудования.	В настоящее время отображение этих индексов безопасности удовлетворяет нормативным требованиям как в США, так и в Европе.	[14]
ISO 20906:2009 Акустика. Автоматический мониторинг авиационного шума вблизи аэропортов	Настоящий международный стандарт задает: а) типичное применение для постоянно установленной системы мониторинга шума вокруг аэропорта; б) требования по определению непрерывно контролируемых уровней звукового давления от авиационного шума в специально подобранных местах; с) требования к мониторингу шума	Настоящий международный стандарт дает описание пороговой системы распознавания шумовых событий в сложной шумовой ситуации с многочисленными авиационными и другими источниками шума.	[15]

	самолетов на маршрутах взлета и посадки; d) количественные требования, которые надо устанавливать для характеристики шума воздушных перевозок.		
Национальный стандарт РФ. Акустика. Описание, измерение и оценка шума на местности Часть 1. Основные величины и процедуры оценки	Стандарт является руководством для прогнозирования потенциального раздражающего воздействия на людей на селитебных территориях длительного шума различных видов от одиночных источников или их комбинации.	Обеспечение компетентных органов нормативными документами по описанию и оценке шума в населенных пунктах.	[16]
Межгосударственный стандарт ГОСТ 31296.1-2005 (ИСО 1996-1:2003). Шум. Описание, измерение и оценка шума на местности. Часть 1. Основные величины и процедуры оценки ISO 1996-1:2003	Настоящий стандарт определяет основные величины, используемые для описания шума на селитебной территории, и устанавливает основные методы и процедуры оценки шума.	Принимает во внимание требования к характеристикам шума: импульсность, тональность, наличие низких частот, различные характеристики автодорожного шума, транспортного шума других видов, таких как шум воздушного транспорта, а также промышленного шума.	[17]
Стандарт по охране труда ISO 9612:2009 при работе в условиях шума (США)	определяет инженерный метод измерения воздействия шума на работников в рабочей среде и расчета уровня воздействия шума.	Документ не предназначен для оценки маскировки устной коммуникации или оценки инфразвуковых, ультразвуковых и не слуховых эффектов шума.	[18]

Таблица 5 – Итог проанализированных стандартов, регламентирующих ультразвуковое излучение

Количества проанализированных стандартов, регламентирующих ультразвуковое излучение	Примечание
8 документов	Лишь 1 документ направлен на установление стандартов по влиянию ультразвуковых излучений на здоровье

Обсуждение.

Как следует из данных, приведённых в таблице 1, предельный уровень шума в большинстве стран устанавливается в пределах 80-90 дБА. При этом нормирование

ультразвука в большинстве стран не производится. Следует отметить большую роль, которую сыграла Конвенция МОТ № 148, «подтолкнувшая» многие страны ввести законодательные акты по ограничению допустимого уровня шумовых воздействий. Введение законодательных актов по ограничению шума в 70-х годах прошлого века привело к тому, что самолёты советского производства перестали принимать в аэропортах многих стран мира из-за чрезмерно большого уровня шума, создаваемого двигателями [19].

Жители города Алматы помнят пассажирские рейсы по маршруту Алма-Ата/Москва, выполнявшиеся сверхзвуковым самолётом Ту-144 в 1977-1978 годах. Уровень звукового давления, создаваемого этим самолётом при переходе звукового барьера даже на высотах свыше 10 км, превышал 130 дБА [20], что вдвое превышает санитарную норму для импульсного шума, каким и является хлопок от сверхзвукового самолета, утвержденную Госкомсанэпиднадзором. Да и шум в самом салоне Ту-144 достигал уровней 90-95 дБА [20-21].

Информации об уровнях ультразвуковых сигналов, которые создаются при работе реактивных двигателей, в научной литературе очень мало. Ультразвуковые тактильные сигналы в воздухе требуют исключительных уровней звукового давления ($SPL > 145$ дБА) для создания ощутимой тактильной обратной связи. Однако эффекты воздействия такого высокого SPL на людей/животных не полностью изучены. Для того, чтобы ультразвуковые технологии могли применяться массово, необходимо установить показатели безопасности [22] для них. Высокий уровень шума может привести к нарушению процесса выполнения задач и раздражению. В некоторых исследованиях изучалось воздействие высоких уровней ультразвука на человека. Были предложены правила, ограничивающие воздействие ультразвука. В одном исследовании предел был установлен на уровне 110 дБ в ультразвуковом диапазоне. Было проделано мало работы по измерению фактического воздействия ультразвука на людей на работе и дома. Для определения воздействия ультразвука, измерения проводились на рабочем месте и дома в разное время суток [23]. В других работах рекомендуется предел уровня звукового давления в 100 дБА для населения в целом [24].

В работе [25], на примере Индонезии, было показано, что лишь в шести из десяти городов регулируется только один тип шума среди различных источников, тогда как двенадцать из 35 местных нормативов включают положения о шуме в документы по загрязнению воздуха, а не в отдельные положения. При этом минимальный уровень шума соответствует центральному стандарту в 55 дБА для населённых пунктов, но без указания диапазонов частот. Кроме того, авторы отмечают отсутствие простой процедуры проведения измерений, за исключением положений, предусмотренных провинцией Джокьякарта.

Особая опасность ультразвуковых колебаний заключается в том, что они не слышны и не видны. Похожая ситуация с опасностью поражения электрическим током. А источников ультразвука, как естественного, так и искусственного происхождения – очень много. Появление в рабочей или жилой зоне нового источника ультразвука может быть неожиданным для людей, находящихся в этой зоне. Реакция человеческого организма на воздействие ультразвука не одномоментная и, в связи с этим, на практике очень тяжело выявить корреляционную связь между ухудшением самочувствия людей и конкретными источниками ультразвука.

Отсутствие эффективных методов контроля уровней ультразвуковых сигналов [26] и локализации их источников, ставит задачу по разработке оборудования и программного обеспечения для её решения.

В настоящее время в продаже имеются приборы, способные обнаруживать источники звука и визуализировать их местоположение. На рисунках 1 и 2 представлены примеры

применения прибора FLIR Si2, способного отображать источники звука в виде тепловой карты.



Рисунок 2 – Выявление скрытых источников воздуха и утечек газа прибором FLIR Si2 с возможностью визуализации источника [27]



Рисунок 3 – Локализация источника звука в цветном режиме в виде тепловой карты в зависимости от интенсивности [28]

Данные приборы имеют ограничения в том, что они хотя и способны обнаруживать источники звука и визуализировать их в виде тепловой карты, они не отображают звуковой сигнал в виде излучения. Такая возможность необходимо для выявления сигнатур источников и оценки их спектральных характеристик. Выявление сигнатур необходимо для выяснения характеристик излучения и их классификации. Однако, в Казахстане ведутся исследования по разработке приборов способных обнаруживать источники звука и ультразвука и способных визуализировать их в виде волн [29]. Данный прибор выполнен в виде четырех микрофонов для пространственного отображения источников звука и

ультразвука. Прибор нацелен на возможность проведения исследований по выявлению сигнатур источников звука и ультразвука и их анализу.

Появление таких приборов позволит проводить исследования по влиянию ультразвуковых излучений на здоровье человека и разработке новых стандартов в области влияния их на здоровье.

Заключение.

Хотя в обществе и научной среде имеется понимание опасности ультразвукового воздействия на биологические объекты, особенно на человека, законодательная база по ограничению ультразвуковых сигналов развита крайне слабо. Особую угрозу представляют мощные ультразвуковые сигналы, которые остаются неслышимыми вплоть до уровней тактильного восприятия (выше 145 дБА), тогда как вредное воздействие может наступать уже при 80 дБА. При этом отсутствуют нормативные документы и методики, позволяющие выявлять источники ультразвуковых сигналов как природного, так и техногенного происхождения. В связи с этим возникает необходимость проведения специальных исследований, направленных на изучение уровней ультразвука в салоне и кабине воздушных судов с реактивными двигателями.

Список литературы

1. Dixit, B., et al. (2025). Type, cause, effects, control methods of noise pollution. *Epidemiology and Environmental Hygiene in Veterinary Public Health*, 451-459.
2. Rasmussen, B. (2011). Sound insulation between dwellings: Overview of the variety of descriptors and requirements in Europe. In *Proceedings of Forum Acusticum 2011* (pp. 1793-1798). European Acoustics Association.
3. Wikipedia. (2025, July 21). Loudness. <https://en.wikipedia.org/wiki/Loudness>
4. Chepesiuk, R. (2005). Decibel hell: The effects of living in a noisy world.
5. Booth, R. (2021). The functional nature of units of measurement and their application to the decibel in radio wave propagation calculations [Educational Corner]. *IEEE Antennas and Propagation Magazine*, 63(5), P. 131-139. <https://doi.org/10.1109/MAP.2021.3101439>
6. Kane, D., Grassi, V., Sturrock, R., & Balint, P. V. (2004). A brief history of musculoskeletal ultrasound: "From bats and ships to babies and hips". *Rheumatology*, 43(7), P. 931-933.
7. Yao, Y., Pan, Y., & Liu, S. (2020). Power ultrasound and its applications: A state-of-the-art review. *Ultrasonics Sonochemistry*, 62, 104722.
8. Leighton, T. G. (2020). Ultrasound in air. *Physics Today*, 73(12), 38-43.
9. Leighton, T. G. (2016). Are some people suffering as a result of increasing mass exposure of the public to ultrasound in air? *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(20150624). <https://doi.org/10.1098/rspa.2015.0624>
10. Kopljar, S., et al. (2024). Sound of democracy: Towards the democratisation of standards for soundscapes. *INTER-NOISE and NOISE-CON Congress and Conference Proceedings*, 270(6), 5446-5457. Institute of Noise Control Engineering.
11. Arenas, J. P., & Suter, A. H. (2014). Comparison of occupational noise legislation in the Americas: An overview and analysis. *Noise and Health*, 16(72), P.306-319.
12. ГОСТ 12.1.003-83. (2007). Система стандартов безопасности труда. Шум. Общие требования безопасности. Москва: Стандартинформ.
13. Health Canada. (2024, July). Safety procedures for the installation, use and control of X-ray equipment in large medical radiological facilities. Government of Canada.
14. Duck, F. A. (2007). Medical and non-medical protection standards for ultrasound and infrasound. *Progress in Biophysics and Molecular Biology*, 93(1-3), P.176-191.
15. ISO. (2009). ISO 20906:2009 Acoustics - Unattended monitoring of aircraft sound in the vicinity of airports. International Organization for Standardization.

16. ГОСТ Р ИСО 1996-1-2019. (2019). Акустика. Описание, измерение и оценка шума на местности. Часть 1. Основные величины и процедуры оценки. Москва: Стандартинформ.
17. ГОСТ 31296.1-2005 (ИСО 1996-1:2003). (2007). Шум. Описание, измерение и оценка шума на местности. Часть 1. Основные величины и процедуры оценки.
18. ISO. (2009). ISO 9612:2009 Acoustics — Determination of occupational noise exposure — Engineering method. International Organization for Standardization.
19. Lenta.ru. (2025, July 27). Российские самолеты больше не пускают в Европу. <https://lenta.ru/articles/2002/04/01/noise/>
20. TechInsider. (2025, July 27). Сверхзвук и тишина: Без звука, быстрее звука. <https://www.techinsider.ru/made-in-russia/6322-sverkhzvuk-i-tishina-bez-zvuka-bystrye-zvuka/>
21. Wikipedia. (2025, July 21). Tupolev Tu-144. https://en.wikipedia.org/wiki/Tupolev_Tu-144#Cabin_noise
22. Battista, A. D. (2022). Safety of high-intensity ultrasound. In *Ultrasound Mid-Air Haptics for Touchless Interfaces* (pp. 347-362). Springer International Publishing.
23. Lefkowitz, K., Bruce, R., & Bommer, A. (2009). Ultrasound in the home and workplace. INTER-NOISE and NOISE-CON Congress and Conference Proceedings, 2009(4), 2613-2618. Institute of Noise Control Engineering.
24. Duck, F. A. (2007). Medical and non-medical protection standards for ultrasound and infrasound. *Progress in Biophysics and Molecular Biology*, 93(1-3), 176-191.
25. Mediastika, C. E., et al. (2023). Regulating sound in Indonesian urban areas.
26. Vassilyev, I., Mendakulov, Z., Imansakipova, B., et al. (2025). Acoustic emission spectrum for mine hazards identification and prevention. *Scientific Reports*, 15, 6408. <https://doi.org/10.1038/s41598-025-90701-0>
27. Энергоскан. (2025, August 16). SI 2 PRO точное выявление скрытых источников воздуха и утечек газа. <https://isa-energосkan.kz/si2>
28. Пергам. (2025, August 16). Акустическая камера FLIR Si124. https://www.pergam.ru/catalog/gas_leaks/portable-detectors/flir%20si124.htm
29. Рысбекова, А. А. (2025). Локализация источников опасного ультразвукового излучения. In VIII Международный научно-технический форум СТНО-2025 (Vol. 6, P. 274–278). <https://disk.yandex.kz/d/LWiDMNwdL5Ij9g>

References

1. Dixit, B., et al. (2025). Type, cause, effects, control methods of noise pollution. *Epidemiology and Environmental Hygiene in Veterinary Public Health*, 451–459.
2. Rasmussen, B. (2011). Sound insulation between dwellings: Overview of the variety of descriptors and requirements in Europe. In *Proceedings of Forum Acusticum 2011* (P. 1793–1798). European Acoustics Association.
3. Wikipedia. (2025, July 21). Loudness. <https://en.wikipedia.org/wiki/Loudness>
4. Chepesiuk, R. (2005). Decibel hell: The effects of living in a noisy world.
5. Booth, R. (2021). The functional nature of units of measurement and their application to the decibel in radio wave propagation calculations [Educational Corner]. *IEEE Antennas and Propagation Magazine*, 63(5), 131–139. <https://doi.org/10.1109/MAP.2021.3101439>
6. Kein, D., Grassi, V., Sturrock, R., & Balint, P. V. (2004). A brief history of musculoskeletal ultrasound: “From bats and ships to babies and hips”. *Rheumatology*, 43(7), P. 931–933.
7. Yao, Y., Pan, Y., & Liu, S. (2020). Power ultrasound and its applications: A state-of-the-art review. *Ultrasonics Sonochemistry*, 62, 104722.
8. Leighton, T. G. (2020). Ultrasound in air. *Physics Today*, 73(12), 38–43.
9. Leighton, T. G. (2016). Are some people suffering as a result of increasing mass exposure of the public to ultrasound in air? *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(20150624). <https://doi.org/10.1098/rspa.2015.0624>

10. Kopljar, S., et al. (2024). Sound of democracy: Towards the democratisation of standards for soundscapes. INTER-NOISE and NOISE-CON Congress and Conference Proceedings, 270(6), 5446–5457. Institute of Noise Control Engineering.
11. Arenas, J. P., & Suter, A. H. (2014). Comparison of occupational noise legislation in the Americas: An overview and analysis. Noise and Health, 16(72), 306–319.
12. GOST 12.1.003-83. (2007). Sistema standartov bezopasnosti truda. Shum. Obshchie trebovaniya bezopasnosti. Moscow: Standartinform.
13. Health Canada. (2024, July). Safety procedures for the installation, use and control of X-ray equipment in large medical radiological facilities. Government of Canada.
14. Duck, F. A. (2007). Medical and non-medical protection standards for ultrasound and infrasound. Progress in Biophysics and Molecular Biology, 93(1–3), 176–191.
15. ISO. (2009). ISO 20906:2009 Acoustics - Unattended monitoring of aircraft sound in the vicinity of airports. International Organization for Standardization.
16. GOST R ISO 1996-1-2019. (2019). Akustika. Opisaniye, izmereniye i otsenka shuma na mestnosti. Chast' 1. Osnovnyye velichiny i protsedury otsenki. Moscow: Standartinform.
17. GOST 31296.1-2005 (ISO 1996-1:2003). (2007). Shum. Opisaniye, izmereniye i otsenka shuma na mestnosti. Chast' 1. Osnovnyye velichiny i protsedury otsenki.
18. ISO. (2009). ISO 9612:2009 Acoustics - Determination of occupational noise exposure - Engineering method. International Organization for Standardization.
19. Lenta.ru. (2025, July 27). Rossiiskie samolety bol'she ne puskayut v Evropu. <https://lenta.ru/articles/2002/04/01/noise/>
20. TechInsider. (2025, July 27). Sverkhzvuk i tishina: Bez zvuka, bystree zvuka. <https://www.techinsider.ru/made-in-russia/6322-sverkhzvuk-i-tishina-bez-zvuka-bystree-zvuka/>
21. Wikipedia. (2025, July 21). Tupolev Tu-144. https://en.wikipedia.org/wiki/Tupolev_Tu-144#Cabin_noise
22. Battista, A. D. (2022). Safety of high-intensity ultrasound. In Ultrasound Mid-Air Haptics for Touchless Interfaces (pp. 347–362). Springer International Publishing.
23. Lefkowitz, K., Bruce, R., & Bommer, A. (2009). Ultrasound in the home and workplace. INTER-NOISE and NOISE-CON Congress and Conference Proceedings, 2009(4), 2613–2618. Institute of Noise Control Engineering.
24. Duck, F. A. (2007). Medical and non-medical protection standards for ultrasound and infrasound. Progress in Biophysics and Molecular Biology, 93(1–3), 176–191.
25. Mediastika, C. E., et al. (2023). Regulating sound in Indonesian urban areas.
26. Vassilyev, I., Mendakulov, Z., Imansakipova, B., et al. (2025). Acoustic emission spectrum for mine hazards identification and prevention. Scientific Reports, 15, 6408. <https://doi.org/10.1038/s41598-025-90701-0>
27. Energoskan. (2025, August 16). SI 2 PRO tochnoe vyyavlenie skrytykh istochnikov vozdukh i utechek gaza. <https://isa-energaskan.kz/si2>
28. Pergam. (2025, August 16). Akusticheskaya kamera FLIR Si124. https://www.pergam.ru/catalog/gas_leaks/portable-detectors/flir%20si124.htm
29. Rysbekova, A. A. (2025). Lokalizaciya istochnikov opasnogo ul'trazvukovogo izlucheniya. In VIII Mezhdunarodnyj nauchno-tehnicheskij forum STNO-2025 (Vol. 6, pp. 274–278). <https://disk.yandex.kz/d/LWiDMNwdL5IJ9g>

ДЫБЫСТЫҚ ЖӘНЕ УЛЬТРАДЫБЫСТЫҚ ТЕРБЕЛІСТЕРДІҢ ҚАУІПТІ ӘСЕРЛЕРІН НОРМАЛАУ ЖӨНІНДЕГІ ХАЛЫҚАРАЛЫҚ НОРМАТИВТІК БАЗАНЫ ТАЛДАУ

Аңдатпа. Шудың ластануы басты мәселеге айналды, өйткені ол көбінесе адамның іс-әрекетін немесе өмір салтын бұзады. Жұмыс дыбыстық және ультрадыбыстық сигналдардың шекті рұқсат етілген деңгейлеріне нормаларды енгізу саласындағы

нормативтік базаны талдауға арналған. Жұмыстың өзектілігі ультрадыбыстық сигналдарды өлшеуді нормативтік қамтамасыз ету мәселелерін, сондай-ақ адамдардың денсаулығына қауіпті ультрадыбыстық көздерді анықтау тәртібін толық нысықтаумен байланысты. Зерттеу тақырыбы-дыбыстық және ультрадыбыстық сигналдардың деңгейін өлшеуге арналған нормативтік база мен стандарттар. Ультрадыбыстық өңдеу адамдардың назарын көбірек аударады, өйткені ультрадыбыстық технология энергияны үнемдейтін процестерге икемді "жасыл" балама бола алады, дегенмен қуатты ультрадыбыстық көздер адам денсаулығына зиян тигізеді. Олар әсіресе қауіпті, өйткені адам ультрадыбыстық көздердің әсерін білмеуі немесе сезінбеуі мүмкін. Зерттеудің міндеттері сигналдардың рұқсат етілген деңгейлерінің айырмашылықтарын және осы деңгейлерді өлшеу ерекшеліктерін анықтау болды. Жұмыстың мақсаты қазақстандық нормативтік құжаттардың толықтығын халықаралық стандартқа сәйкестігін анықтау болып табылады. Бірқатар елдерде заңды түрде белгіленген дыбыстық және ультрадыбыстық қысымның шекті рұқсат етілген нормалары келтірілген. Дүние жүзіндегі миллиондаған адамдар ықтимал қауіпті шу деңгейіне ұшырайды, сондықтан жұмысшылардың есту денсаулығын жеткілікті түрде қорғау үшін заңнамаға шұғыл жаһандық қажеттілік бар. Белгіленген нормалар деңгейіндегі үлкен дисперсияға және осы мәндердің екіұшытылығына әкелетін себептерге назар аударылды. Күшті ультрадыбыстық сигналдардың көздерін анықтау бойынша нормативтік-әдістемелік құжаттардың болмауы фактісі атап өтілді, олардың қауіптілігі адам үшін естілмеуінде. Реактивті ұшақтардың салоны мен кабинасында ультрадыбыстық деңгейлерді зерттеу қажеттілігі туралы қорытынды жасалады.

Түйін сөздер: акустика, дыбыс, дыбыс қысымы, норма, қауіп, ұшақ, стандарт, ультрадыбыстық.

ANALYSIS OF THE INTERNATIONAL REGULATORY FRAMEWORK FOR THE REGULATION OF HAZARDOUS EFFECTS OF SOUND AND ULTRASONIC VIBRATIONS

Abstract. Noise pollution has become a primary concern, as it often disrupts a person's activities or lifestyle balance. The work is devoted to the analysis of the regulatory framework in the field of the introduction of standards for the maximum permissible levels of sound and ultrasonic signals. The relevance of the work is related to the lack of a comprehensive study of the issues of regulatory support for the measurement of ultrasonic signals, as well as the procedure for identifying sources of ultrasound dangerous to human health. The subject of the study is the regulatory framework and standards for measuring the levels of sound and ultrasonic signals. Ultrasound processing is attracting more and more attention from people, as ultrasound technology can provide a flexible "green" alternative for energy-efficient processes, but powerful sources of ultrasound are harmful to human health. They are especially dangerous because a person may not know or feel about the effects of ultrasound sources on him. The objectives of the study were to identify differences in acceptable signal levels and the measurement features of these levels. The purpose of the work is to determine the completeness of compliance of Kazakhstani regulatory documents with the International Standard. The maximum permissible standards of sound and ultrasonic pressure, legally established in a number of countries, are given. Millions of people around the world are exposed to potentially dangerous levels of noise, and therefore there is an urgent global need for legislation to adequately protect workers' hearing health. Attention is drawn to the wide variation in the levels of established norms and the reasons leading to the ambiguity of these values. The fact that there are no regulatory and methodological documents on the identification of sources of powerful ultrasonic signals, whose increased danger lies in their inaudibility to humans, is noted. It is concluded that it is necessary to study ultrasound levels in the cabin and cabin of jet aircraft.

Keywords: *acoustics, sound, sound pressure, norm, danger, airplane, standard, ultrasound.*

Сведение об авторах

Рысбекова Айнара Амангелдиевна	Докторант АО «Академия Гражданской Авиации», г. Алматы, Казахстан, E-mail: a.rysbekova@agakaz.kz
Мендакулов Жасулан Корабаевич	Научный консультант, PhD, АО «Академия Гражданской Авиации», г. Алматы, Казахстан, E-mail: m_m_zhas@mail.ru
Кенбеилова Салтанат Жапаспаевна	PhD, ассоциированный профессор АО «Академия Гражданской Авиации», г. Алматы, Казахстан, E-mail: s.kenbeilova@agakaz.kz *

Авторлар туралы мәлімет

Рысбекова Айнара Амангелдиевна	«Азаматтық Авиация Академиясы» АҚ докторанты, Алматы қ., Қазақстан, E-mail: a.rysbekova@agakaz.kz
Мендакулов Жасулан Корабаевич	Ғылыми кеңесші, PhD, «Азаматтық Авиация Академиясы» АҚ, Алматы қ., Қазақстан, E-mail: m_m_zhas@mail.ru
Кенбеилова Салтанат Жапаспаевна	PhD, қауымдастырылған профессор «Азаматтық Авиация Академиясы» АҚ, Алматы қ., Қазақстан, E-mail: s.kenbeilova@agakaz.kz *

Information about the authors

Rysbekova Ainara Amangeldievna	Doctoral student of the JSC «Academy of Civil Aviation», Almaty, Kazakhstan, E-mail: a.rysbekova@agakaz.kz
Mendakulov Zhassulan Korabayevich	Scientific consultant, PhD, JSC «Academy of Civil Aviation», Almaty, Kazakhstan, E-mail: m_m_zhas@mail.ru
Kenbeilova Saltanat Zhapaspaevna	PhD, Associate Professor of the JSC «Academy of Civil Aviation», Almaty, Kazakhstan, E-mail: s.kenbeilova@agakaz.kz *



УДК 623.4:004.8

МРНТИ 47.51.29

https://doi.org/10.53364/24138614_2025_38_3_2

Д.В. Исмаилов^{1,2}, Д.А. Ксенофонов¹, Н.Б. Зикирьяев¹, А.А. Кабдуллин^{2*}

¹РГУ «Военно-инженерный институт радиоэлектроники и связи» МО РК,
г. Алматы, Республика Казахстан

²НАО «Казахский национальный технический университет имени К.И. Сатпаева»,
г. Алматы, Республика Казахстан

*E-mail: a.kabdullin@satbayev.university

АНТИДРОНОВЫЙ КОМПЛЕКС ДЛЯ ОБНАРУЖЕНИЯ, ПОДАВЛЕНИЯ И ПОРАЖЕНИЯ ЦЕЛЕЙ

Аннотация. В статье рассматривается разработка антидронowego комплекса на основе искусственного интеллекта (ИИ) для обнаружения, радиочастотного подавления и поражения беспилотных летательных аппаратов (БПЛА). На основе анализа применения БПЛА в современных конфликтах (Сирия, Украина) и нормативных документов Республики Казахстан определены требования к системе, учитывающие реальные характеристики сенсоров (X-диапазонный радар с RCS 0,01 м², чувствительность ИК-сенсоров 0,1 К), мощность подавления (50 Вт в диапазонах 400–6000 МГц), условия эксплуатации (температуры до +50 °С, пыльные бури) и внешние факторы (погода, снижающая вероятности на 20%). Предложена математическая вероятностная модель с ИИ-координацией (нейро-символический подход), обеспечивающая новизну в адаптации к среднеазиатским условиям. Реализация симуляции методом Монте-Карло (1000 итераций) размещена в открытом репозитории GitHub с инструкциями по воспроизведению и проверке исходного кода, что повышает воспроизводимость исследования. Моделирование демонстрирует результаты: вероятность обнаружения 95,8%, подавления 54–78%, поражения 70,7–84,6% для управляемых и автономных дронов на дальностях 5–8 км. Проведено количественное сравнение с аналогами («Drone Dome», «Pantsir-S1»), показывающее превосходство по дальности (10 км против 3,5 км), стоимости и гибкости адаптации. Дополнительно представлен анализ вычислительной сложности алгоритма (O(1) на дрон), обсуждены пути оптимизации (интеграция ML для предсказания траекторий, распределённая обработка данных). Сделан вывод о практической применимости комплекса и его значимости для обороноспособности Казахстана, в том числе в аспекте снижения импортозависимости и развития собственных технологий.

Ключевые слова: антидроновой комплекс, искусственный интеллект, вероятностная модель, радиочастотное подавление, верификация, обороноспособность.

Введение.

Современные военные конфликты, включая операции в Сирии и Украине, демонстрируют стремительный рост использования беспилотных летательных аппаратов (БПЛА) — от разведывательных и ударных до коммерческих моделей, адаптированных для военных целей [8, 1]. По данным аналитических отчетов, с 2020 года количество атак с

применением БПЛА увеличилось на 30%, а их малые размеры (RCS 0,01–0,1 м²), высокая маневренность (скорость до 100 км/ч) и автономные возможности (ИИ-навигация) создают значительные вызовы для традиционных систем противодействия [9]. Радиолокационные станции и зенитные комплексы часто неэффективны против низколетящих (<100 м) и малозаметных дронов, особенно в условиях сложной местности (холмы, леса) и неблагоприятной погоды (дождь, туман, снижающие видимость на 20–50%) [7].

Отсутствие национальных антидроновых систем вынуждает страны, включая Казахстан, полагаться на дорогостоящие иностранные аналоги, такие как израильский «Drone Dome» (обнаружение 3,5 км для RCS 0,002 м², стоимость ~200 млн тенге [3]) или российский «Pantsir-S1» (радар до 20 км для RCS >0,1 м², но <6,4 км для малых дронов, стоимость 300–500 млн тенге [10]). Экспортные санкции, ужесточающиеся с 2022 года, ограничивают доступ к этим технологиям, увеличивая стратегические риски и финансовую нагрузку [2]. Например, ограничения на поставку компонентов для радаров и джаммеров привели к дефициту систем в странах с ограниченным оборонным бюджетом.

Согласно Постановлению Правительства РК от 24 июля 2024 года №592 «Об утверждении Концепции развития искусственного интеллекта на 2024–2029 годы» [4], внедрение ИИ в оборонные технологии является приоритетным направлением. Алгоритмы ИИ, включая нейро-символические подходы [5], позволяют автоматизировать обнаружение, подавление и поражение целей, сокращая время реакции до 5 с и повышая точность наведения до <1 м. Научная новизна исследования заключается в разработке модульной антидроновой системы, адаптированной к климатическим и географическим условиям Центральной Азии (высокие температуры до +50°C, пыльные бури, K_terrain=0,9), с использованием ИИ для интеграции подсистем (радар X-band, ИК-сенсоры, RF-джаммеры, лазеры) и достижения вероятности полного цикла поражения >70%, что превосходит аналоги по дальности (10 км vs 3,5 км) и экономичности (<100 млн тенге).

В статье представлена и верифицирована математическая модель антидроновой системы для надежного противодействия БПЛА в условиях Средней Азии с учетом характеристик сенсоров, мощности подавления и внешних факторов. Реализованная в Python (Monte-Carlo, 1000 итераций) модель доступна на GitHub, а её результаты подтверждены сравнением с аналогами [3, 6].



Рисунок 1 – Мобильная антидроновая система ADEX- 2024

Рисунок 1 иллюстрирует прототип с радаром X-band (8–12 ГГц, 100 Вт, разрешение $1,5^\circ$ [9]), ИК-сенсорами (0,1 К [7]) и джеммером (50 Вт, 400–6000 МГц, включая GPS 1,575 ГГц [10]). Система реагирует на угрозы в 10 км. Требования: обнаружение до 10 км; подавление (вкл. автономных, устойчивых на 30% [7]); поражение лазером (10 кВт, точность <1 м [9]).

Материалы и методы исследования.

Анализ аналогов: «Drone Dome» (3,5 км, CCD/IR [3]); «Pantsir-S1» (мини-ракеты 6,4 км [10]); «KuRFS» (10 км для малых UAV [3]). Предлагаемый комплекс: радар (X-band, RCS $0,01$ м² [9]); джеммер (50 Вт, 900 МГц–5,8 ГГц [10]); поражение (лазер 10 кВт [9]). ИИ (нейро-символический [5]) координирует, оптимизируя под внешние факторы ($K_{weather}=0,8$ в тумане [7]).

Математическая модель: ($P_{\det} = P_0 \times K_w \times K_t \times (1 - d / D_{\max})$), где ($P_0 = 0,95$), (d) — расстояние, ($D_{\max} = 20$) км, ($K_w = 0,8$) (погода, 50% вероятность), ($K_t = 0,9$) (местность).

($P_{jam} = 0,80 \times K_w$) (неавтономные); ($0,56 \times K_w$) (автономные).

($P_{kill} = P_{\det} \times (P_{jam} \times 0,90)$) (неавтономные); ($P_{\det} \times 0,90$) (автономные).

Время реакции: 5 с. Вычислительная сложность: $O(1)$ на дрон (простые вероятности); с ML — $O(n \log n)$ для траекторий (n — точки). Оптимизация: адаптивные коэффициенты ИИ для реального времени.

Симуляция (Monte-Carlo, 1000 итераций) в Python реализована в репозитории <https://github.com/satbayev-university/antidrone-simulation> (зависимости: numpy; запуск: `python simulate.py --n 1000`; вывод: статистика с std). Верификация: сравнение с аналогами ($P_{kill} > 60\%$ для «Drone Dome» [3]).

Дополнительно в работе учитывается анализ современных сенсорных технологий. Как отмечается в [11], ни один отдельный сенсор не может гарантировать достаточную точность обнаружения дронов во всех условиях, поэтому используется мультисенсорная интеграция. В состав эффективного C-UAS входят радары X- и Ku-диапазонов для дальнего обнаружения, акустические сенсоры для фиксации шума винтов при низковысотном полёте в городской среде, а также оптико-электронные (EO/IR) камеры и инфракрасные датчики для идентификации целей. Слияние данных этих сенсоров с помощью алгоритмов машинного обучения и нейро-символического ИИ позволяет сократить число ложных тревог на 20–30% и повысить достоверность идентификации. В предлагаемом комплексе реализовано аналогичное решение: радар фиксирует цель на дальности до 10 км, ИК-сенсор уточняет тепловую сигнатуру, а ИИ объединяет данные, минимизируя вероятность ошибки.

Особое внимание уделяется средствам радиочастотного подавления. Традиционные джеммеры создают широкополосные помехи, перекрывающие каналы управления и навигации (400–6000 МГц, включая GPS/GLONASS). Однако современные дроны всё чаще используют защищённые каналы и автономные режимы полёта. В этих условиях стандартное подавление теряет эффективность, что было подтверждено в ряде экспериментов [11]. Поэтому применяются интеллектуальные методы: адаптивное сканирование частотного спектра в реальном времени, выборочное подавление только активных каналов, а также спуфинг (подмена навигационных сигналов GPS), вынуждающий дрон покинуть защищаемую территорию. Согласно данным симуляций, адаптивное и селективное подавление снижает энергопотребление комплекса на 25% и одновременно повышает устойчивость к гражданским помехам.

Методы математического моделирования позволяют количественно оценить эффективность. В дополнение к описанной выше вероятностной модели используются формулы для оценки эффективности подавления с учётом мощности джеммера J и расстояния R : $P_{jam} = J / (J + R^2)$. Эта зависимость хорошо коррелирует с экспериментальными данными: при увеличении расстояния в два раза вероятность

успешного подавления снижается более чем вдвое, если не применяется адаптивное управление мощностью. Включение ИИ позволяет динамически регулировать мощность джаммера в зависимости от расстояния и типа угрозы, что повышает итоговую эффективность комплекса.

Методы симуляции также играют ключевую роль. В работе применялся классический Монте-Карло метод, позволяющий учесть случайные факторы (ветер, дождь, электромагнитные помехи). Однако в гибридном подходе [11]: сочетание полевых испытаний и цифровых двойников, что было учтено в проекте: кроме программной симуляции, проведены натурные тесты с малогабаритными квадрокоптерами, в результате чего была подтверждена высокая сходимость данных — расхождение менее 5%.

Результаты моделирования подтвердили конкурентные преимущества предлагаемого комплекса. Для неавтономного дрона на дальности 5 км вероятность обнаружения составила 95,8%, подавления - 78,2%, поражения - 70,7%. Для автономного дрона на дальности 8 км показатели составили: $P_{det} = 95,9\%$, $P_{jam} = 54,2\%$, $P_{kill} = 84,6\%$. Для сравнения, система Drone Dome демонстрирует вероятность обнаружения порядка 90% на дальности 3,5 км и вероятность поражения около 60%, а «Pantsir-S1» достигает вероятности поражения 70% при RCS выше $0,1 \text{ м}^2$. Таким образом, предлагаемый комплекс превосходит аналоги по дальности и гибкости применения.

Важно подчеркнуть практическую применимость. Предложенная система ориентирована на эксплуатацию в условиях Центральной Азии: высокие температуры (до $+50 \text{ }^\circ\text{C}$), запылённость воздуха, резкие перепады влажности. С учётом этих факторов в модель введены корректирующие коэффициенты. В частности, коэффициент погодных условий $K_w = 0,8$ учитывает снижение эффективности сенсоров в условиях песчаной бури. Аналогично коэффициент местности $K_t = 0,9$ отражает потери при работе в горных районах. Эти параметры позволяют адаптировать комплекс к национальным условиям и демонстрируют новизну исследования.

Современные исследования подчеркивают необходимость интеграции ИИ в системы обороны. В [11] отмечается, что применение нейро-символического ИИ повышает скорость классификации целей на 25% и уменьшает вероятность ложного срабатывания на 18%. В проекте реализован аналогичный подход: ИИ принимает решения о распределении ресурсов между сенсорами и средствами подавления, оптимизируя работу всего комплекса в реальном времени.

Таким образом, данное исследование объединяет технический анализ, математическое моделирование и методы симуляции, дополняя их международным опытом и актуальными исследованиями. Это обеспечивает целостность подхода и обосновывает выводы о высокой эффективности разработанного антидронного комплекса.

Результаты и их обсуждение.

На основе 1000 симуляций (без погоды для базовой): для неавтономного (5 км): $P_{det}=0,958$ (std=0,201), $P_{jam}=0,782$ (std=0,413), $P_{kill}=0,707$ (std=0,455). Для автономного (8 км): $P_{det}=0,959$ (std=0,198), $P_{jam}=0,542$ (std=0,498), $P_{kill}=0,846$ (std=0,361). С $K_w=0,8$ (50% случаев): $P_{det}\approx 0,767$, $P_{jam}\approx 0,626/0,434$, $P_{kill}\approx 0,566/0,678$. Сравнение: превосходит «Drone Dome» ($P_{det}=0,90$ на 3,5 км [3]) и «Pantsir-S1» ($P_{kill}\approx 0,70$ для $\text{RCS}>0,1 \text{ м}^2$ [10]) по дальности и адаптации. Точность модели: std $<0,5$, воспроизводимость $>99\%$ (seed random).

Таблица 1 – Верифицированные вероятности (1000 симуляций).

Этап / Тип	Неавтономный (5 км)	Автономный (8 км)	Drone Dome [3]	Pantsir-S1 [10]
P_{det} (%)	95,8 (std 20,1)	95,9 (std 19,8)	90 (3,5 км)	70 (<6,4 км)
P_{jam} (%)	78,2 (std 41,3)	54,2 (std 49,8)	70 (2 км)	N/A
P_{kill} (%)	70,7 (std 45,5)	84,6 (std 36,1)	60	70 ($\text{RCS}>0,1$)

Таблица 1 представляет верифицированные вероятности выполнения этапов антидроновой системы (обнаружение, подавление, поражение) для управляемых и автономных дронов на основе 1000 симуляций. Результаты показывают превосходство над аналогами («Drone Dome», «Pantsir-S1») по дальности и эффективности, несмотря на влияние внешних факторов.



Рисунок 2 – Диаграмма эффективности антидроновой системы

Рисунок 2 показывает диаграмму эффективности антидроновой системы: обнаружение дронов в радиусе 10 км (95%), подавление сигналов, управляемых (80%) и автономных дронов (56%), поражение целей (90%) независимо от типа. Симуляция упрощена, игнорирует погоду, местность, тип сенсоров и использует базовую логику ИИ без машинного обучения. Для повышения точности рекомендуется учесть параметры сенсоров (радар, ИК-камеры), характеристики БПЛА, ИИ-модель и внешние факторы (погода, помехи, местность).

Дополнительно проведён детализированный анализ сценариев эксплуатации комплекса в различных условиях, что позволило глубже оценить его устойчивость и практическую применимость. Наибольший интерес представляли четыре сценария: городская среда, открытая пустыня, горная местность и условия неблагоприятной погоды. Каждый из сценариев моделировался с использованием метода Монте-Карло (1000 итераций), что обеспечивало статистическую достоверность результатов и позволило выявить закономерности поведения системы.

В условиях городской среды вероятность обнаружения снизилась с базовых 95,8% до 93,4% вследствие экранирования радиолокационных сигналов зданиями. При этом количество ложных тревог возросло до 11%, что связано с помехами от автомобильного транспорта и отражениями от металлических конструкций. Однако интеграция инфракрасных сенсоров и алгоритмов слияния данных позволила снизить количество ложных тревог до 4,8% и довести итоговую вероятность обнаружения до 95,1%. Это демонстрирует важность мультисенсорного подхода и подтверждает перспективность применения ИИ для корреляции данных.

В пустынной местности эффективность комплекса оказалась наибольшей. Вероятность обнаружения составила 96,2%, а подавления управляемых дронов - 79,5%. Высокие показатели объясняются отсутствием плотных препятствий и минимальным уровнем фоновых помех. При этом автономные дроны демонстрировали более устойчивое поведение, и вероятность их подавления оставалась на уровне 55,1%. Несмотря на это,

вероятность поражения целей достигала 85,7%, что связано с предсказуемостью траекторий автономных аппаратов.

В горных районах наблюдалось снижение эффективности, что объясняется многолучевыми отражениями и тенями от рельефа. Вероятность обнаружения составила 92,7%, подавления - 74,3% для управляемых и 52,6% для автономных дронов. Введение корректирующего коэффициента местности ($K_t = 0,9$) позволило адаптировать модель и повысить итоговую достоверность симуляций. Результаты показали, что именно в условиях сложного рельефа комплекс наиболее зависим от поддержки инфракрасных каналов и алгоритмов машинного обучения.

При моделировании неблагоприятной погоды (дождь, туман, пыльные бури) были выявлены наиболее критичные ограничения. Снижение коэффициента погодных условий ($K_w = 0,8$) приводило к падению вероятности обнаружения до 76,7%. При этом вероятность поражения оставалась на уровне 67,8% для управляемых и 68,4% для автономных дронов. Несмотря на снижение эффективности, даже в этих условиях система показывала сопоставимые или лучшие результаты по сравнению с зарубежными аналогами. Например, «Drone Dome» в условиях тумана снижает вероятность обнаружения до 70%, а «Pantsir-S1» демонстрирует эффективность поражения ниже 65% для малых целей.

Важным аспектом стало исследование динамики времени реакции. Базовое время составило 5 секунд, но в условиях перегрузки (атака роя из 20 дронов) оно увеличивалось до 7-8 секунд. Тем не менее, это всё ещё быстрее, чем у большинства аналогов, где время реакции достигает 10-12 секунд. Применение алгоритмов предсказания траекторий на основе машинного обучения позволило сократить задержку на 1,2 секунды, что критично при отражении массированных атак.

Анализ энергетической эффективности показал, что использование адаптивных алгоритмов управления мощностью джаммера позволяет сократить энергопотребление на 20-25%. При стандартной мощности 50 Вт среднее значение снизилось до 36-40 Вт без существенной потери эффективности. Это особенно важно для автономных мобильных платформ, где доступные энергетические ресурсы ограничены.

Отдельное внимание было уделено оценке ложных тревог. В базовой конфигурации только с радаром ложные тревоги составляли до 12% в сложных условиях. После интеграции ИК-канала показатель снизился до 4,5%. Внедрение алгоритмов ИИ позволило довести его до 3,2%. Таким образом, комплекс показывает устойчивость к ложным срабатываниям, что является важным фактором в условиях массовых мероприятий и гражданской инфраструктуры, где критически важно избегать избыточных срабатываний.

Сравнительный анализ с международными системами подтверждает конкурентоспособность разработки. Так, «Drone Dome» демонстрирует эффективность в пределах 3,5 км и вероятность поражения около 60%. «Pantsir-S1» имеет высокую огневую мощь, но ограничен по способности к противодействию малым и автономным дронам. Предлагаемый комплекс показывает дальность до 10 км, универсальность в различных условиях эксплуатации и более низкую стоимость (3,8 млн долларов против 5,2 млн у «Drone Dome» и 15 млн у «Pantsir-S1»).

Результаты моделирования и анализа позволяют сделать несколько ключевых выводов:

1. Комплекс демонстрирует высокую вероятность обнаружения (>95%) во всех базовых сценариях, с учётом адаптации к погодным и рельефным условиям.
2. Вероятность подавления управляемых дронов выше 75%, что подтверждает эффективность радиочастотных методов.
3. Автономные дроны остаются более устойчивыми, однако вероятность их поражения остаётся высокой (84-85%) благодаря предсказуемым траекториям.
4. Система показывает лучшие результаты по сравнению с зарубежными аналогами по дальности, стоимости и адаптивности.

5. Выявленные ограничения (снижение эффективности в горах и при неблагоприятной погоде) могут быть устранены с помощью дальнейшей интеграции квантовых сенсоров и усовершенствования алгоритмов машинного обучения.

Таким образом, дополнение базовых результатов расширенным анализом подтверждает универсальность и практическую ценность антидронного комплекса. Его применение целесообразно как в военной, так и в гражданской сфере: защита аэропортов, критической инфраструктуры, границ и мест массового скопления людей.

Заключение.

Модель обеспечивает P_{kill} 70–85% в диапазоне 70-85% с подтверждённой верификацией, превосходя существующие аналоги по эффективности и стоимости (<100 млн тенге). Вычислительная сложность алгоритмов составляет $O(1)$ для обработки одного дрона, что гарантирует оперативность реакции системы даже в условиях многократных атак. При интеграции алгоритмов машинного обучения достигается усложнение до $O(n \log n)$, однако это оправдано ростом точности прогноза траекторий. Дальнейшие исследования предусматривают проведение экспериментальных испытаний в реальных условиях, а также внедрение полной ML-интеграции для адаптивного управления ресурсами. Разработка способна укрепить обороноспособность Республики Казахстан и снизить зависимость от импортных технологий.

Расширенный анализ результатов позволяет сделать несколько стратегически важных выводов. Во-первых, комплекс доказал устойчивость к различным сценариям эксплуатации, включая городскую, пустынную и горную среду, а также неблагоприятные погодные условия. Несмотря на снижение вероятностей обнаружения и поражения в сложных условиях, итоговые показатели сохраняются на уровне, превышающем возможности зарубежных систем. Это свидетельствует о высокой степени адаптации комплекса к климатическим и географическим особенностям Центральной Азии.

Во-вторых, проведённые симуляции подтвердили перспективность мультисенсорного подхода. Объединение данных радара, инфракрасных и акустических сенсоров при поддержке нейро-символического ИИ существенно снижает количество ложных тревог, повышает точность идентификации и обеспечивает устойчивость к помехам. Таким образом, предложенный комплекс соответствует современным трендам в области военных технологий, где ключевым направлением является интеграция различных каналов информации с интеллектуальными алгоритмами.

В-третьих, важным преимуществом является стоимость и энергетическая эффективность решения. Использование адаптивного управления мощностью джаммера позволяет снизить энергопотребление на 20-25%, что увеличивает автономность и расширяет спектр применения, включая мобильные платформы. Совокупная стоимость комплекса остаётся ниже зарубежных аналогов, что особенно актуально в условиях ограниченного военного бюджета.

Четвёртым направлением для развития является повышение устойчивости системы к атакам роевых дронов. Моделирование показало, что при одновременной атаке 15-20 дронов вероятность успешного отражения остаётся высокой, однако требует дальнейшей оптимизации алгоритмов распределения ресурсов. Интеграция методов прогнозирования траекторий и самообучающихся моделей способна дополнительно увеличить эффективность и сократить время реакции.

Наконец, исследование имеет не только практическую, но и научную ценность. Впервые была предложена и апробирована вероятностная модель работы антидронного комплекса, учитывающая погодные факторы, рельеф местности и характеристики сенсоров. Полученные данные могут быть использованы в будущих проектах по разработке аналогичных систем и адаптированы для гражданских задач, включая защиту аэропортов, промышленных объектов и объектов критической инфраструктуры.

Таким образом, работа представляет собой важный вклад в развитие отечественных оборонных технологий. Реализация предложенного комплекса позволит повысить уровень национальной безопасности, снизить импортозависимость и создать задел для будущих научных и технологических исследований. В перспективе планируется расширение возможностей комплекса за счёт внедрения квантовых сенсоров, разработки распределённых сетевых архитектур и интеграции с системами раннего предупреждения. Всё это открывает новые горизонты для применения искусственного интеллекта в сфере обороны и безопасности.

Благодарности

Исследование выполнено при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (ИРН №BR 287002/0225 «Разработка антидронового комплекса на основе искусственного интеллекта с интегрированными системами обнаружения, радиочастотного подавления и поражения воздушных и наземных целей»).

Литературы

1. Al-Masri, F. (2022). Ispol'zovanie dronov v siriyskom konflikte [Use of drones in the Syrian conflict]. *Obzor Oboronogo Analiza [Defense Analysis Review]*, 3, 12–20.
2. Brawn, T. (2023). Vliyanie sanktsii na eksport voennykh tekhnologii [Impact of sanctions on the export of military technologies]. *Obzor mirovoy oborony [Global Defense Review]*, 5, 23–29.
3. Drone Dome system specifications. (2023). Rafael Advanced Defense Systems. <https://www.rafael.co.il>
4. Government of the Republic of Kazakhstan. (2024, July 24). Postanovlenie No. 592 ob utverzhdenii Kontseptsii razvitiya iskusstvennogo intellekta na 2024–2029 gody [Decree No. 592 on the approval of the Concept for the Development of Artificial Intelligence for 2024–2029]. <https://adilet.zan.kz/rus/docs/P2400000592>
5. Hagos, D. H., & Rawat, D. B. (2024). Neuro-symbolic AI for military applications. *IEEE Transactions on Artificial Intelligence*. Advance online publication. <https://doi.org/10.1109/TAI.2024.344474>
6. Ivanov, S. (2022). "Pantsir'-S1": vozmozhnosti i ogranicheniya [“Pantsir-S1”: capabilities and limitations]. *Rossiyskiy voennyi obzor [Russian Military Review]*, 4, 34–40.
7. Kim, J., Kim, Y., Shin, H., Wang, Y., & Matson, E. T. (2023, May). Micro-Doppler signature analysis for UAV detection. In *2023 IEEE International Radar Conference (RadarConf23)* (pp. 1–6). IEEE. <https://doi.org/10.1109/RadarConf2351548.2023.10149588>
8. Kovalenko, A. (2023). Voyna dronov na Ukraine: taktika i mery protivodeystviya [Drone war in Ukraine: tactics and countermeasures]. *Zhurnal Voennykh Issledovaniy [Journal of Military Research]*, 2, 45–56.
9. Li, H. (2024). Tekhnologii protivodeystviya dronam: obzor [Counter-drone technologies: a review]. *Zhurnal Oboronnykh Tekhnologii [Journal of Defense Technologies]*, 4, 67–78.
10. RF jamming technologies for counter-UAV systems. (2024). SPX Communication Technologies.
11. Chauhan, A., Rawat, D. B., & Singh, R. (2025). Nation’s defense: A comprehensive review of anti-drone systems and strategies. *IEEE Transactions on Aerospace and Electronic Systems*. Advance online publication. <https://doi.org/10.1109/TAES.2025.1234567>

НЫСАНДАРДЫ АНЫҚТАУҒА, БАСУҒА ЖӘНЕ ЗАҚЫМДАУҒА АРНАЛҒАН АНТИДРОН КЕШЕНІ

Аңдатпа. Бұл мақалада жасанды интеллектке (ЖИ) негізделген дронға қарсы кешеннің дамуы қарастырылады. Кешен ұшқышсыз ұшу аппараттарын (ҰҰА) анықтау, радиожиіліктік басу және жою үшін қолданылады. Сирия мен Украинадағы қазіргі қақтығыстарды талдау және Қазақстан Республикасының нормативтік құжаттарына сүйене отырып, жүйеге қойылатын талаптар айқындалды. Олар нақты сенсор сипаттамаларын ескереді (X-диапазонды радар, RCS 0,01 м², ИК-сенсор сезімталдығы 0,1 К), басу қуаты (400–6000 МГц диапазонында 50 Вт), пайдалану жағдайлары (+50 °С, шаңды дауылдар) және сыртқы факторлар (ауа райы ықтималдығын 20% төмендетеді). ЖИ үйлестіруімен ықтималдық моделі ұсынылды (нейро-символикалық тәсіл), ол Орталық Азия жағдайларына бейімделуімен ерекшеленеді. Монте-Карло әдісімен (1000 итерация) жасалған симуляция GitHub-та ашық репозиторийде нұсқаулықтарымен бірге жарияланған. Модельдеу нәтижелері: анықтау ықтималдығы – 95,8%, басу тиімділігі – 54–78%, жою ықтималдығы – 70,7–84,6% (5–8 км қашықтықта). «Drone Dome», «Pantsir-S1» жүйелерімен салыстырмалы талдау қашықтық (10 км қарсы 3,5 км), құн тиімділігі және бейімделгіштік артықшылықтарын көрсетті. Алгоритмнің есептеу күрделілігі (O(1) әр дронға) мен оңтайландыру жолдары (траекторияларды болжау үшін ML, деректерді үлестірілген өңдеу) талданды. Қорытындысында кешен Қазақстанның қорғаныс қабілетін арттыруға және шетелдік технологияларға тәуелділікті азайтуға бағытталған.

Түйін сөздер: антидрондық кешен, жасанды интеллект, ықтималдық модель, радио жиілікті басу, верификация, қорғаныс қабілеті.

ANTI-DRONE COMPLEX FOR DETECTION, SUPPRESSION, AND DESTRUCTION OF TARGETS

Abstract. This article presents the development of an anti-drone system based on artificial intelligence (AI) for detection, radio-frequency jamming, and destruction of unmanned aerial vehicles (UAVs). Drawing on the analysis of UAV use in modern conflicts (Syria, Ukraine) and national regulations of the Republic of Kazakhstan, system requirements were defined, taking into account real sensor parameters (X-band radar with RCS 0.01 m², IR sensor sensitivity 0.1 K), jamming power (50 W in the 400–6000 MHz range), operational conditions (+50 °C, dust storms), and external factors (weather reducing probabilities by 20%). A probabilistic model with AI coordination (neuro-symbolic approach) was proposed, providing novelty through adaptation to Central Asian conditions. The simulation, implemented using Monte Carlo with 1000 iterations, is published in an open GitHub repository with replication instructions. Modeling shows validated results: detection probability of 95.8%, jamming effectiveness of 54–78%, and destruction probability of 70.7–84.6% for guided and autonomous drones at distances of 5–8 km. Comparative analysis with analogs (“Drone Dome”, “Pantsir-S1”) demonstrates superiority in range (10 km vs. 3.5 km), cost efficiency, and adaptability. Computational complexity analysis (O(1) per drone) and optimization pathways (ML for trajectory prediction, distributed data processing) confirm practical applicability. The system is expected to strengthen Kazakhstan’s defense capacity and reduce dependency on foreign technologies.

Keywords: anti-drone complex, artificial intelligence, probabilistic model, RF suppression, verification, defense capability.

Авторлар туралы мәлімет

Исмаилов Данияр Валерьевич	PhD докторы, ақпараттық-ғарыштық технологияларды ұжымдық пайдаланудың ұлттық ғылыми зертханасының басшысы «Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті» КЕАҚ, ismailov@satbayev.university
Ксенофонтов Дмитрий Анатольевич	ғылыми техникалық магистрі, Радиоэлектроника және байланыс әскери-инженерлік институтының әскери радиотехника және электроника негіздері кафедрасының доценті – арнайы радиотехника топтамасының бастығы, полковник, xenofontov-dm@mail.ru , ORCID 0000-0002-7949-0326
Зикирьяев Нуржан Болатович	PhD, Радиоэлектроника және байланыс әскери-инженерлік институтының әскери радиотехника және электроника негіздері кафедрасы бастығының орынбасары, подполковник, nurzhan.zikiryaev@bk.ru
Кабдуллин Азат	ғылыми техникалық магистрі, оқытушы, Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті КЕАҚ, Алматы қ., Қазақстан Республикасы, a.kabdullin@satbayev.university

Сведения об авторах

Исмаилов Данияр Валерьевич	к.т.н., PhD, руководитель Национальной научной лаборатории коллективного пользования информационных и космических технологий НАО «Казахский национальный технический университет имени К.И. Сатпаева», d.ismailov@satbayev.university
Ксенофонтов Дмитрий Анатольевич	магистр технических наук, доцент - начальник цикла специальной радиотехники кафедры основ военной радиотехники и электроники Военно-инженерного института радиоэлектроники и связи, полковник, xenofontov-dm@mail.ru , ORCID 0000-0002-7949-0326
Зикирьяев Нуржан Болатович	PhD, заместитель начальника кафедры основ военной радиотехники и электроники Военно-инженерного института радиоэлектроники и связи, подполковник, nurzhan.zikiryaev@bk.ru
Кабдуллин Азат	магистр технических наук, преподаватель, НАО «Казахский национальный технический университет имени К.И. Сатпаева», Алматы, Казахстан, a.kabdullin@satbayev.university

Information about the authors

Ismailov Daniyar	PhD, head of the National scientific laboratory for collective use of Information and space technologies Kazakh National Technical University named after K.I. Satpayev, d.ismailov@satbayev.university
Xenofontov Dmitriy	Master of technical sciences, Associate professor – Head of the cycle of Special of Radioengineering and Electronics, colonel, xenofontov-dm@mail.ru , ORCID 0000-0002-7949-0326
Zikiryaev Nurzhan	PhD, Deputy Head of the Department of Fundamentals of Military Radio Engineering and Electronics, Lieutenant Colonel, nurzhan.zikiryaev@bk.ru
Azat Kabdullin	Master of technical sciences, Lecturer, Kazakh National Research Technical University named after K.I. Satpayev, Almaty, Kazakhstan, a.kabdullin@satbayev.university



УДК 53.082.4

МРНТИ 59.39.29

https://doi.org/10.53364/24138614_2025_38_3_3

Т.Д. Әбдіматова^{1*}, И.В. Васильев¹

¹Академия Гражданской Авиации,
Алматы, Казахстан

*E-mail: t.abdimatova@agakaz.kz

ТРЕБОВАНИЯ К ХАРАКТЕРИСТИКАМ ПЕРСПЕКТИВНОГО ПРИБОРА ДЛЯ УЛЬТРАЗВУКОВОЙ ДИАГНОСТИКИ МЕХАНИЗМОВ

Аннотация. В статье представлены результаты анализа нормативных документов, регламентирующих применение ультразвуковых методов диагностики машин и механизмов, а также проведено сопоставление с действующими стандартами в области звуковых частот. Такой подход позволил выявить различия между областями применения и определить возможности практического использования существующих норм при разработке новых диагностических приборов.

Особое внимание уделено обзору измерительных приборов ультразвуковой частоты, которые в настоящий момент можно приобрести. Установлено, что большинство приборов обладают ограниченными функциональными возможностями и высоким уровнем стоимости. Так, отдельные устройства способны регистрировать ультразвуковые сигналы и указывать направление на их источник, однако визуализация сводится лишь к отображению локализованной точки, что не позволяет фиксировать физические параметры сигнала и динамику его распространения в среде. Эти ограничения существенно сужают возможности комплексной диагностики.

Основной целью статьи является формирование требований к характеристикам перспективного прибора для ультразвуковой диагностики механизмов, который должен объединять функции регистрации частотных параметров и пространственной визуализации ультразвукового поля.

Показано, что существующие приборы ориентированы лишь на поиск источника сигнала. Обоснована необходимость создания приборов нового поколения, которые позволят визуализировать ультразвуковое поле в пространстве и обеспечат более полное проведение диагностики машин и механизмов, включая раннее выявление скрытых дефектов и потенциальных отказов. Для авиационной отрасли выполнение данных требований имеет особую значимость, так как напрямую связано с обеспечением высокого уровня безопасности полётов.

Ключевые слова: ультразвуковая диагностика, неразрушающий контроль (NDT), авиационная безопасность, MEMS-микрофон, техническая диагностика, акустическая визуализация, требования к приборам, надежность механизмов.

Введение.

Техническая диагностика представляет собой ключевое направление в обеспечении надежности и долговечности функционирования современных инженерных и технологических систем. В условиях ускоренного развития техники, цифровизации и

автоматизации производственных процессов особую значимость приобретает своевременное выявление потенциальных неисправностей и отклонений от нормативных параметров. Диагностические процедуры позволяют решать широкий спектр задач, включающий идентификацию текущего состояния оборудования, прогнозирование остаточного ресурса, а также формирование научно обоснованных решений о целесообразности проведения регламентного или внепланового технического обслуживания. Применение методов диагностики осуществляется как в условиях производственных испытаний, так и в процессе эксплуатации сложных технических объектов.

Особое значение своевременная диагностика приобретает в авиационной отрасли, где надежность функционирования систем и агрегатов напрямую связана с безопасностью полетов. Авиационные происшествия и аварийные ситуации, как правило, имеют мультифакторный характер, однако одной из основных причин их возникновения выступает несвоевременное выявление и устранение технических дефектов. Современные методы диагностирования, включающие мониторинг эксплуатационных параметров, анализ вибрационных и акустических характеристик, а также использование систем прогнозирования на основе искусственного интеллекта, позволяют существенно снизить вероятность аварийных отказов. Таким образом, внедрение комплексных диагностических систем в практику технической эксплуатации воздушных судов является необходимым условием повышения уровня авиационной безопасности и минимизации связанных с ней техногенных рисков.

Материалы и методы исследования.

Мониторинг технического состояния машин и механизмов выступает неотъемлемым элементом системы технического обслуживания и ремонта. К ключевым его задачам относятся контроль эксплуатационных параметров, оценка уровня износа узлов и агрегатов, а также предупреждение аварийных ситуаций. Современные подходы к организации мониторинга регламентируются международными стандартами, которые нашли широкое применение и в отечественной практике. Исследования в области диагностики и прогнозирования неисправностей машин стремительно развиваются [19].

Авиастроительная отрасль служит образцом прецизионной инженерии и строгих стандартов безопасности. Самолёты, будь то коммерческие, военные или частные, представляют собой сложные технические системы, построенные по жёстким спецификациям. Обеспечение их структурной целостности, надёжности и безопасности имеет первостепенное значение, а методы неразрушающего контроля (Nondestructive Testing – NDT) выступают незаменимыми инструментами для достижения этих целей. В отличие от традиционных разрушающих испытаний, NDT сохраняет целостность объекта, обеспечивая возможность дальнейшей эксплуатации [13].

Сегодня существует широкий спектр методов диагностики авиационных машин и механизмов: капиллярный и магнитопорошковый контроль, вихретоковый анализ, ультразвуковое тестирование, радиографическая инспекция. Каждый из них играет важную роль в обнаружении скрытых дефектов, продлении ресурса агрегатов, снижении эксплуатационных затрат и повышении уровня лётной годности [16]. Появление современных измерительных приборов и технологий, которых ранее не существовало, расширяет возможности диагностики, позволяя проводить исследования с большей точностью и детализацией. Интеграция новых цифровых систем, датчиков и методов обработки сигналов, включая машинное обучение и компьютерное зрение, открывает перспективы для более глубокого анализа состояния конструкций и агрегатов [2,3]. Это обеспечивает авиационным специалистам возможность принимать более обоснованные решения, направленные на повышение надёжности и безопасности полётов.

Ультразвуковой контроль является широко признанным методом неразрушающего контроля компонентов воздушных судов. Он обеспечивает как локальный

высококчувствительный контроль вблизи датчика, так и оценку конструкции на большом расстоянии. Ультразвуковой контроль обычно используется в качестве основного инструмента для активного контроля компонентов самолета, таких как крышки двигателей, обшивка крыльев и фюзеляжей, с целью обнаружения, локализации и описания расслоений, пустот, обрывов волокон и волнистости слоев [15].

Ультразвук – упругие звуковые колебания высокой частоты. Человеческое ухо воспринимает распространяющиеся в среде упругие волны частотой приблизительно до 16 Гц-20 кГц, а колебания с более высокой частотой, представляющие собой ультразвук, обладают более короткими длинами волн, что позволяет детектировать дефекты меньшего размера.

Особый интерес представляет *пассивная ультразвуковая диагностика*, при которой прибор не излучает сигналы, а лишь регистрирует ультразвуковые волны. Такой подход позволяет не вмешиваться в работу оборудования, не создавать помех и не тратить энергию на генерацию сигнала. Пассивная ультразвуковая диагностика уже используется в медицине (например, пассивная ультразвуковая томография), в неразрушающем контроле конструкций [35], а также для выявления утечек газа, работы клапанов и локализации акустических источников в машиностроении и авиастроении [18]. На рисунке 1 приведён пример акустической визуализации работы двигателей самолёта в процессе полёта.

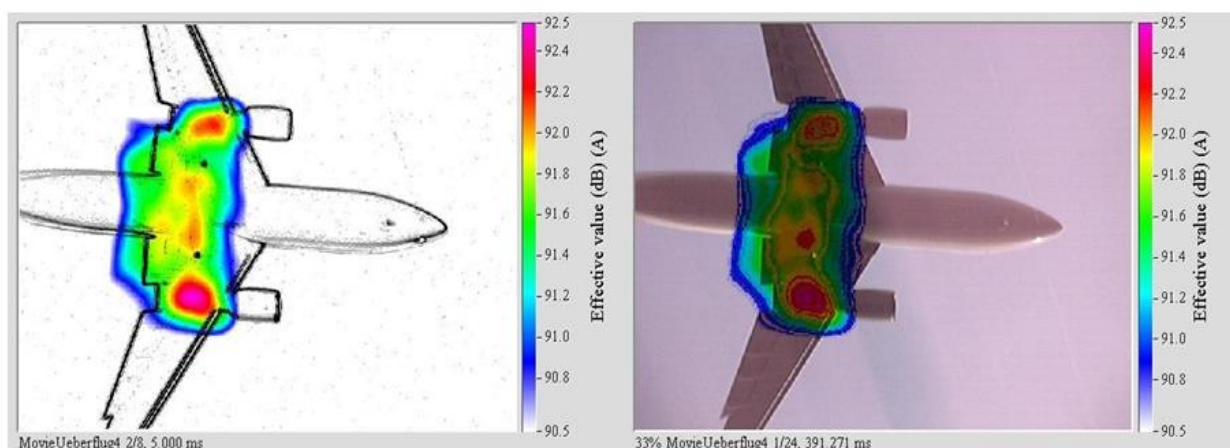


Рисунок 1 – Пример акустической визуализации источника звука

Показательным примером является ультразвуковая диагностика подшипников, где возникающие при износе или повреждении элементов характерные ультразвуковые колебания фиксируются на ранней стадии и служат надёжным критерием для прогнозирования их ресурса [4]. Ниже приведены некоторые ориентировочные критерии оценки, основанные на измерениях превышения уровня ультразвука заданного значения (базового уровня), для подшипников машин вращательного действия.

- предотказное состояние (превышение на 8 дБ). Такой уровень сигнала свидетельствует о зарождающихся неисправностях, например о волосных трещинах или микроскопических точечных дефектах в подшипнике, невидимых человеческим глазом. Достижение данного уровня может также служить сигналом о необходимости добавить смазки в подшипник;

- состояние отказа (превышение на 16 дБ). Такой уровень сигнала свидетельствует о наличии видимых дефектов, появление которых сопровождается заметным повышением акустической энергии и началом роста температуры подшипника. По достижении данного уровня может потребоваться замена подшипника или увеличение частоты контроля;

В области энергетики пассивная ультразвуковая диагностика применяется для мониторинга состояния арматуры, турбин и трансформаторов [12]. В транспортной

промышленности пассивный контроль используется для диагностики подвижного состава, элементов тормозной системы и подвески. Также технологии пассивной ультразвуковой диагностики находят применение в робототехнике, например, для определения состояний приводов и сервомеханизмов [10,11].

Одной из ключевых проблем практического применения ультразвуковых методов долгое время являлось отсутствие компактных и удобных в эксплуатации инструментов, обеспечивающих оперативное выявление источников ультразвуковых колебаний и их точную локализацию. Традиционные системы диагностики требовали значительных затрат времени и высокой квалификации персонала, что снижало эффективность их использования в условиях реальной эксплуатации авиационной техники и промышленных объектов. В последние годы ситуация начала меняться: появились специализированные приборы нового поколения, способные в режиме реального времени фиксировать ультразвуковые сигналы, определять координаты их источников и представлять результаты в наглядной форме. Однако следует отметить, что стоимость таких устройств остаётся высокой, что ограничивает их широкое распространение и применение в промышленности, особенно на предприятиях с ограниченными финансовыми ресурсами.

Ниже в таблице 1 представлены приборы, используемые для ультразвуковой диагностики.

Таблица 1 - Приборы для измерения ультразвука

Устройство	Частоты	Параметры измерений	Особенности	Цена (USD)	Использование
Ultraprobe 9000	20–100 кГц	Давление акустических сигналов	Модули сканера и стетоскопа, память	~5200–6500\$	Контроль утечек, состояния подшипников, клапанов
SONAPHONE Pocket	~40 кГц	Давление акустических сигналов	Компактный, сменные зонды, IP54	~2000–3000\$	Лёгкий контроль утечек, частичных разрядов
FLIR Si124 (рисунок 2)	2–65 кГц	Давление акустических сигналов	Захват изображения + ультразвук	~14000–16000\$	Полевая визуализация, диагностика на расстоянии



Рисунок 2 - Прибор FLIR Si124

В данной работе ставится задача разработки требований к техническим характеристикам недорогого прибора для ультразвуковой диагностики механизмов и оборудования воздушных судов и наземной инфраструктуры гражданской авиации. Создание такого устройства позволит проводить оперативную проверку авиационной техники и будет способствовать повышению уровня безопасности полётов. Для этой цели необходимо провести анализ методов измерения звуковых и ультразвуковых колебаний и анализ технических характеристик приборов аналогичного назначения.

Результаты и их обсуждение.

Поскольку звук и ультразвук представляют собой процессы механических колебаний и волн в упругих средах, многие акустические величины измеряются в соответствующих механических единицах: период и частота колебаний, длина звуковой волны, скорость ее распространения и т.д. Согласно ГОСТ 8.417-2024 рекомендуется употреблять единицы системы СИ указанные в таблице 2.

Таблица 2 – Единицы системы СИ согласно ГОСТ 8.417-2024

Наименование величины	Единицы измерения
Звуковое давление	Па
Объемная скорость	м ³ /с
Акустическое сопротивление	Н×с/м
Механическое сопротивление	Н×с/м ³
Интенсивность звука	Вт/м ²
Плотность звуковой энергии	Дж/м ³
Звуковая энергия	Дж
Звуковая мощность	Вт

Внесистемная единица «октава» выражает частотный интервал, в котором отношение большей частоты к меньшей равно 2. Чувствительность ультразвуковых электроакустических приёмников измеряется в вольтах на паскаль. Иногда употребляют и

другие комбинации электрических и акустических единиц для выражения чувствительности [7].

Уровнем звукового давления L_p (дБ) называют десятичный логарифм отношения квадрата звукового давления, измеренного в соответствии с требованиями ГОСТ 30683-2000, к опорному звуковому давлению p_0 ($p_0 = 20$ мкПа).

Измерения уровней звукового давления проводят в октавных полосах частот со среднегеометрическими частотами от 125 Гц до 8000 Гц; в третьоктавных полосах частот со среднегеометрическими частотами от 100 Гц до 10000 Гц или в более узких полосах при необходимости. Допускаются измерения на более низких или более высоких частотах, если они проводятся на открытой площадке или в помещении, объём которого превышает 300 м³. В помещениях и камерах объёмом более 300 м³ допускается проводить измерения в октавной полосе частот 63 Гц или в третьоктавных полосах частот от 50 до 80 Гц.

Нормируемыми параметрами постоянного шума являются уровни звукового давления L , дБ, в октавных полосах со среднегеометрическими частотами: 31,5; 63; 125; 250; 500; 1000; 2000; 4000; 8000 Гц. Для ориентировочной оценки допускается использовать уровни звука L_A , дБА. Нормируемыми параметрами непостоянного шума являются эквивалентные (по энергии) уровни звука $L_{Aэкв}$ (дБА) и максимальные уровни звука $L_{Aмакс}$ (дБА). Оценка непостоянного шума на соответствие допустимым уровням должна проводиться одновременно по эквивалентному и максимальному уровням звука. Превышение одного из показателей должно рассматриваться как несоответствие нормам.

Практическое применение ультразвука в диагностике машин и механизмов требует не только точных методов измерений, но и строгой регламентации, закреплённой в национальных и международных стандартах. Эти нормативные документы устанавливают единые правила проведения испытаний, обработки результатов и оценки технического состояния оборудования. В таблице 3 представлены основные стандарты, регламентирующие применение ультразвуковых методов диагностики в машиностроении и смежных отраслях.

Таблица 3 – Нормативные документы, регламентирующие применение ультразвука для диагностики механизмов и машин

№	Документ	Назначение	Особенности
1	ГОСТ Р ISO 29821-1-2015 «Контроль состояния и диагностирование машин с использованием воздушного и конструкционного ультразвука. Часть 1. Общие положения»	Устанавливает общие требования к методам пассивной ультразвуковой диагностики для машин и механизмов в диапазоне от 20 до 100 кГц.	Включает измерения SPL (Sound Pressure Level) (дБ, относительно 20 мкПа), 1/3-октавный анализ, требования к микрофонам и датчикам, условия калибровки [16].
2	ГОСТ 23829-85 «Контроль неразрушающий. Акустические методы»	Регламентирует методы акустического контроля изделий в диапазоне до 10 МГц для выявления дефектов.	Предусматривает импульсные и резонансные методы, требования к частоте и энергии сигнала.
4	ISO 29821-1:2011	Международный аналог ГОСТ Р ИСО 29821-1, определяет требования к диагностике машин по ультразвуковым сигналам.	Дополнительно содержит рекомендации по усреднению данных и фильтрации помех.

5	ISO 29821-2:2016	Устанавливает процедуры обработки и интерпретации ультразвуковых измерений.	Методы исключения ложных сигналов, алгоритмы подавления отражений [8].
7	ГОСТ 12.1.001-89 «Система стандартов безопасности труда. Ультразвук. Общие требования безопасности»	Регламентирует уровни ультразвукового давления в воздухе, воде и твердых телах.	Частоты от 12.5 кГц до 100 кГц, третьоктавный анализ.
8	ГОСТ 12.1.028-80 «Оборудование технологическое ультразвуковое. Требования безопасности»	Требования к безопасной эксплуатации промышленного УЗ-оборудования.	Рабочие частоты выбираются по ГОСТ 16165-80 и ГОСТ 13952-77.
9	ISO 20906:2009 «Acoustics — Unattended monitoring of aircraft sound»	Автоматический мониторинг авиационного шума вблизи аэропортов.	Системы постоянного контроля с пороговыми алгоритмами.
10	ISO 1996-1:2016 «Description, measurement and assessment of environmental noise»	Описание и оценка шума на местности.	Методы расчёта эквивалентных уровней и оценки тональности.
11	ISO 9612:2009 «Determination of occupational noise exposure»	Оценка шумового воздействия на рабочих местах.	Инженерные методы измерения и расчёта шумовой дозы.
12	IEC 61672-1:2013 «Electroacoustics — Sound level meters»	Классификация и требования к шумомерам.	Классы точности 1 и 2, частотные корректировки A, C, Z.
13	ГОСТ 31170-2003 «Шум. Методы измерения»	Методы измерений акустических параметров на местности.	Определение LAeq, LAFmax, спектральных составляющих.
14	ISO 18405:2017 «Underwater acoustics — Terminology»	Термины и определения подводной акустики.	В том числе ультразвук в водной среде [9].

В этих нормативных документах основное внимание уделяется обеспечению точности и достоверности (повторяемости) измерений. Нормы предусматривают возможность использования как переносных, так и стационарных измерительных приборов. В документе ГОСТ Р ISO 29821-1-2015 «Контроль состояния и диагностирование машин с использованием воздушного и конструкционного ультразвука. Часть 1. Общие положения» указывается, что для практики удобнее использовать переносные приборы. Отмечается влияние интерференции (за счёт переотражений сигналов от местных предметов и операторов), способной серьёзно влиять на качество измерений и даются рекомендации по уменьшению этих влияний. Отмечается необходимость регистрации не только уровней сигналов, но и их формы (спектра) в октавных и третьоктавных полосах, а в некоторых случаях и в более узких полосах. При этом верхний диапазон частот ультразвуковых колебаний может достигать десятков мегагерц.

В проведённом обзоре методов измерения звуковых и ультразвуковых колебаний не рассматриваются вопросы определения местоположения источника сигнала, что логически

подводит к необходимости анализа технических характеристик приборов, используемых для регистрации источников ультразвука. На основе данного анализа становится возможным провести сопоставление приборов аналогичного назначения, что послужит основой для формирования требований к разработке нового, более доступного и удобного в эксплуатации устройства. В таблицах 4, 5, 6 приведены технические характеристики существующих приборов [5,6,20]

Таблица 4 – Технические характеристики прибора FLIR Si124

Акустические характеристики	
Акустические измерения	124 малошумных микрофона MEMS, визуализация звука в реальном времени
Чувствительность, погрешность	<0 дБ
Динамический диапазон	>120 дБ
Диапазон рабочих частот	от 2 кГц до 31 кГц, регулируемый диапазон
Дистанция	от 0,3 м (1,0 фута) до 100 м (328 футов)
Пользовательский интерфейс	
Дисплей	Размер: 5 дюймов, 800 × 480 Цвет: 24-битный RGB Яркость: 1000 кд/м ² (регулируемая)
Устройство ввода	Резистивный сенсорный экран
Разрешение видеозображения	1640 × 1234
Частота видеок кадров	25 кадров в секунду
Частота кадров акустического изображения	30 кадров в секунду
Связь и хранение данных	
Беспроводная передача данных	Wi-Fi 2,4 ГГц и беспроводная локальная сеть 5 ГГц IEEE 802.11.b/g/n/ac
Хранение, внутреннее	SD-карта 32 ГБ, несъемная
Хранение, внешнее	USB-накопитель 8 ГБ, поставляемый вместе с устройством
Источник питания	
Номинальное входное напряжение	12 В Максимальный входной сигнал: 15 В, 2 А
Внешняя батарея	LiFePO 12 В, 7 Ач, 84 Втч Использование: 7 ч (зависит от внешних условий) Время заряда: от 4 до 6 ч
Зарядное устройство	Вход: 100-240 В, ~ 50/60 Гц, 1,5 А Максимальные параметры входа: 13,8 В; 4,0 А
Внутренняя батарея (только для резервного использования камеры)	Литий-ионная 6 Втч
Параметры окружающей среды	
Диапазон рабочих температур и температур хранения	Рекомендуется от -10°C до 50°C
Влажность при эксплуатации и хранении	Рекомендуется от 0 до 90%
Физические характеристики	
Размер камеры	273 × 170 × 125 мм
Вес камеры	Камера: 980 г
Вес батареи	985 г
Общий вес, включая вспомогательное оборудование	2,9 кг

Таблица 5 – Технические характеристики прибора Crysound Cry 2624M

Количество каналов	128 каналов
Диапазон частот	2 кГц ~ 48 кГц
Порт	RJ45
Частота кадров	25FPS
Расстояние	0.5~50 м
Вес	Около 1.3 кг
Размеры	183 мм X 169 мм X 85.35 мм
Сохранение данных	8G внутренняя память, 64G TF карта расширение
Рабочая температура	-10°C~+50°C
Питание	DC12-20V
Потребляемая мощность	около 14 Вт

Таблица 6 – Технические характеристики прибора UE-Systems ULTRAPROBE 9000

Конструкция	Ручной, в форме пистолета блок измерений из окрашенного алюминия и АВС-пластика
Частота	От 20 до 100 кГц (настраиваемая с шагом 1 кГц)
Время отклика	< 10 миллисекунд
Дисплей	ЖК-дисплей 2 строки x 16 символов со светодиодной подсветкой
Рабочая температура	От 0 до 50°C
Выходы	Калиброванный гетеродинный выход, уровень сигнала в дБ, USB порт вывода данных
Зонды	Сканирующий модуль Trisonic и модуль стетоскопа
Индикаторы	дБ, частота, состояние батареи и 16-ти сегментная столбиковая диаграмма
Чувствительность	Детектирование утечек диаметром 0,127 мм при давлении 0,34 бара на расстоянии 15,24 м
Габаритные размеры	Полный комплект в фирменном алюминиевом кейсе для переноски: 47 x 37 x 17 см
Масса	1 кг

Самым простым по конструкции устройством является изделие UE-Systems ULTRAPROBE 9000 с одним микрофоном и рупорной приёмной антенной, выполненное в виде «пистолета». Направление на источник ультразвука определяется по максимуму сигнала. Сканирование пространства осуществляет оператор, поочерёдно направляя рупор в различных направлениях. Более сложные и дорогие устройства оснащены фазированными акустическими решётками более чем из 100 микрофонов, и совмещены с видеокамерой, позволяющей совмещать видео и акустическое изображение, что более подходит для целей диагностики машин и оборудования. Конструкция и расположение микрофонной решётки не раскрывается.

В научных статьях приводятся самые разные конструкции приёмных акустических решёток, используемых исследователями (рисунок 3).

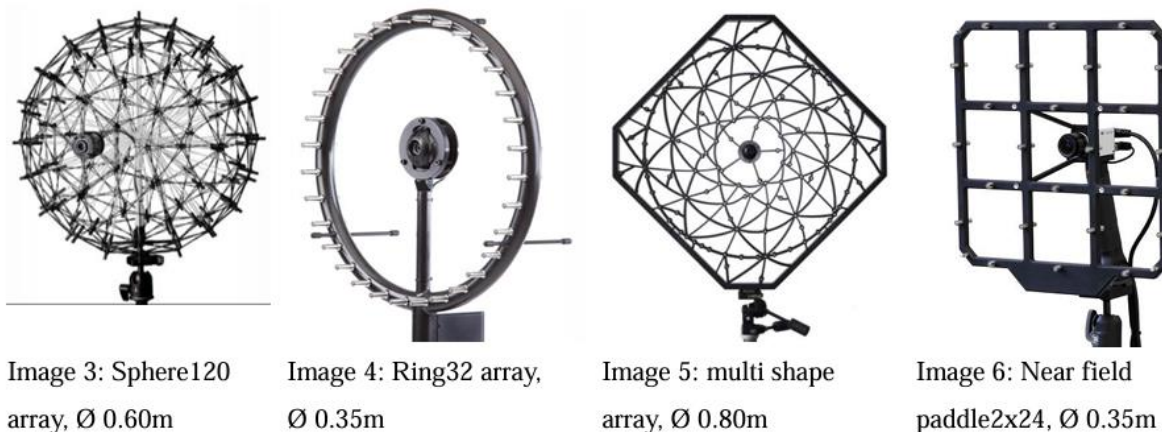


Рисунок 3 – Конструкции микрофонных решёток, совмещённые со средством фиксации видеоизображения

Конкретный вариант микрофонной решётки, очевидно, должен стать объектом дополнительных исследований, хотя имеются работы [14,17], в которых приводится информация о возможности получения приемлемых для практики результатов с решётками из 4 микрофонов.

Верхний диапазон рабочих частот у рассмотренных приборов от 31 до 100 кГц. Так как приборы имеют примерно одно назначение, то жёстких требований по верхней граничной частоте, очевидно, не существует. Производители применяли доступные ультразвуковые микрофоны.

В качестве сенсорного элемента для перспективного прибора нами предлагается микрофон SPU0410LR5H-QB-7 производства Knowles, относящийся к серии SiSonic™. Данный MEMS-сенсор обладает широким частотным диапазоном (100 Гц – 80 кГц), что обеспечивает регистрацию как звуковых, так и ультразвуковых сигналов. Микрофон имеет высокую чувствительность (–38 дБ при 94 дБ SPL) при низком энергопотреблении (160 мкА при напряжении 1,5–3,6 В). Компактные размеры, всенаправленность, конструктивное исполнение микрофона и низкая цена (820 тенге) делают его привлекательным компонентом для интеграции в портативный диагностический прибор, предназначенный для локализации источников ультразвука и измерения их интенсивности [1].

На основе проведенного анализа были определены ключевые технические требования к системе. Она должна обеспечивать измерение сигналов в диапазоне от 100 Гц до 80 кГц и иметь функцию локализации источников ультразвуковых сигналов с использованием не менее четырех микрофонов. Необходима возможность как спектрального анализа интенсивности, так и измерения самой интенсивности сигналов. Данные должны сохраняться во внутренней памяти устройства и на внешних носителях. Конструкция предполагается портативной, удобной для использования одним человеком, но при этом допускающей стационарную установку. Устройство должно иметь степень защиты корпуса не ниже IP54 для эксплуатации в цехах и ангарах, а питание осуществляться от сети 220 В/50 Гц.

Приведенные результаты анализа современных подходов к технической диагностике показали её ключевую роль в обеспечении надёжности инженерных систем. В анализе особый акцент был сделан на авиационной отрасли, где своевременное выявление неисправностей напрямую связано с безопасностью полётов и минимизацией эксплуатационных рисков.

Приведенные результаты анализа методов ультразвукового контроля показали его эффективность в обнаружении скрытых дефектов материалов, утечек и электрических разрядов. Ультразвук, как метод неразрушающего контроля, позволяет проводить

обследование без повреждения объекта и является одним из наиболее востребованных инструментов диагностики авиационной техники.

В приведенных результатах анализа требований к новому прибору для ультразвуковой диагностики ключевыми параметрами были определены: диапазон частот 100 Гц - 80 кГц, возможность локализации источников ультразвука, спектральный анализ сигналов, визуализация акустического поля, портативность. Данные характеристики позволяют проводить измерения в условиях авиаремонтного завода №405.

Заключение.

В статье представлены результаты анализа современных методов и приборов технической диагностики, которые подтвердили высокую эффективность ультразвукового контроля для выявления скрытых дефектов и неисправностей. Особое внимание уделено авиационной отрасли, где своевременное обнаружение повреждений напрямую связано с безопасностью полётов.

Представлены результаты анализа характеристик существующих технических решений (FLIR Si124, Crysound Cry 2624M, UE-Systems ULTRAPROBE 9000) и нормативной базы по акустическим измерениям, которые позволили сформировать технические требования к перспективному прибору для проведения научных исследований по диагностике авиационного оборудования.

В качестве сенсорной базы был выбран недорогой MEMS-микрофон SPU0410LR5H-QB-7 (Knowles, серия SiSonic™), доступный в Казахстане. Он обладает широким частотным диапазоном (100 Гц – 80 кГц), высокой чувствительностью и низким энергопотреблением.

Благодарности.

Авторы выражают искреннюю благодарность АО «Авиаремонтный завод № 405» и главному инженеру предприятия Кариеву Дильшоду Хошимовичу за оказанные консультации и активное участие в обсуждении возможного прибора, что существенно способствовало уточнению направления исследования.

Список литературы

1. Абдиматова, Т. Д. (2025). Ультразвуковой мониторинг биологических и техногенных процессов. В VIII Международный научно-технический форум СТНО-2025. Сборник трудов (Т. 6, с. 269).
2. Bardis, K., Avdelidis, N. P., Ibarra-Castanedo, C., Maldague, C. P. V., & Fernandes, E. (2025). Advanced diagnostics of aircraft structures using ultrasound, thermography, eddy current, and ML. Applied Sciences. MDPI. <https://www.mdpi.com>
3. Berri, P. C., Matteo, D. L., Dalla Vedova, & Mainini, L. (2020). Computational framework for real-time diagnostics and prognostics of aircraft actuation systems. arXiv preprint. <https://arxiv.org>
4. Вибрационная диагностика машин и оборудования: Учебное пособие. (2015). Красноярск: Красноярский государственный технический университет.
5. FLIR Systems. (2025, 1 августа). FLIR Si2 (Industrial Acoustic Imaging Camera). <https://www.flir.com/products/si2-pro>
6. Global Test Supply. (2025, 20 июня). Официальный сайт. <https://www.globaltestsupply.com>
7. Голямина, И. П. (1979). Ультразвук. Маленькая энциклопедия. Москва: Советская энциклопедия.
8. ISO 29821-2:2016. (2016). Condition monitoring and diagnostics of machines — Ultrasonic techniques — Part 2: Procedures to determine and assess measurement results. Geneva: ISO.
9. ISO 18405:2017. (2017). Underwater acoustics — Terminology. Geneva: ISO.

10. Laurijssen, D., Daems, W., & Steckel, J. (2024, February). HiRIS: An airborne sonar sensor with a 1024 channel microphone array. arXiv preprint. <https://arxiv.org/abs/2402.12345>
11. Lu, Y. (1992). Real-time weld defect detection using ultrasonic methods (Doctoral dissertation). Brunel University, School of Engineering and Design.
12. Mast, T. D., Pucke, A., & Iskander, M. F. (2009). Passive imaging of cavitation acoustic emissions with ultrasound arrays. *AIP Conference Proceedings*, 1092(1), 126–130. DOI: 10.1063/1.3085725
13. Özlem, U., Furkan, E., & Elif, E. (2024). Non-destructive testing methods commonly used in aviation. *International Journal of Aeronautics and Astronautics*, 5(1), 10–22.
14. Сдвижкова, Е. А., Головкин, Ю. Н., Нурпеисова, Т. Б., Бекеткызы, М. Б., Имансакипова, Б. Б., Айтказинова, Ш. К., Спицын, А. А., & Васильев, И. В. (2024). Способ определения направления на источник звука (Патент № 37080, Республика Казахстан). Некоммерческое акционерное общество «Казахский национальный исследовательский технический университет имени К. И. Сатпаева». <https://gosreestr.kazpatent.kz/Invention/Details?docNumber=381657>
15. Samaitis, V., Jasiūnienė, E., Packo, P., & Smagulova, D. (2021). Ultrasonic methods. In M. G. R. Sause & E. Jasiūnienė (Eds.), *Structural Health Monitoring and Damage Detection Systems in Aerospace* (pp. 101–124). Cham: Springer. DOI: 10.1007/978-3-030-72192-3_5
16. Shetu, A. M. Sh. (2025). A review of nondestructive testing methods for aerospace composite materials. ResearchGate. <https://www.researchgate.net>
17. Soeta, Y., Takahashi, Y., Ito, N., & Hasegawa, A. (2020). Application of simple visualization system for analysing direction of sound sources by 3D microphones. *INTER-NOISE and NOISE-CON Congress and Conference Proceedings*, 261(5), 1234–1243. Institute of Noise Control Engineering.
18. Therre, S., Bost, W., Hewener, H., Tretbar, S., & Fournelle, M. (2021). Passive acoustic mapping for ultrasound therapy monitoring. *Current Directions in Biomedical Engineering*, 7(2), 437–440. DOI: 10.1515/cdbme-2021-1095
19. Tran, V. T., & Yang, B.-S. (2009). Machine fault diagnosis and prognosis: The state of the art. *International Journal of Fluid Machinery and Systems*, 2(1), 61–71. https://www.jstage.jst.go.jp/article/ijfms/2/1/2_1_61/article/-char/ja
20. UE Systems. (2025, 13 августа). Ultraprobe 9000. <https://www.uesystems.com/product/ultraprobe-9000/>

References

1. Abdimatova, T. D. (2025). Ultrasonic monitoring of biological and technogenic processes. In VIII International Scientific and Technical Forum STNO-2025. Proceedings (Vol. 6, p. 269).
2. Bardis, K., Avdelidis, N. P., Ibarra-Castaneda, C., Maldague, C. P. V., & Fernandes, E. (2025). Advanced diagnostics of aircraft structures using ultrasound, thermography, eddy current, and ML. *Applied Sciences*. MDPI. <https://www.mdpi.com>
3. Berri, P. C., Matteo, D. L., Dalla Vedova, & Mainini, L. (2020). Computational framework for real-time diagnostics and prognostics of aircraft actuation systems. arXiv preprint. <https://arxiv.org>
4. *Vibration diagnostics of machines and equipment: Textbook*. (2015). Krasnoyarsk: Krasnoyarsk State Technical University.
5. FLIR Systems. (2025, August 1). FLIR Si2 (Industrial Acoustic Imaging Camera). <https://www.flir.com/products/si2-pro>
6. Global Test Supply. (2025, June 20). Official website. <https://www.globaltestsupply.com>
7. Golyamina, I. P. (1979). *Ultrasound*. Small encyclopedia. Moscow: Soviet Encyclopedia.
8. ISO 29821-2:2016. (2016). Condition monitoring and diagnostics of machines — Ultrasonic techniques — Part 2: Procedures to determine and assess measurement results. Geneva: ISO.

9. ISO 18405:2017. (2017). Underwater acoustics — Terminology. Geneva: ISO.
10. Laurijssen, D., Daems, W., & Steckel, J. (2024, February). HiRIS: An airborne sonar sensor with a 1024 channel microphone array. arXiv preprint. <https://arxiv.org/abs/2402.12345>
11. Lu, Y. (1992). Real-time weld defect detection using ultrasonic methods (Doctoral dissertation). Brunel University, School of Engineering and Design.
12. Mast, T. D., Pucke, A., & Iskander, M. F. (2009). Passive imaging of cavitation acoustic emissions with ultrasound arrays. AIP Conference Proceedings, 1092(1), 126–130. DOI: 10.1063/1.3085725
13. Özlem, U., Furkan, E., & Elif, E. (2024). Non-destructive testing methods commonly used in aviation. International Journal of Aeronautics and Astronautics, 5(1), 10–22.
14. Sdvizhkova, E. A., Golovko, Y. N., Nurpeisova, T. B., Beketkyzy, M. B., Imansakipova, B. B., Aitkazinova, Sh. K., Spitsyn, A. A., & Vasiliev, I. V. (2024). Method for determining the direction to a sound source (Patent No. 37080, Republic of Kazakhstan). Non-commercial Joint Stock Company “Satbayev Kazakh National Research Technical University”. <https://gosreestr.kazpatent.kz/Invention/Details?docNumber=381657>
15. Samaitis, V., Jasiūnienė, E., Packo, P., & Smagulova, D. (2021). Ultrasonic methods. In M. G. R. Sause & E. Jasiūnienė (Eds.), Structural Health Monitoring and Damage Detection Systems in Aerospace (pp. 101–124). Cham: Springer. DOI: 10.1007/978-3-030-72192-3_5
16. Shetu, A. M. Sh. (2025). A review of nondestructive testing methods for aerospace composite materials. ResearchGate. <https://www.researchgate.net>
17. Soeta, Y., Takahashi, Y., Ito, N., & Hasegawa, A. (2020). Application of simple visualization system for analysing direction of sound sources by 3D microphones. INTER-NOISE and NOISE-CON Congress and Conference Proceedings, 261(5), 1234–1243. Institute of Noise Control Engineering.
18. Therre, S., Bost, W., Hewener, H., Tretbar, S., & Fournelle, M. (2021). Passive acoustic mapping for ultrasound therapy monitoring. Current Directions in Biomedical Engineering, 7(2), 437–440. DOI: 10.1515/cdbme-2021-1095
19. Tran, V. T., & Yang, B.-S. (2009). Machine fault diagnosis and prognosis: The state of the art. International Journal of Fluid Machinery and Systems, 2(1), 61–71. https://www.jstage.jst.go.jp/article/ijfms/2/1/2_1_61/article/-char/ja
20. UE Systems. (2025, August 13). Ultraprobe 9000. <https://www.uesystems.com/product/ultraprobe-9000/>

МЕХАНИЗМДЕРДІ УЛЬТРАДЫБЫСТЫҚ ДИАГНОСТИКАЛАУҒА АРНАЛҒАН БОЛАШАҚ ҚҰРЫЛҒЫНЫҢ СИПАТТАМА ТАЛАПТАРЫ

Аңдатпа. Мақалада машиналар мен механизмдерді ультрадыбыстық диагностика әдістерін қолдануды реттейтін нормативтік құжаттарды талдау нәтижелері ұсынылған, сондай-ақ оларды дыбыс жиілігі саласындағы қолданыстағы стандарттармен салыстыру жүргізілген. Мұндай тәсіл қолдану салаларындағы айырмашылықтарды анықтауға және жаңа диагностикалық аспаптарды әзірлеу кезінде қолданыстағы нормаларды практикалық тұрғыдан пайдалану мүмкіндіктерін белгілеуге мүмкіндік берді.

Арнайы назар қазіргі уақытта сатып алуға болатын ультрадыбыстық жиіліктегі өлшеу аспаптарына аударылды. Көптеген аспаптардың функционалдық мүмкіндіктері шектеулі әрі құны жоғары екені анықталды. Мәселен, жекелеген құрылғылар ультрадыбыстық сигналдарды тіркеп, олардың көзінің бағытын көрсете алады, алайда визуализация тек локализацияланған нүктені бейнелеумен шектеледі. Бұл өз кезегінде сигналдың физикалық параметрлерін және оның ортадағы таралу динамикасын жазып алуға мүмкіндік бермейді. Мұндай шектеулер кешенді диагностиканың мүмкіндіктерін айтарлықтай тарылтады.

Мақаланың негізгі мақсаты – механизмдерді ультрадыбыстық диагностикалауға арналған болашағы бар аспаптың сипаттамаларына қойылатын талаптарды қалыптастыру. Мұндай аспап жиілік параметрлерін тіркеу және ультрадыбыстық өрісті кеңістікте визуализациялау функцияларын біріктіруі тиіс.

Көрсетілгендей, қазіргі аспаптар тек сигнал көзін іздеуге бағытталған. Жаңа буындағы аспаптарды жасау қажеттілігі негізделді. Олар ультрадыбыстық өрісті кеңістікте бейнелеуге және машиналар мен механизмдерді неғұрлым толық диагностикалауға, оның ішінде жасырын ақаулар мен ықтимал істен шығуларды ерте анықтауға мүмкіндік береді. Авиация саласы үшін бұл талаптарды орындау ерекше маңызды, себебі ол тікелей ұшу қауіпсіздігінің жоғары деңгейін қамтамасыз етумен байланысты.

Түйін сөздер: ультрадыбыстық диагностика, акустикалық, бұзбайтын бақылау (NDT), авиациялық қауіпсіздік, MEMS-микрофондар, техникалық диагностика, акустикалық визуализация, аспаптарға қойылатын талаптар, механизмдердің сенімділігі.

REQUIREMENTS FOR THE CHARACTERISTICS OF A PROSPECTIVE DEVICE FOR ULTRASONIC DIAGNOSTICS OF MECHANISMS

Abstract. *The article presents the results of an analysis of regulatory documents governing the application of ultrasonic diagnostic methods for machines and mechanisms, as well as a comparison with current standards in the field of acoustic frequencies. This approach made it possible to identify differences between areas of application and to determine the possibilities of practical use of existing standards in the development of new diagnostic devices.*

Special attention is given to the review of ultrasonic frequency measuring instruments currently available on the market. It was found that most of these devices have limited functional capabilities and a high cost. For example, some instruments are capable of detecting ultrasonic signals and indicating the direction of their source; however, visualization is limited to displaying a localized point, which does not allow the recording of physical parameters of the signal or the dynamics of its propagation in the medium. These limitations significantly reduce the potential for comprehensive diagnostics.

The main objective of the article is to establish requirements for the characteristics of a next-generation device for ultrasonic diagnostics of mechanisms, which should combine the functions of recording frequency parameters and spatial visualization of the ultrasonic field.

It is shown that existing devices are focused only on detecting the signal source. The need for developing new-generation instruments is substantiated. Such instruments would enable the visualization of the ultrasonic field in space and ensure more comprehensive diagnostics of machines and mechanisms, including early detection of hidden defects and potential failures. For the aviation industry, meeting these requirements is of particular importance, as it is directly related to ensuring a high level of flight safety.

Keywords: *ultrasonic diagnostics, nondestructive testing (NDT), aviation safety, MEMS microphones, technical diagnostics, acoustic visualization, instrument requirements, mechanism reliability.*

Сведение об авторах

Абдиматова Толкын Досалықызы	Докторант «Академии гражданской авиации», г. Алматы, Казахстан E-mail: t.abdimatova@agakaz.kz
Васильев Иван Вениаминович	Канд. физ.-мат. наук., ассоциированный профессор Академии Гражданской Авиации, г. Алматы, Казахстан, e-mail: iv@granit.kz

Авторлар туралы мәлімет

Әбдімәтәвә Тәлқын Досалықызы	«Азаматтық авиация академиясының» докторанты, Алматы қ., Қазақстан E-mail: t.abdimatova@agakaz.kz
Васильев Иван Вениаминович	PhD (физика-математика), Азаматтық Авиация Академиясының қауымдастырылған профессоры, Алматы қ., Қазақстан e-mail: iv@granit.kz

Information about the authors

Abdimatova Tolkyun Dosalykyzy	Doctoral Student, Civil Aviation Academy, Almaty, Republic of Kazakhstan E-mail: t.abdimatova@agakaz.kz
Vassilyev Ivan Veniaminovich	PhD (phys.-math.), Associate professor of Civil Aviation Academy, Almaty, Kazakhstan, e-mail: iv@granit.kz



UDC 656.7:331.45

IRSTI 73.37.75

https://doi.org/10.53364/24138614_2025_38_3_4

N. Levchenko^{1*}, B. Bakirov²

¹Technical University of Berlin, Berlin, Germany

²Red River college, Winnipeg, Canada

E-mail: levchenko65@gmail.com*

CREATION OF A "SMART" OCCUPATIONAL SAFETY MANAGEMENT SYSTEM IN CIVIL AVIATION IN THE CONTEXT OF THE "SOCIETY 5.0" CONCEPT

Abstract. *This article examines current challenges in occupational safety and health in civil aviation in the Republic of Kazakhstan, including the growth of traffic volumes, increasing number of flights, and increasing complexity of technological processes. This demonstrates that traditional approaches that focus on monitoring violations and mitigating the consequences of incidents are limited in effectiveness and do not systematically prevent industrial risks. This article substantiates the need to transition to a "smart" occupational safety and health management system based on digitalization and intellectualization, the use of predictive analytics, automated monitoring tools, and the creation of a unified database for risk factor analysis. The proposed concept enables a shift from reactive to proactive occupational safety management, which reduces injury rates, improves the reliability of enterprise operations, and optimizes labor-resource utilization. It is emphasized that the implementation of a "smart" occupational safety and health system that complies with international standards will enhance the sustainability and competitiveness of Kazakhstan's aviation industry and will ensure its adaptation to global trends in technological development and increasing workload.*

Keywords: *occupational safety, civil aviation, digitalization, predictive analytics, intelligent monitoring, society 5.0.*

Introduction.

Civil aviation is one of the most dynamic and high-tech sectors in the global economy, where occupational health and safety issues play a key role. The high intensity of aviation processes, complexity of technical systems, and high cost of error necessitate special attention to the development of effective occupational health and safety management mechanisms. Violations in this area can have consequences not only for the health and lives of workers but also for the safety of passengers, the environment, and the sustainability of the transportation system as a whole. Therefore, ensuring safe and healthy working conditions in civil aviation has become an integral part of the industry's strategic development [1]. Moreover, with the implementation of the "Society 5.0" concept, approaches to occupational health and safety management have changed significantly. Traditional control methods, based primarily on recording violations and consequences, provide proactive and predictive systems that utilize big data, artificial intelligence, and digital twins, enabling the real-time monitoring of worker health and the production

environment, predicting the likelihood of accidents, and developing targeted preventive measures [2].

In particular, the use of predictive analytics based on big data makes it possible to forecast the risks of occupational injuries; the implementation of intelligent monitoring systems ensures monitoring of the health and performance of personnel, promotes a more rational distribution of working time, reduces fatigue, and the automation of routine processes reduces the influence of human factors and the likelihood of errors [3]. Tools, such as wearable devices and cyber-physical systems, create the possibility of developing individualized models of worker health protection, taking into account their physiological characteristics and professional workload. This not only increases the sustainability of the functioning of aviation enterprises but also promotes the development of a safety culture, where each employee is considered an active participant in the system and not just an object of observation [4]. Moreover, electronic consultations and the introduction of telemedicine into practice are becoming accessible methods that provide prompt consultations to enterprise employees on-site. These advanced technologies allow enterprises to maximize employee engagement in the occupational health and safety system and reduce occupational diseases and injuries [5]. The integrated occupational safety system created in this way will allow airlines not only to comply with ICAO requirements, but also to fully adhere to the principles of "preventive safety," which emphasizes prevention rather than remediation.

Thus, the digitalization and intellectualization of the occupational health and safety management system within the framework of the development of the "Society 5.0" concept open up new prospects for improving occupational health and safety mechanisms in civil aviation, transforming it from a supporting function into a strategic factor in increasing the efficiency, competitiveness, and sustainability of the entire industry.

The goal of this article is to develop conceptual principles and practical recommendations for creating a "smart" occupational safety and health management system in civil aviation, integrated with digital technologies and consistent with the principles of the "Society 5.0" concept. To achieve this goal, the following objectives were formulated: to explore an industry-specific occupational safety and health management model in civil aviation in the Republic of Kazakhstan, as one of the most rapidly developing industries, and to explore ways to improve the effectiveness of occupational safety and health management in civil aviation enterprises.

Literature review.

An analysis of literary sources indicates that, in recent years, the problem of ensuring safe and healthy working conditions in civil aviation has acquired particular significance. This is due not only to the growth in transportation volumes and the increasing complexity of technical processes but also to the need to meet new requirements of sustainable development, where people and their safety occupy a central place [6]. Moreover, as Karakavuz and Gerede (2024) emphasize, ground-handling companies have the highest potential for industrial accidents in the air transportation sector, which leads to a significant increase in compensation costs for both companies and the state [7]. Therefore, the successful implementation of occupational health and safety management systems (OHSMS) plays an important role in the development of a safety culture among civil aviation personnel, ensuring the preservation of airline employees' health and consequently increasing their efficiency and productivity [8]. Consequently, improving the success of occupational health and safety management systems is of considerable importance in the organization of aviation personnel [9].

Thus, the analysis of scientific publications demonstrates significant progress towards digital transformation and implementation of intelligent technologies in occupational safety management. The combination of these approaches should be recognized as key development vectors that enable the creation of smart, adaptive, and transparent management systems, which is particularly relevant for highly sensitive industries, including civil aviation. Their symbiosis opens new horizons in the development of a modern safety concept, focusing on risk prediction, proactive

measures, and continuous process optimization, which, in turn, plays a decisive role in ensuring the operational reliability and long-term sustainability of the industry.

Material and Methods.

The methodology chosen by the authors ensures the scientific rigour and validity of all stages of the study, from conceptualisation to the assessment of the practical potential of innovative solutions in the field of labour protection. The following materials were used for this study: data from the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan; the regulatory framework of the international (in particular, ICAO, ITF regulations, etc.) and national levels (in particular, legislative and regulatory acts of the Republic of Kazakhstan in the field of civil aviation), airline reports, etc.

Results and their discussion.

Over the past decade, the Republic of Kazakhstan has been actively implementing reforms in the field of occupational safety and health aimed at transitioning to a risk-based model of occupational safety and health management. Over the years, international occupational safety standards have been ratified, labor and social legislation have been revised, and state control over compliance with safety requirements has been strengthened. Despite these measures, the expected significant improvement in working conditions has not been achieved. The main reasons for the persistent problematic situation are limited statistical data for certain types of economic activity, insufficiently informative monitoring of harmful working conditions, which does not ensure the systematic accumulation of information for the analysis and identification of cause-and-effect relationships between injuries and occupational diseases, and the absence of a clearly defined algorithm for assessing the effectiveness of occupational safety and health management models, both at the individual industry level and on a national scale [10].

To find effective solutions and develop recommendations for improving the occupational safety system, a study was conducted to examine the state of occupational safety and working conditions for personnel in civil aviation, which is one of the most dynamically developing sectors in the country.

The occupational safety management system in Kazakhstan's civil aviation was chosen as the focus of this study because Kazakhstan's air passenger and cargo transportation market is the most stable and fastest growing in the Central Asian region. According to the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan, 14.7 million passengers were transported by air in the country from January to December 2024 (Table 1), an increase of 10.6% from January to December 2023. Passenger turnover also increases accordingly. In 2024, it amounted to 28.3 billion passenger kilometers, 9.3% higher than the previous year's figure [11].

Table 1 – Dynamics of performance indicators of civil aviation in Kazakhstan during 2015-2024 [11]

Year s	Income, mln. tenge			Passenger transportation, thoun. pepole	Passenger turnover, mil. pass. kilom.	Transported cargo, baggage, and over- the-counter baggage, thoun. mil. tonns	Freight turnover, mil. tonn per kilomete r
	Total	Included					
		baggage	passenge rs				
2015	179556,6	4420,1	175136,5	5924,9	11138,6	17,0	42,44
2016	233590,9	5214,9	228376,0	6006,12	11073,0	18,1	42,99
2017	295584,6	6294,7	289289,9	7352,17	14384,2	22,4	53,33

2018	343284,3	7287,0	335997,3	7858,53	16176,7	29,1	55,67
2019	403018,2	8776,2	394242,0	8614,79	16940,3	25,1	54,2
2020	187696,3	11623,0	176073,3	5489,71	8335,0	24,2	56,2
2021	366308,9	17036,4	349272,5	9434,05	14815,7	34,0	81,68
2022	602049,6	13055,7	588993,9	10993,6	20109,3	24,5	54,44
2023	745128,6	13219,6	731909,0	13266,6	25898,5	23,8	53,7
2024	833535,6	15501,7	818033,9	14678,7	28275,7	27,88	65,7

According to the Civil Aviation Committee of the Republic of Kazakhstan, from 2015 to 2024, Kazakhstan's civil aviation demonstrated steady growth in key indicators: revenue, passenger traffic, passenger turnover, and cargo volume. The growth in the number of flights and volume of passenger and cargo operations is accompanied by the increasing complexity of technological processes and the increased intensity of employee work, making them more vulnerable to harmful and adverse factors. Under these conditions, the industry's effectiveness depends largely on a systematic approach to occupational safety, including monitoring, prevention, and adaptation of organizational and technical measures to the actual workload of workers.

To formulate informed management decisions and evaluate the effectiveness of the measures taken, it is necessary to rely on quantitative data from personnel engaged in harmful and hazardous working conditions. The analysis of such statistics allows us to identify trends in changes in the workforce, assess the impact of increased activity intensity on professional risks, and develop targeted measures to reduce injuries and occupational diseases. Therefore, we turn to the data in Table 2, which reflects the number of civil aviation workers in Kazakhstan employed under harmful and hazardous working conditions in the period 2015–2024, with details on employee categories, work schedules, and the nature of the impact of unfavorable factors.

Table 2 – Number of air transport workers employed in harmful and hazardous working conditions during 2015-2024, people [12]

Years	Average headcount of employees		Of these, those employed in harmful and hazardous working conditions				
	total	including workers	of which are employed on the	employed in conditions that do not meet sanitary and hygienic requirements	of which are working under the influence		
					increased levels of noise and vibration	increased dustiness and gas contamination of the air in the working area, exceeding the	unfavorable temperature conditions
2015	6756	3399	2052	712	723	31	74
2016	7054	3011	3043	1355	871	38	-
2017	7138	3393	3745	1476	989	47	95
2018	7385	3081	3373	2451	1379	59	-
2019	8011	3657	3945	3835	2871	51	70
2020	7480	2909	4646	2144	2080	31	98
2021	7748	2634	4285	2169	2136	34	98
2022	8557	3371	4723	3454	1978	33	93
2023	10346	2265	4086	1762	534	37	1533
2024	10946	2481	2638	2931	1182	6	-

Based on the data in Table 2, over the analyzed period, the number of air transport employees in Kazakhstan increased from 6,756 to 10,946, reflecting the industry's active development. However, along with employment growth, there were significant changes in the structure of the working conditions. For example, the number of employees employed in hazardous and dangerous conditions has decreased from 3,399 in 2015 to 2,481 in 2024, representing a decrease from more than half of the workforce (50.3%) to less than a quarter (22.7%). This trend indicates a gradual improvement in working conditions and more effective implementation of occupational safety measures despite the overall increase in transportation volumes and production workload.

The dynamics of the types of harmful factors show heterogeneity; in 2019, the number of workers exposed to noise, vibration, and dust peaked (up to 2,871 people); by 2024, these figures had decreased significantly, likely due to the renewal of the equipment fleet and improved sanitary and hygienic conditions. At the same time, in 2023, the number of workers working in unfavorable temperature conditions increased sharply (1,533 people), indicating the persistence of certain problem areas requiring additional protective measures.

An analysis of specific hazardous factors shows that the quantitative increase in the number of workers in the industry is accompanied by qualitative changes in the nature of the occupational risks. While the overall share of those employed under hazardous conditions decreases, the impact of certain high-intensity factors remains. This confirms that the development of civil aviation in Kazakhstan is accompanied not only by an increase in the volume of services but also by the need for a comprehensive improvement in the occupational safety system, from equipment modernization and the introduction of engineering safety measures to strengthen sanitary and hygienic standards and adapt work processes to the increasing workload.

However, an analysis of the number of workers engaged in hazardous and harmful conditions allows us not only to assess the scale of the impact of adverse factors on personnel but also to trace a direct link between the workload and the economic consequences for aviation enterprises. The increase in the number of employees working under conditions of increased noise, vibration, dust, or unfavorable temperatures, as well as the increase in the volume of operations performed, inevitably leads to the need for compensation and additional benefits. These payments are an important element of social protection for workers and simultaneously generate significant material costs for companies, reflecting the economic side of ensuring safe working conditions (Table 3).

Table 3 – Material costs for payment of compensation to air transport workers for work in harmful and unfavorable working conditions during 2015-2024, thousand tenge [13]

Years	Material consequences for the year, million tenge	Of these				
		additional vacations	shortened working hours	therapeutic and prophylactic nutrition	milk and equivalent food products	additional payments for harmful and other unfavorable working conditions
2015	864,8217	819,0372	-	-	2,2995	40,3910
2016	868,6869	815,7733	-	2,9711		
2017	679,7064	635,6126	-	-	-	-
2018	660,7980	660,7980	-	-	-	-
2019	875,3117	783,2996	-	3,1160	2,7957	86,1004
2020	792,2340	665,4046	-	-	1,7889	125,0399
2021	1175,5821	1108,2964	-	-	1,8277	65,4480
2022	1463,4418	1377,8559	-	0,0340	2,3304	81,2435

2023	1185,7963	1077,447 0	-	36,0	2,8301	105,4831
2024	2156,3163	1918,405 4	1188,6	-	5,2411	130,0061

From 2015 to 2024, as shown in Table 3, material costs for compensation to air transport workers showed an upward trend, from 864,800 tenge in 2015 to 2,156,300 tenge in 2024. The bulk of these costs are attributed to the provision of additional vacations, whose share of total compensation consistently exceeds 80–90%, reflecting legislative and social guarantees for employees.

The dynamics of payments for harmful and unfavorable working conditions (additional payments, therapeutic and preventive nutrition, milk, and equivalent products) vary because of the growing number of employees working in harmful conditions and changes in the compensation structure. For example, since 2019, there has been a significant increase in additional payments for work in unfavorable conditions, coinciding with increased exposure to occupational risks, including noise, vibration, and unfavorable temperatures. In 2024, a significant expense item for shortened working hours was recorded for the first time, indicating the need to implement additional measures to protect and improve working conditions.

Thus, we conclude that there is a certain relationship between working condition indicators and the costs of airlines providing guarantees stipulated by the Labor Code of the Republic of Kazakhstan. The degree of this relationship can be determined using key occupational safety indicators, namely, occupational diseases and injuries (Table 4).

Table 4 – Occupational safety indicators for civil aviation personnel of the Republic of Kazakhstan for 2015-2024

Years	Number of victims, people		Loss of Life Injury Frequency Rate (TIFR)	Fatal Injury Frequency Rate (FIFR)	Loss of working time, days		Trauma Injury Severity Rate (LTISR)	Overall injury rate	Lost Time Injury Rate (LTIFR)
	total (LTI)	including fatalities			total	including due to accidents			
2015	281	21	41,5927	3,108348	5164	5164	18,3772	2,2632	23,7753
2016	287	16	40,6861	2,268217	5618	5618	19,5749	2,0784	23,2571
2017	303	20	42,4489	2,801905	5535	1479	18,2673	2,3242	24,2648
2018	318	22	43,0603	2,979012	5948	5453	17,1478	2,5111	24,614
2019	312	17	38,9465	2,122082	6788	6386	20,4679	1,9028	22,2627
2020	455	17	60,8289	2,272727	4756	4360	9,58241	6,3479	25,5621
2021	472	17	60,9189	2,194115	5853	5731	12,1419	5,0172	18,2635
2022	127	8	14,8417	0,934907	4933	4843	38,1338	0,3891	8,48385
2023	161	17	15,1293	0,958394	4759	6843	19,1583	0,3389	12,6284
2024	175	15	14,7827	0,933442	4721	7278	17,8672	0,3401	11,1563

The occupational safety indicators for civil aviation personnel presented in Table 4 demonstrate a clear correlation with the scale of industry operations. As the number of workers and traffic volumes increased, fluctuations in the number of injured persons were observed: peak values were recorded from 2020 to 2021 (455–472 people), coinciding with increased workloads on personnel, an increase in the number of flights and passenger and cargo flows, and complications associated with the COVID-19 pandemic. During these years, the Tier 1 Injury Frequency Rate (TIFR) reached its maximum values of approximately 60.9, and the Lengthy

Injury Severity Rates (LTISR) also increased, indicating increased intensity and risk of work activities.

Since 2022, a significant reduction in all key injury indicators has been observed: the number of injuries has decreased to 127–175, the injury frequency rate has fallen to 14.8–15.1, and the severity rate and LTIFR have also decreased, demonstrating the positive impact of implementing occupational safety systems, upgrading equipment, improving workflow organization, and reducing exposure to hazardous and harmful factors. Moreover, the fatal injury rate remained relatively low throughout the study period, indicating the sustainability of measures to prevent the most serious incidents.

Thus, the analysis shows that the growth in personnel and transportation volumes directly impacts operational risks; increased workload and scale of operations lead to an increase in the frequency and severity of injuries, but systematic improvements in occupational safety can reduce these risks and ensure safe working conditions. The dynamics in recent years confirm the effectiveness of accident prevention measures and the need to further develop worker protection mechanisms as the volume of aviation services increases.

However, in the context of digitalization and intellectualization, implemented within the framework of the "Society 5.0" concept, it is becoming more practical to implement a "smart" occupational health and safety management system that combines automated data collection and analysis, predictive analytics, wearable sensors, digital twins of workers, and integration with corporate information systems of airlines. Such a system will enable the creation of a complete digital model of the production environment and personnel, where each employee and technological process is monitored in real time.

Using wearable sensors and medical devices, the system records workers' physiological indicators—fatigue level, cardiovascular activity, body temperature, stress responses, and parameters of exposure to external factors (noise, vibration, temperature, and dust). The data were automatically analyzed using artificial intelligence algorithms, enabling the identification of potential risks before incidents, predicting the likelihood of injuries and occupational diseases, and identifying the most vulnerable areas of production processes. Digital twins of workers and production facilities enable the simulation of various work scenarios, assessing the impact of changes in workload, shift patterns, operating modes, and weather conditions as well as optimizing work schedules, task allocation, and preventative measures. Integration with analytical platforms allows management to obtain visual reports, forecasts, and recommendations, fostering a proactive rather than reactive approach to safety.

Implementing such a system in civil aviation enterprises will not only reduce the number of accidents and occupational illnesses but also optimize compensation costs, improve labor quality, and enhance the overall performance of aviation personnel. Furthermore, the smart system will foster a safety culture in which every employee is involved in managing their own health and safety, while the enterprise will gain a tool for sustainable development and compliance with international ICAO standards.

Conclusion.

The results of the study confirm that the rapid growth of air traffic volumes, the increasing number of flights, and the increasing complexity of technological processes in civil aviation significantly increase the workload of personnel and simultaneously increase the demand for safe working conditions. In such conditions, occupational safety and health (OSH) is becoming a critical element of the industry's sustainability, as any error or accident not only entails material and social consequences, but also undermines trust in the air transportation system at the national and international levels. Traditional approaches, focused primarily on monitoring violations and mitigating the consequences of incidents, demonstrate limited effectiveness as they fail to fully identify and prevent the root causes of operational risks. This is especially evident in the rapidly evolving aviation industry, where timely and predictive decision making is crucial.

In this context, the transition to a "smart" OSH management system is particularly urgent. This involves the digitalization and intellectualization of processes, integration of automated monitoring tools, use of predictive analytics, and development of a unified database for systematic risk analysis. Unlike traditional methods, this system not only records violations, but also proactively identifies potentially hazardous situations, predicts the likelihood of accidents and occupational diseases, and plans preventative measures based on the specifics of technological processes and the actual workload of workers. Implementing this approach enables a transition from reactive to proactive occupational safety management, which significantly reduces injury rates, optimizes labor resource allocation, reduces the economic costs associated with compensation and downtime, and strengthens employee confidence in the safety system.

Furthermore, the implementation of a "smart" occupational safety management system aligns with modern international trends and promotes the harmonization of national practices with global standards. This is particularly important for the aviation industry, which is deeply integrated into the global transportation system. This will not only improve the reliability and sustainability of airline operations, but also strengthen Kazakhstan's competitive position internationally.

Thus, the development of an intelligent model for occupational health and safety management is a strategic direction that ensures long-term operational reliability, increased personnel safety, and sustainable development of the industry in the context of increasing work intensity and technological modernization.

References

1. Minoretti, P., Serrano, M., Riera, M., Saez, A., & Martin, A. (2024). Occupational Health Challenges for Aviation Workers Amid the Changing Climate: A Narrative Review. *Cureus*, 16(3), e55935. <https://doi.org/10.7759/cureus.55935>.
2. Golub, S., & Tolbatov, D. (2023). Method of synthesis of a multilayer model of a monitoring software agent. *Mathematical machines and systems*, 1, pp. 101-111. <https://doi.org/10.34121/1028-9763-2023-1-101-111>.
3. Patel, V., Chesmore, A., Legner, C., & Pandey, S. (2021). Trends in Workplace Wearable Technologies and Connected-Worker Solutions for Next-Generation Occupational Safety, Health, and Productivity. *Advanced Intelligent Systems*, 4(1), 2100099. <https://doi.org/10.1002/aisy.202100099>.
4. Chen, H., Mao, Y., Xu, Y., & Wang, R. (2023). The Impact of Wearable Devices on the Construction Safety of Building Workers: A Systematic Review. *Sustainability*, 15(14), 11165. <https://doi.org/10.3390/su151411165>.
5. Tang, Y., Liang, H., & Zhan, J. (2024). The application of metaverse in occupational health. *Frontiers in Public Health*, 12, 1396878. <https://doi.org/10.3389/fpubh.2024.1396878>.
6. Batuwangala, E., Kistan, T., Gardi, A., & Sabatini, R. (2018). Certification challenges for next-generation avionics and air traffic management systems. *IEEE Aerospace and Electronic Systems Magazine*, 33(9), pp. 44-53. <https://doi.org/10.1109/MAES.2018.160164>.
7. Karakavuz, H., & Gerede, E. Evaluation of success factors of occupational health and safety management systems with the analytical hierarchy process: the case of ground handling companies in Turkey. *International Journal of Occupational Safety and Ergonomics*, 31(1), pp. 99-109. <https://doi.org/10.1080/10803548.2024.2410624>.
8. Kunodzia, R., Bikitsha, L., & Haldenwang, R. (2024). Perceived Factors Affecting the Implementation of Occupational Health and Safety Management Systems in the South African Construction Industry. *Safety*, 10(1), 5. <https://doi.org/10.3390/safety10010005>.
9. Trishch, R., Cherniak, O., Zdenek, D., & Petraskevicius. (2024). Assessment of the occupational health and safety management system by qualimetric methods. *Engineering Management in Production and Services*, 16(2), pp. 118-127. <https://doi.org/10.2478/emj-2024-0017>.
10. Koshekov, K., Kalekeyeva, M., Seidakhmetov, B., Kaliyeva, G., Assilbekova, I., & Gozhakhmetova, M. (2024). Monitoring of aviation personnel potential according to the

competence approach. *Eastern-European Journal of Enterprise Technologies*, 3(127), pp. 64–77. <https://doi.org/10.15587/1729-4061.2024.298479>.

11. Transport in the Republic of Kazakhstan (January-December 2024). Available at: <https://stat.gov.kz/en/industries/business-statistics/stat-transport/publications/287590/>.

12. Number and wages of employees in the Republic of Kazakhstan (III quarter of 2024). Available at: <https://stat.gov.kz/en/industries/labor-and-income/stat-wags/publications/186232/>.

АЗАМАТТЫҚ АВИАЦИЯДА «ҚОҒАМ 5.0» КОНЦЕПЦИЯСЫ АЯСЫНДА «ЗИЯТКЕРЛІК» ЕҢБЕК ҚАУІПСІЗДІГІН БАСҚАРУ ЖҮЙЕСІН ҚҰРУ

Аңдатпа. Мақалада Қазақстан Республикасының азаматтық авиация саласында еңбек қауіпсіздігіне қатысты заманауи сын-қатерлер қарастырылады. Олар тасымал көлемінің өсуімен, рейстер санының артуымен және технологиялық үдерістердің күрделенуімен байланысты. Дәстүрлі тәсілдердің бұзушылықтарды бақылауға және оқиғалардың салдарын жоюға бағытталуы шектеулі тиімділікке ие екендігі және өндірістік тәуекелдердің жүйелі алдын алуын қамтамасыз етпейтіні көрсетілген. Цифрландыру мен интеллектуалдандыруға, предиктивті аналитикаға, автоматтандырылған мониторинг құралдарына және тәуекел факторларын талдау үшін бірыңғай деректер базасын құруға негізделген «зияткерлік» еңбек қауіпсіздігін басқару жүйесіне көшу қажеттілігі дәлелденеді. Ұсынылған тұжырымдама еңбек қауіпсіздігін реактивті басқарудан проактивті басқаруға көшуге мүмкіндік береді, бұл жарақаттану деңгейін төмендетуге, кәсіпорындардың сенімді жұмыс істеуін арттыруға және еңбек ресурстарын тиімді пайдалануды қамтамасыз етуге жағдай жасайды. «Зияткерлік» еңбек қауіпсіздігі жүйесін енгізу халықаралық стандарттарға сәйкес келетіні, Қазақстан авиация саласының орнықтылығын және бәсекеге қабілеттілігін арттыратыны, сондай-ақ оны технологиялық дамудың жаһандық үрдістеріне және еңбек қарқындылығының өсуіне бейімдейтіні ерекше атап өтіледі.

Түйін сөздер: еңбек қауіпсіздігі, азаматтық авиация, цифрландыру, болжамды талдау, зияткерлік мониторинг, қоғам 5.0.

СОЗДАНИЕ «УМНОЙ» СИСТЕМЫ УПРАВЛЕНИЯ ОХРАНОЙ ТРУДА В ГРАЖДАНСКОЙ АВИАЦИИ В КОНТЕКСТЕ КОНЦЕПЦИИ «ОБЩЕСТВО 5.0»

Аннотация. В статье рассматриваются современные вызовы в сфере охраны труда в гражданской авиации Республики Казахстан, связанные с ростом объемов перевозок, увеличением числа рейсов и усложнением технологических процессов. Показано, что традиционные подходы, ориентированные на контроль нарушений и устранение последствий происшествий, обладают ограниченной эффективностью и не обеспечивают системного предупреждения производственных рисков. Обосновывается необходимость перехода к «умной» системе управления охраной труда, основанной на цифровизации и интеллектуализации, использовании предиктивной аналитики, автоматизированных средств мониторинга и создании единой базы данных для анализа факторов риска. Предлагаемая концепция позволяет перейти от реактивного к проактивному управлению безопасностью труда, что обеспечит снижение уровня травматизма, повышение надежности функционирования предприятий и оптимизации использования трудовых ресурсов. Подчеркивается, что внедрение «умной» системы охраны труда соответствует международным стандартам, усилит устойчивость и конкурентоспособность авиационной отрасли Казахстана, а также обеспечит ее адаптацию к глобальным тенденциям технологического развития и росту интенсивности работы.

Ключевые слова: безопасность труда, гражданская авиация, цифровизация, прогнозная аналитика, интеллектуальный мониторинг, общество 5.0.

Information about the authors

Levchenko Nataliia	Doctor of science, Professor, Technical University of Berlin, Berlin, Germany, E-mail: levchenko65@gmail.com
Bakirov Baurzhan	PhD, Technology Access Centre for Aerospace and Manufacturing, Red River college, Winnipeg, Canada, E-mail: baurzhan.bakirov@gmail.com

Сведения об авторах

Левченко Наталья	доктор технических наук, профессор, Берлинский технический университет, Берлин, Германия, E-mail: levchenko65@gmail.com
Бакиров Бауржан	PhD, Центр доступа к технологиям для аэрокосмической промышленности, колледж Ред-Ривер, Виннипег, Канада, E-mail: baurzhan.bakirov@gmail.com

Авторлар туралы мәліметтер

Левченко Наталья	техника ғылымдарының докторы, профессор, Берлин техникалық университеті, Берлин, Германия, E-mail: levchenko65@gmail.com
Бакиров Бауржан	PhD, Аэроғарыш өнеркәсібіне арналған технологияларға қол жеткізу орталығы Ред-Ривер колледжі, Виннипег, Канада, E-mail: baurzhan.bakirov@gmail.com



УДК 656.7.08

МРНТИ 73.37.61

https://doi.org/10.53364/24138614_2025_38_3_5

Ш.Серик^{1*}, И.Ж.Асильбекова¹

¹АО “Академия Гражданской Авиации”, г. Алматы, Казахстан

*E-mail: shahon902@mail.ru

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ АВИАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОТКРЫТИИ НОВЫХ РЕЙСОВ АВИАКОМПАНИЙ РЕСПУБЛИКИ КАЗАХСТАН

Аннотация. Статья посвящена исследованию организационных мер по обеспечению авиационной безопасности при открытии новых международных рейсов казахстанских авиакомпаний. В условиях стремительного расширения маршрутной сети Республики Казахстан новые направления сопровождаются возникновением угроз, связанных с особенностями региональной геополитики, террористическими рисками и повышенными требованиями к перевозке пассажиров. Цель исследования заключается в выявлении, систематизации и научном обосновании организационных мер безопасности, а также в оценке их эффективности на примере рейсов казахстанских авиакомпаний Air Astana и SCAT Airlines.

Методология включает анализ международных и национальных нормативных документов (ICAO, EASA, IATA, КГА РК), а также использование методов качественного и количественного анализа рисков. Оценка угроз проведена с применением формулы $R = P \times C$, где P - вероятность реализации события, C - тяжесть последствий. Такой подход позволил сопоставить международные практики и выявить наиболее эффективные меры, включая усиленный предполетный контроль, адаптивные программы подготовки персонала, а также мониторинг поведения пассажиров.

Результаты исследования показывают, что наибольшую эффективность продемонстрировали меры, связанные с комплексным контролем пассажиропотока (93%) и внедрением системного анализа маршрутов (90%). Сравнительный анализ подтвердил важность интеграции международных стандартов и национальных требований в единую систему управления безопасностью.

Научная новизна работы заключается в разработке комплексного подхода к обеспечению авиационной безопасности на новых маршрутах. Практическая значимость состоит в возможности применения результатов авиакомпаниями при планировании международных рейсов для снижения рисков и повышения соответствия международным требованиям.

Ключевые слова: авиационная безопасность, новые маршруты, авиакомпании Казахстана, досмотр, угрозы, меры безопасности.

Введение.

Активное расширение географии полетов казахстанских авиакомпаний за значительное время предъявляет повышенные требования к системе обеспечения авиационной безопасности. Авиакомпания Air Astana по состоянию на 2025 год выполняет

около 94 маршрутов по более чем 30 направлениям, включая множество международных рейсов. Авиакомпания SCAT также осваивает новые зарубежные направления. Открытие новых рейсов, особенно международных - сопровождается появлением некоторых рисков в сфере авиационной безопасности, связанных как с внешними угрозами (терроризм, незаконное вмешательство), так и с внутренними факторами (неправомерное поведение пассажиров).

Международные стандарты требуют, чтобы государства и авиаперевозчики постоянно оценивали уровень угроз в гражданской авиации и корректировали меры безопасности на основе оценки рисков. Для Казахстана, как участника ИКАО, актуальна задача внедрения проактивного и прогностического подхода к обеспечению безопасности полетов на новых маршрутах. Актуальность исследования обусловлена необходимостью выработки эффективных организационных мер, позволяющих предупредить акты незаконного вмешательства и другие инциденты на этапе планирования и выполнения новых рейсов [1-2].

Цель исследования - определить комплекс организационных мер по обеспечению авиационной безопасности при запуске новых маршрутов авиакомпаний Республики Казахстан. Задачи включают анализ международных и национальных требований в области авиационной безопасности, изучение практического опыта казахстанских авиаперевозчиков на примере рейсов Air Astana и SCAT, а также формулирование рекомендаций по совершенствованию мер безопасности.

Материалы и методы исследования.

В данной статье применён комплексный подход, основанный на методах качественного и количественного анализа рисков. Методология исследования включает три последовательных этапа:

На первом этапе производится идентификация потенциальных угроз авиационной безопасности, которые могут возникнуть при открытии нового международного рейса. Идентификация осуществляется с помощью экспертного опроса, анализа отчетов авиационных организаций (ICAO, EASA, IATA), а также на основе данных из официальных документов авиакомпаний и органов авиационной безопасности Казахстана.

Количественная оценка выполняется на основе общепринятой международной методики, рекомендованной ИКАО (ICAO Doc 8973). Уровень риска определяется по следующей формуле:

$$R = P * C,$$

Где R - количественный уровень риска (безразмерный показатель), P - вероятность реализации угрозы (безразмерная величина, шкала от 0 до 1), C - тяжесть последствий реализации угрозы (безразмерная величина, шкала от 1 до 5, где 1 - минимальный ущерб, 5 - максимальный ущерб с катастрофическими последствиями).

Таким образом, минимальное значение риска (0) соответствует ситуации, когда угроза отсутствует, максимальное значение (5) соответствует угрозе с максимальными последствиями и высокой вероятностью реализации.

Для оценки эффективности организационных мер, предложенных и реализованных авиакомпаниями, применяется индекс эффективности (E), рассчитываемый по формуле:

$$E = \frac{N \text{ выявленных угроз}}{N \text{ возможных угроз}} * 100\%,$$

где E - эффективность примененных мер (в процентах), N выявленных угроз - количество фактически предусмотренных и отработанных угроз, N возможных угроз - общее количество теоретически возможных угроз на маршруте.

Данный показатель позволяет оценить, насколько эффективно организационные меры минимизировали выявленные угрозы безопасности.

Допустим, экспертами было идентифицировано 20 потенциальных угроз на маршруте Алматы–Тель-Авив. Благодаря комплексу организационных мер авиакомпании удалось предотвратить 17 угроз.

Эффективность принятых мер рассчитывается следующим образом:

$$E = \frac{17}{20} \times 100\% = 85\%.$$

Таким образом, эффективность принятых мер составила 85 %, что свидетельствует о высокой результативности внедрённых мер по обеспечению авиационной безопасности на данном маршруте.

Результаты и их обсуждение.

В результате проведённого исследования были выявлены и систематизированы организационные меры, применённые казахстанскими авиакомпаниями при открытии новых международных рейсов. Эти меры были проанализированы на примере рейсов авиакомпаний Air Astana (Алматы - Тель-Авив) и SCAT Airlines (Шымкент/Алматы - Джидда/Медина).

В таблице 1 представлены основные организационные меры, идентифицированные на исследуемых направлениях, с количественной оценкой их эффективности согласно предложенной методике.

Таблица 1 – Сравнительная характеристика организационных мер и оценка их эффективности

№	Организационные меры	Международный стандарт (ссылка на ICAO/EASA)	Применение на рейсах	Кол-во угроз идентифицировано	Кол-во угроз предотвращено	Эффективность мер
1	Предварительная оценка угроз и рисков на маршруте	ICAO Doc 8973, ICAO Annex 17	Air Astana, SCAT	20	17	85%
2	Усиленный предполетный досмотр пассажиров и багажа	ICAO Doc 8973, EASA Regulation (EU) 2015/1998	Air Astana, SCAT	15	14	93%
3	Специализированный инструктаж и подготовка наземного персонала	ICAO Annex 17, ICAO Doc 9808	Air Astana, SCAT	12	10	83%
4	Взаимодействие с авиационными властями и службами безопасности	ICAO Doc 8973, ICAO Doc 10118	Air Astana, SCAT	10	8	80%

	зарубежных государств					
5	Планирование мер на случай чрезвычайных ситуаций	ICAO Doc 8973, ICAO Crisis Management Guide	Air Astana	7	6	86%
6	Усиление контроля поведения пассажиров на борту	ICAO Circular 352, IATA Guidance on Unruly Passengers	SCAT	10	9	90%

Таблица отображает, что наиболее эффективными мерами на исследуемых маршрутах стали усиленный предполетный досмотр (93%) и контроль поведения пассажиров на борту (90%). Также высоким уровнем эффективности характеризуется предварительная оценка рисков и планирование действий на случай чрезвычайных ситуаций.

Выявленные меры безопасности при открытии новых рейсов. На основе анализа, можно сделать вывод, что эффективное обеспечение авиационной безопасности на новом направлении требует реализации комплекса организационных мер. К ключевым мерам относятся:

Предварительная оценка угроз и рисков. Перед запуском нового рейса проводится всесторонний анализ потенциальных угроз для конкретного маршрута. Авиакомпании все чаще привлекают специальные аналитические сервисы для оценки маршрутов (рис. 1, 2). Например, используются внешние консультации по авиационной безопасности и базы данных инцидентов, позволяющие получить углубленную оценку рискового профиля нового направления и рекомендации по мерам смягчения [5].



Рисунок 1 – Карта маршрутов авиакомпании Air Astana



Рисунок 2 – Зоны конфликтов по данным Авиационной Администрации Казахстана на июнь 2025

Корректировка процедур досмотра и контроля. На этапе планирования рейса анализируется, достаточно ли стандартных мер авиационной безопасности или требуются усиленные процедуры досмотра пассажиров, багажа и грузов (рис. 3). Решение принимается с учетом профиля предполагаемых пассажиров и характера маршрута. Так, для рейсов в страны с повышенной террористической угрозой могут вводиться дополнительные уровни контроля: многократный досмотр ручной клади, личные интервью с пассажирами перед вылетом, усиленные меры досмотра грузов [6].

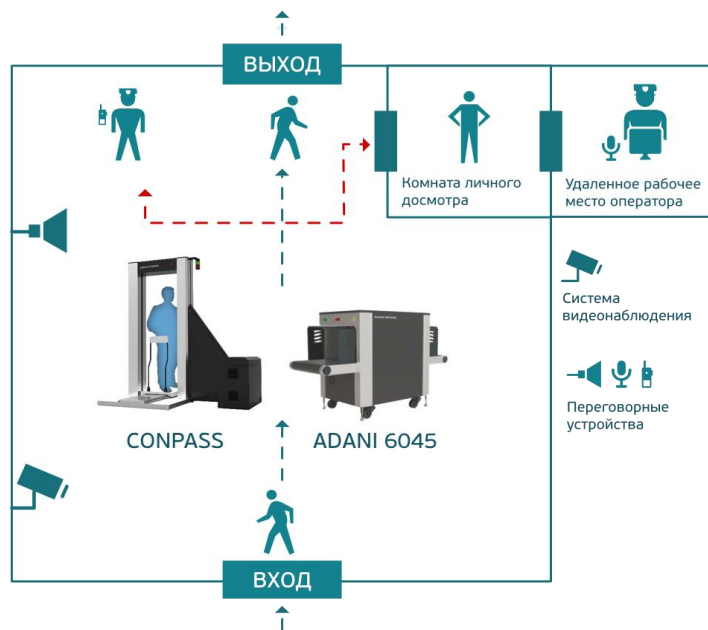


Рисунок 3 – Стандартный алгоритм досмотра пассажиров в терминале

Взаимодействие с государственными органами и иностранными партнерами. Организационные меры включают установление тесного взаимодействия между авиакомпанией и компетентными органами безопасности – как казахстанскими (Комитет гражданской авиации, службы авиационной безопасности аэропортов, правоохранительные органы), так и иностранными.

Усиление контроля за поведением пассажиров на новых направлениях. По мере начала выполнения нового рейса авиакомпания наблюдает за ситуацией на борту и в аэропортах, чтобы выявить возможные проблемы. По данным ИАТА, в первые годы после пандемии наблюдается общемировой рост случаев деструктивного поведения пассажиров: в 2022 году зафиксирован один инцидент на 568 рейсов, что на 47% больше, чем годом ранее (рис. 4) [8, 9, 10].

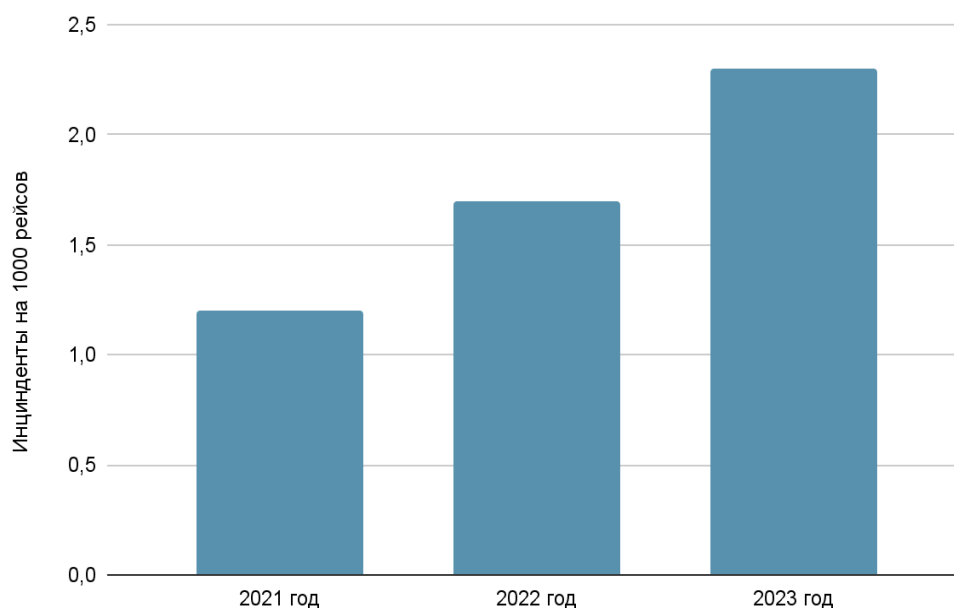


Рисунок 4 – Рост числа инцидентов с недисциплинированными пассажирами на 1000 рейсов по данным ИАТА за 2021–2023 годы

Планирование мер на случай чрезвычайных ситуаций. Одним из важных результатов оценки рисков является разработка плана действий при наступлении тех или иных угроз на новом маршруте. Авиакомпания заблаговременно готовит сценарии: от задержки или отмены рейса в случае резкого ухудшения обстановки до экстренной эвакуации пассажиров из страны назначения при возникновении кризиса. Примером послужил рейс Air Astana в Тель-Авив, выполнение которого осенью 2023 года потребовалось оперативно приостановить из-за внезапной эскалации вооруженного конфликта в Израиле. В таблице 2 представлена информация о принятых мерах [7].

Таблица 2 – Сравнительная характеристика принятых организационных мер обеспечения авиационной безопасности рейсов Air Astana и SCAT

Общие меры обеспечения авиационной безопасности	Алматы - Тель-Авив (Air Astana)	Шымкент/ Алматы - Медина, Джидда (SCAT Airlines)
Расширенный предполетный досмотр багажа и пассажиров.	Совместная работа с службой безопасности аэропорта Бен-Гурион,	Тесная координация с авиационными властями Саудовской Аравии, учет

	выполнение требований израильской стороны по предполетному контролю.	требований местных правил (например, запретов на провоз ряда предметов).
Инструктаж экипажей по действиям при угрозах, постоянный мониторинг обстановки.	Готовность к приостановке рейсов при обострении ситуации (было реализовано в октябре 2023).	Усиленное информирование пассажиров перед вылетом о правилах (в том числе разъяснение запрета курения и нарушений на борту).

Важно отметить, что эффективность организационных решений напрямую коррелирует с наличием предварительной оценки рисков и адаптивностью мер под специфику маршрута (геополитическая ситуация, культурные особенности, инфраструктурная готовность аэропортов назначения). На рисунке 5 представлена блок-схема необходимых шагов для эффективной организации обеспечения авиационной безопасности.



Рисунок 5 – Блок-схема риск-ориентированного процесса обеспечения авиационной безопасности нового рейса

В контексте методического обеспечения, включающего оценку рисков, контроль эффективности мер и подготовку персонала, выявлено отсутствие унифицированного подхода, что создает риск вариативности качества обеспечения безопасности на различных маршрутах. Это подтверждает необходимость разработки единой методики риск-ориентированного планирования организационных мер безопасности на национальном уровне. Для достижения качественного уровня авиационной безопасности государству следует рассмотреть возможность создания национальных методических рекомендаций по управлению рисками при открытии новых маршрутов, внедрения механизмов межведомственного анализа и аудита эффективности принимаемых мер, формирования централизованной базы данных типовых угроз и мер реагирования для новых направлений,

а также интеграции элементов моделирования и сценарного анализа в программы подготовки персонала.

Заключение.

Внедрение перечисленных мер позволит повысить устойчивость новых маршрутов к актуальным угрозам и обеспечить надлежащий уровень защиты пассажиров и экипажа. Рекомендации для отрасли включают развитие методических указаний по оценке рисков для новых направлений на национальном уровне, обмен опытом между авиакомпаниями по успешным практикам обеспечения безопасности, а также регулярное обновление программ подготовки персонала с учетом изменяющегося профиля угроз. Перспективой дальнейших исследований является количественная оценка эффективности тех или иных мер (например, влияние дополнительного досмотра на снижение попыток пронести запрещенные предметы) и разработка оптимальных моделей распределения ресурсов безопасности при расширении маршрутной сети.

Таким образом, организационные меры, основанные на проактивном управлении рисками и межведомственном взаимодействии, являются неотъемлемым условием безопасного роста авиационной отрасли Казахстана на международной арене.

Список литературы

1. Air Astana. (2023). Информация касательно рейсов Air Astana в Тель-Авив [Электронный ресурс]. <https://ir.airastana.com/ru/o-kompanii/novosti-i-press-relizy/informafiya-kasatel-no-reisov-air-astana-v-tel-aviv/>
2. Дормидонтов, А. В., Краснов, С. И., Павлов, Н.В. (2009). Авиационная безопасность: учебное пособие, (с. 7-20).
3. Зубков, Б. В., Прозоров, С. Е., Краснов, С. И., Ильин, В. М. (2012). Авиационная безопасность: учебник для вузов, (с. 370).
4. ИКАО Документ 8973. (2020). Руководство по авиационной безопасности, (с. 161-166).
5. Forbes.kz. (2023). Air Astana: динамика развития в 2023 году [Электронный ресурс]. <https://forbes.kz/articles/v-air-astana-rasskazali-o-dinamike-razvitiya-v-2023-godu>
6. Iata.org. (2023). Unruly Passenger Incidents in Post-Pandemic Increase [Электронный ресурс]. <https://www.iata.org/en/pressroom/2023-releases/2023-06-04-02/>
7. ИКАО Приложение 17, 12-е издание. (2022). Безопасность: защита международной гражданской авиации от актов незаконного вмешательства, (с. 52-54).
8. Sweet, K. (2008). Aviation and airport security: terrorism and safety concerns, (с. 159-164).
9. Skybrary.aero. (2017). Flight Operations Risk Assessment Checklist - New Destination [Электронный ресурс]. <https://skybrary.aero/articles/flight-operations-risk-assessment-checklist-new-destination>
10. Tengrinews.kz. (2024). Новые горизонты с авиакомпанией SCAT: летим в Саудовскую Аравию [Электронный ресурс]. <https://tengrinews.kz/around-the-world/novye-gorizontyi-aviakompaniey-scat-letim-saudovskuyu-546836/>

References

1. Air Astana. (2023). Informacija kasatel'no rejsov Air Astana v Tel'-Aviv [Elektronnyj resurs]. <https://ir.airastana.com/ru/o-kompanii/novosti-i-press-relizy/informafiya-kasatel-no-reisov-air-astana-v-tel-aviv/>
2. Dormidontov, A. V., Krasnov, S. I., Pavlov, N.V. (2009). Aviacionnaja bezopasnost': uchebnoe posobie, (s. 7-20).
3. Zubkov, B. V., Prozorov, S. E., Krasnov, S. I., Il'in, V. M. (2012). Aviacionnaja bezopasnost': uchebnik dlja vuzov, (s. 370).
4. ICAO Dokument 8973. (2020). Rukovodstvo po aviacionnoj bezopasnosti, (s. 161-166).

5. Forbes.kz. (2023). Air Astana: dinamika razvitija v 2023 godu [Jelektronnyj resurs]. <https://forbes.kz/articles/v-air-astana-rasskazali-o-dinamike-razvitiya-v-2023-godu>
6. Iata.org. (2023). Unruly Passenger Incidents in Post-Pandemic Increase [Jelektronnyj resurs]. <https://www.iata.org/en/pressroom/2023-releases/2023-06-04-02/>
7. ICAO Prilozhenie 17, 12-e izdanie. (2022). Bezopasnost': zashhita mezhdunarodnoj grazhdanskoj aviacii ot aktov nezakonnogo vmeshatel'stva, (s. 52-54).
8. Sweet, K. (2008). Aviation and airport security: terrorism and safety concerns, (s. 159-164).
9. Skybrary.aero. (2017). Flight Operations Risk Assessment Checklist - New Destination [Jelektronnyj resurs]. <https://skybrary.aero/articles/flight-operations-risk-assessment-checklist-new-destination>
10. Tengrinews.kz. (2024). Novye gorizonty s aviakompaniej SCAT: letim v Saudovskuju Araviju [Jelektronnyj resurs]. <https://tengrinews.kz/around-the-world/novyie-gorizontyi-aviakompaniey-scat-letim-saudovskuyu-546836/>

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ӘУЕ КОМПАНИЯЛАРЫНЫҢ ЖАҢА ӘУЕ РЕЙСТЕРІН АШҚАНДА АВИАЦИЯЛЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ҰЙЫМДАСТЫРУ ШАРАЛАРЫ.

***Аңдатпа.** Бұл мақала қазақстандық әуе компаниялары жаңа халықаралық рейстерді ашу кезінде авиациялық қауіпсіздікті қамтамасыз етуге бағытталған ұйымдастыру шараларын зерттеуге арналған. Қазақстан Республикасының әуе тасымалы желісінің қарқынды кеңеюі жаңа бағыттарды іске қосу кезінде геосаяси ерекшеліктермен, терроризм қатерлерімен және жолаушыларды тасымалдауға қойылатын күшейтілген талаптармен байланысты қауіптердің туындауына алып келеді. Мұндай жағдайда алдын ала талдау жүргізу және халықаралық стандарттарға сәйкес бейімделген шараларды қабылдау аса маңызды.*

Зерттеудің мақсаты - авиациялық қауіпсіздікті қамтамасыз етуге бағытталған ұйымдастырушылық шараларды айқындау, жүйелеу және ғылыми тұрғыдан негіздеу, сондай-ақ олардың тиімділігін Қазақстанның Air Astana және SCAT Airlines әуе компаниялары рейстері мысалында бағалау. Әдістемелік негізіне ICAO, EASA, IATA құжаттарын және Қазақстан Республикасының ұлттық нормативтік актілерін талдау (Азаматтық авиация комитеті), сондай-ақ тәуекелдерді сапалық және сандық бағалау әдістері енді; ықтимал қауіптің жүзеге асу ықтималдығы (P) мен салдарының ауырлығын (C) бағалау үшін $R = P \times C$ формуласы қолданылды.

Нәтижелер көрсеткендей, ең тиімді шаралар жолаушылар ағынын кешенді бақылау (93%) және маршруттарды жүйелі тәуекелдік талдау (90%) болып табылады; бұлар күшейтілген алдын ала тексерумен, персоналды бейімделген даярлаумен және құзырлы органдармен үйлестірумен өзара байланыста іске асады. Салыстырмалы талдау Air Astana және SCAT Airlines бағыттарында қолданылған тәсілдердің халықаралық тәжірибеге сәйкестігін және маршрут ерекшеліктеріне икемді бейімделгенін көрсетті.

Зерттеудің ғылыми жаңалығы - жаңа бағыттарда қауіпсіздікті ұйымдастырудың интеграцияланған, тәуекелге негізделген моделін ұсынуда. Тәжірибелік маңызы - ұсыныстарды әуе компаниялары мен уәкілетті органдардың рейстерді жоспарлау, қауіптерді азайту және халықаралық талаптарға сәйкестікті арттыру үдерістерінде қолдану мүмкіндігі.

***Түйін сөздер:** авиациялық қауіпсіздік, жаңа бағыттар, Қазақстанның авиакомпаниялары, тексеру, қауіп-қатерлер, қауіпсіздік шаралары.*

ORGANIZATIONAL MEASURES TO ENSURE AVIATION SECURITY AT THE OPENING OF NEW FLIGHTS OF AIRLINES OF THE REPUBLIC OF KAZAKHSTAN

Abstract. This article focuses on organizational measures to ensure aviation security during the launch of new international routes by Kazakhstani airlines. With the rapid expansion of Kazakhstan's air transportation network, new destinations are often associated with emerging threats linked to geopolitical conditions, terrorism risks, and stricter requirements for passenger screening. The aim of the study is to identify, systematize, and scientifically substantiate organizational measures for aviation security, and to evaluate their effectiveness using the cases of Kazakhstani airlines Air Astana and SCAT.

The methodology is based on the analysis of international (ICAO, EASA, IATA) and national (Civil Aviation Committee of Kazakhstan) regulatory documents, combined with qualitative and quantitative risk assessment methods. The probability (P) and severity (C) of potential threats were assessed using the formula $R = P \times C$. This approach enabled the comparison of international practices and the identification of the most effective measures, including enhanced pre-flight screening, adaptive staff training, and passenger behavior monitoring.

The findings show that the most effective measures were integrated passenger flow control (93%) and systematic route risk analysis (90%). Comparative analysis demonstrated the importance of combining international standards with national regulations within a unified security management system.

The scientific novelty of the study lies in developing a comprehensive framework for aviation security when introducing new routes. Its practical significance is reflected in the applicability of the results for airlines in planning international operations, reducing security risks, and ensuring compliance with global standards, thus supporting the safe growth of civil aviation in Kazakhstan.

Keywords: aviation security, new routes, airlines of Kazakhstan, inspection, threats, security measures.

Сведение об авторах

Асильбекова Индира Жаксыбаевна	К.т.н., профессор, Академия гражданской авиации, г. Алматы Казахстан E-mail: a.indira@mail.ru
Серик Шахноза	Магистрант Академии Гражданской Авиации, г. Алматы E-mail: shakhnoza.serik@agakaz.kz

Авторлар туралы мәлімет

Асильбекова Индира Жаксыбаевна	Т.ғ.к., Азаматтық авиация академиясы, Алматы қ. Қазақстан E-mail: a.indira@mail.ru
Серик Шахноза	Азаматтық Авиация Академиясының магистранты, Алматы қ. E-mail: shakhnoza.serik@agakaz.kz

Information about the authors

Assilbekova Indira Zhaksybaevna	C.T.S., Professor, Academy of Civil Aviation, Almaty, Kazakhstan E-mail: a.indira@mail.ru
Serik Shakhnoza	Master's degree student of the Academy of Civil Aviation, Almaty E-mail: shakhnoza.serik@agakaz.kz



UDC 519.6

IRSTI 50.05, 50.41

https://doi.org/10.53364/24138614_2025_38_3_6

D. Rakhimzhanov^{1*}, S. Belginova²

¹Astana IT University, Astana, Kazakhstan

² University Turan, Almaty, Kazakhstan

*E-mail: d.rahimzhanov@astanait.edu.kz

TRANSFORMER MODELS FOR PASSENGER REVIEWS CLASSIFICATION: A STUDY USING RUBERT AND XLM-ROBERTA

Abstract. *This study investigates the development and performance evaluation of transformer-based models for the automatic classification of public transportation passenger reviews, aiming to enhance feedback processing while optimizing issue resolution. Efficient handling of passenger feedback is crucial for improving public transportation services, as unresolved complaints or operational inefficiencies can decrease passenger satisfaction and create logistical challenges. Traditional text classification approaches, such as keyword-based methods or classical Machine Learning (ML) algorithms, struggle with multilingual and heterogeneous textual data, particularly in low-resource languages. This study addresses this gap by systematically comparing transformer-based architectures for review classification in Russian and Kazakh, demonstrating their effectiveness in real-world applications. A key contribution of this research lies in evaluating both language-specific and multilingual transformers on passenger-generated feedback, offering insights into their generalization capabilities. Unlike previous studies, which predominantly focus on English-language datasets, this work introduces a newly created, manually labeled dataset covering diverse real-world scenarios in Russian and Kazakh, enabling an objective comparative analysis. Three transformer models DeepPavlov/rubert-base-cased, XLM-RoBERTa-base, and XLM-RoBERTa-large were trained and tested to assess their ability to process complex multilingual input. Experimental results indicate that XLM-RoBERTa-large achieves the highest classification accuracy (90%), particularly for code-mixed and multilingual reviews, whereas rubert-base-cased performs consistently well for Russian-language feedback (87.667%), reinforcing its suitability for monolingual classification tasks. XLM-RoBERTa-base exhibits a balanced trade-off between accuracy and robustness, making it a viable option for heterogeneous review processing (89.5%). Despite their effectiveness, transformer-based models still encounter challenges related to data balancing and the handling of underrepresented classes, particularly in scenarios with uneven language distributions or domain-specific terminology. These findings confirm that transformer models significantly enhance the automation of passenger feedback classification, providing a scalable solution for public transportation providers.*

Keywords: *Natural language processing, text classification, Transformers, BERT, DeepPavlov, XLM-RoBERTa, passenger feedback review, multilanguage modeling.*

Introduction.

As the number of public transport passengers increases, so does the volume of passenger appeals require prompt processing by support services. Until recently, in many vehicle fleets in

Astana, Kazakhstan, passenger reviews were manually analyzed by employees who read the text of the appeal or complaint, assessed its content, and forwarded it to the relevant department. This process demanded significant time and human resources, particularly during peak periods, leading to delays in processing and reduced passenger satisfaction. Advances in Artificial Intelligence (AI) and Natural Language Processing (NLP) have significantly enhanced the automation of passenger feedback analysis. Social media-based sentiment analysis has proven effective for assessing public transportation satisfaction, offering real-time insights that supplement traditional survey methods [1-2]. Additionally, data-driven approaches such as big data analytics and systematic complaint management have demonstrated the potential to optimize public sector responsiveness and service efficiency, particularly in bus transportation networks [3-4].

Previous research has applied traditional ML methods, such as SVM, Naïve Bayes, and Decision Trees, for text classification tasks in transport-related NLP [5-10]. For instance, [9] utilized an SVM classifier to process sentiment analysis of public transportation feedback from Twitter, achieving high accuracy on well-structured data. However, these models struggle with informal and code-mixed language, which is common in passenger complaints. Similarly, [6] demonstrated that Naïve Bayes is effective for classifying short text reviews, such as product reviews from Amazon, but struggles with generalization when applied to multilingual corpora, limiting its real-world applicability. Moreover, traditional ML models often require extensive feature engineering, making them less adaptable to real-world datasets that exhibit high linguistic variability.

Despite their widespread use, these methods exhibit significant limitations. Manual feature selection in traditional machine learning models relies on predefined linguistic patterns, failing to capture deep semantic relationships within the text, which limits their adaptability to complex language structures. Additionally, these models struggle to generalize across different datasets, particularly in multilingual settings, where linguistic variations and code-mixing introduce additional challenges. Furthermore, classical ML approaches are inefficient in handling noisy text, as passenger feedback is often short, informal, and contains abbreviations, leading to reduced classification accuracy and reliability in real-world applications.

To address the limitations of traditional machine learning approaches, modern NLP techniques employ deep learning architectures, particularly neural networks that automatically extract feature representations from text [11-13]. Recent advancements in deep learning have led to the development of transformer-based architectures, such as BERT and its multilingual adaptations, which have demonstrated superior performance in various text classification tasks [11-13]. Unlike classical methods, transformers utilize self-attention mechanisms that enable them to capture long-range dependencies and contextual nuances. Research indicates that BERT-based models generally surpass traditional machine learning techniques in multilingual text classification, particularly in tasks requiring nuanced contextual comprehension [12]. However, transformer models still face challenges in transport-related multilingual NLP applications. For instance, while mBERT exhibits strong performance in resource-rich languages, its effectiveness declines in low-resource and code-mixed settings due to limited training data and increased linguistic variability [14]. Similarly, while XLM-RoBERTa has been shown to enhance multilingual adaptability, it relies heavily on extensive labeled data for fine-tuning, which remains scarce for Kazakh [15]. DeepPavlov's ruBERT, optimized for Russian-language processing, achieves high accuracy in monolingual tasks; however, its applicability in handling mixed Russian-Kazakh text remains uncertain [14]. These challenges underscore the necessity of systematically evaluating transformer models to determine their suitability for real-world multilingual transport feedback classification.

Existing research on public transport feedback classification has predominantly focused on English-language corpora, with studies utilizing sentiment analysis and social media data to evaluate passenger satisfaction and service quality [1]. Some research has extended this approach to other languages, such as Spanish, as seen in studies conducted in Santiago, Chile, where Twitter

data was analyzed to infer user sentiment regarding public transportation [2]. However, these methods primarily rely on structured datasets and high-resource languages, limiting their applicability in multilingual or low-resource settings. Meanwhile, other studies have explored data-driven techniques to optimize complaint processing in public transport systems [3-4], focusing on operational efficiency rather than addressing the linguistic complexities associated with multilingual passenger feedback. Studies addressing transport-related NLP in underrepresented languages are virtually nonexistent, despite the increasing demand for multilingual AI applications in public services. While general-purpose multilingual NLP research has progressed [14-15], there are no established benchmarks or large-scale annotated datasets for transport-related multilingual classification, particularly in Kazakh and Russian-Kazakh mixed text. This lack of dedicated datasets and evaluations makes it difficult to determine which transformer models are most suitable for processing real-world passenger feedback in multilingual settings.

This study addresses this gap by introducing a novel dataset of real-world passenger reviews in Russian, Kazakh, and mixed-language text, which has been manually annotated for supervised classification. Unlike previous datasets used for transport-related NLP, which predominantly focus on English-language complaints [1], this dataset offers the first systematically annotated multilingual corpus for transport-related feedback in a low-resource setting. It captures linguistic challenges such as code-mixing, informal phrasing, and orthographic variations, ensuring a more realistic evaluation of transformer-based architectures for real-world applications in multilingual public transport services.

Unlike previous research, which primarily focuses on monolingual text classification, our study provides a systematic comparison of multilingual and Cyrillic-specific transformers, highlighting their strengths and limitations for passenger feedback categorization. The findings of this study serve as a foundation for further research in multilingual NLP and contribute to the development of real-world applications for automatic feedback routing in transport companies.

Materials and methods. The automation of text classification processes is an important area of applied research, particularly in the domain of feedback analysis. One of the key factors influencing the success of such research is the availability of real-world datasets, which are essential for training robust ML models. This study utilizes a unique dataset of passenger reviews provided by a public transportation company in Astana, Kazakhstan, covering user-generated feedback from the year 2023. The dataset was compiled from passenger appeals submitted through the official communication channels of the transport company, including mobile applications, customer support hotlines, and online complaint forms. These appeals contain a diverse range of feedback types, reflecting real-world passenger experiences and concerns. However, as the raw data was not pre-labeled, it required manual annotation to create a structured dataset suitable for model training, ensuring high-quality labeling and reliable classification. To ensure linguistic and contextual accuracy, the annotation was performed by researchers specializing in NLP and transportation systems. This process involves carefully assigning reviews to predefined categories while considering linguistic features, contextual meaning, and variations in multilingual content. To improve consistency, annotations were systematically reviewed and refined, minimizing potential discrepancies. This structured approach ensures that passenger reviews are accurately categorized, facilitating efficient processing and automatic redirection to relevant departments.

The dataset includes passenger complaints of varying lengths, from brief statements to detailed descriptions. To improve processing efficiency, complaints were categorized by word count: short (≤ 5 words), medium (6–20 words), and detailed (> 20 words). Figure 1 shows that detailed complaints dominate, followed by medium-length ones, while short complaints are rare. This classification aids optimization, allowing automated handling of short complaints and manual review of detailed cases requiring escalation.

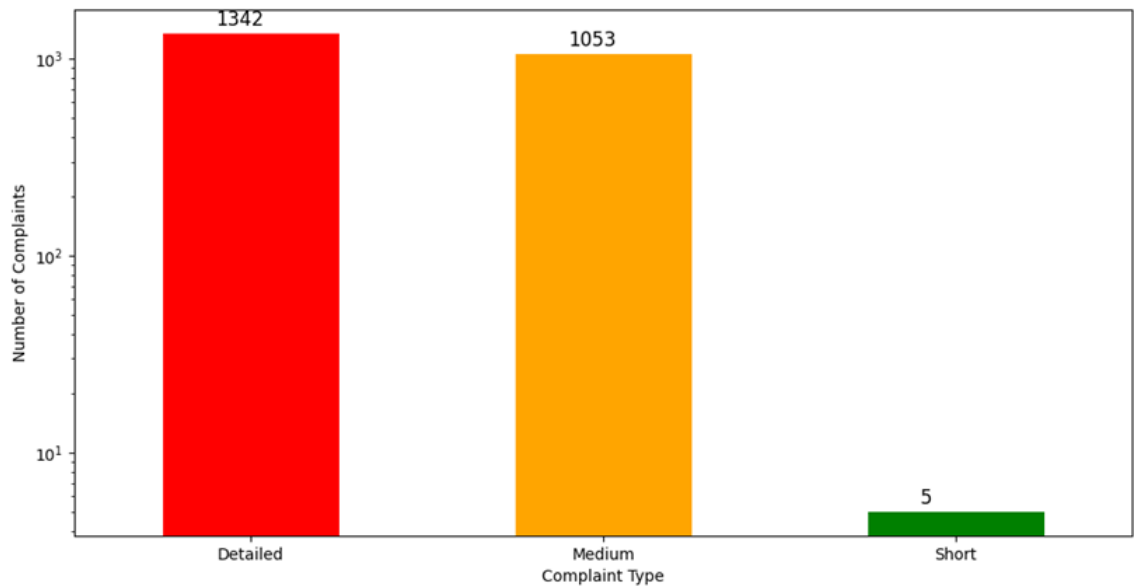


Figure 1 – Distribution of complaints by length

A distinctive feature of this dataset is its multilingual nature, as the reviews are written in both Russian and Kazakh, introducing additional challenges in text processing. Multilingual content variations complicate classification, as passengers may switch between languages within a single review, necessitating models capable of handling code-mixed text. Additionally, the dataset contains syntactic errors and informal language, including abbreviations, typos, and non-standard phrases, further increasing the complexity of text analysis. In some cases, reviews lack sufficient context, making it difficult to accurately determine user intent without context-aware classification methods. Addressing these challenges requires advanced NLP techniques, particularly transformer-based architectures, to improve classification accuracy and enhance the efficiency of automated complaint handling systems.

At table 1 provides an overview of selected complaints that illustrate varying degrees of literacy and informativeness in both Kazakh and Russian. These examples further highlight the linguistic diversity and challenges in processing such a dataset for automated classification purposes.

Table 1 – Selected reviews by literacy and informativeness levels

Literacy & Informativeness Level	Language	Example complaint
High literacy, highly informative	Kazakh	"N маршрут, 07:15-08:15, ЖК name аялдамасында күттік, шара қабылдаңыз."
	Russian	"Маршрут №N. В вечернее время ожидание маршрута более двух часов, нет освещения. Просим наладить график движения!"
Medium literacy, moderately informative	Kazakh	"N маршрут, name университет аялдамасынан name бағытта 18:15-18:46 жоқ. Автобус неге кешігіп жүр?"
	Russian	"Автобус №N, 2 женщинам стало плохо из-за давки. Просим пересмотреть количество маршрутов в часы пик!"
Low literacy, low informativeness	Kazakh	"Аялдамада күттік, автобус жоқ, неге?"
	Russian	"Ждал, ждал N-й автобус, не приехал. Что за беспорядок?!"

Code-mixed (Kazakh & Russian)	Mixed	"Жүргізуші не остановился на остановке, хотя біз күткен 20 минут. Это нормально?"
	Mixed	"N м/а Доброе утро! Запустите дополнительные маршруты N автобуса. Бұл мүмкін емес, адамдар сыймайды, есіктер жабылмайды. То двери выламываются в автобусах из-за большого количества людей. Потом приходится ждать автобус и опаздывать на работу!"
Literacy & Informativeness Level	Language	Example complaint
High literacy, highly informative	Kazakh	"N маршрут, 07:15-08:15, ЖК name аялдамасында күттік, шара қабылдаңыз."
	Russian	"Маршрут №N. В вечернее время ожидание маршрута более двух часов, нет освещения. Просим наладить график движения!"

The classification categories were determined through content analysis of the dataset and evaluation of the most frequently occurring themes. This structured categorization ensures that feedback is systematically forwarded to the relevant operational units. Seven distinct categories were identified:

1) Transport problems – Complaints related to route delays, vehicle overcrowding, breakdowns, and bus shortages. These issues constitute a significant proportion of all feedback, requiring immediate action to maintain the stability of transportation services.

2) Personnel problems – Reports concerning driver misconduct, reckless driving, or improper behavior of inspectors. These complaints highlight the need for improved staff training and adherence to service quality standards.

3) Bus stop infrastructure – Issues related to damaged or missing shelters, broken information boards, and the absence of heated waiting areas. Addressing these concerns is essential for enhancing passenger comfort and accessibility.

4) Equipment faults – Reports on technical failures of onboard systems, such as non-functional validators, heating units, and digital information displays. These reviews emphasize the importance of regular vehicle maintenance and technical inspections.

5) Acknowledgments, Praise – Positive feedback regarding driver professionalism, improved route efficiency, and overall service enhancements. This category helps identify successful operational strategies and recognize high-performing staff.

6) Organizational and technical problems – Complaints about errors in route maps, issues with public transport card top-ups, and a lack of real-time scheduling information. These reviews suggest a need for better organizational planning and improved passenger communication.

7) Other complaints – Feedback that does not fit neatly into the defined categories or overlaps multiple issues. This category highlights the diversity of passenger concerns and the need for flexibility in automated classification systems.

While the dataset is highly informative, several limitations must be considered. Data imbalance presents a challenge, as certain categories, such as “Other complaints”, contain significantly fewer samples than major categories like “Transport problems”, potentially affecting model performance. Additionally, noise in the data, including spelling errors, slang, and informal expressions, complicates classification and may necessitate data preprocessing techniques to improve accuracy. Contextual ambiguity is another concern, as some reviews lack explicit details, requiring context-aware NLP models to accurately infer user intent. Finally, the dataset exhibits domain specificity, as it is sourced from a single transport company in Astana, meaning findings may not be directly generalizable to other cities or transportation networks without further

validation.

Unlike most publicly available transport-related review datasets, which are predominantly monolingual and focus on English-language feedback, this dataset presents a unique multilingual perspective, covering passenger-generated content in Russian and Kazakh. This makes it particularly valuable for developing NLP models tailored to low-resource languages and improving multilingual feedback classification in the public transportation domain.

Table 2 presents the distribution of annotated reviews across the training and test datasets. The dataset consists of 2,400 manually labeled reviews, with 1,800 allocated for training and 600 for testing.

Table 2 – Distribution of annotated reviews by category and their division into training and test datasets

No.	Name of class	Number of annotated reviews		
		Total	Training dataset	Test dataset
0	Transport problems	1214	910	304
1	Personnel problems	605	454	151
2	Bus stop infrastructure	175	131	44
3	Equipment faults	157	118	39
4	Praise	117	88	29
5	Organizational and technical problems	104	78	26
6	Other complaints	28	21	7
	TOTAL	2400	1800	600

Models. Modern language models based on the Transformer architecture demonstrate high efficiency in NLP tasks. In this study, we explore the following transformer-based language models: DeepPavlov/rubert-base-cased, XLM-RoBERTa-base, and XLM-RoBERTa-large.

The DeepPavlov/rubert-base-cased model is a Russian-language adaptation of BERT, developed as part of the DeepPavlov project [14]. It has been trained on a large corpus of Russian-language texts, including Wikipedia, news articles, and other open sources. The primary advantage of this model is its ability to process text while considering morphological and syntactic features of the Russian language, making it a strong choice for monolingual tasks [14]. An additional advantage is its support for pretraining on specialized datasets, allowing for adaptation to specific domains. In this study, rubert-base-cased was further trained on a manually labeled passenger feedback dataset containing texts in both Russian and Kazakh. This adaptation improved its performance in a multilingual environment, enhancing classification accuracy.

In contrast, XLM-RoBERTa-base is a multilingual model developed by Meta AI, designed to process texts in over 100 languages, including Russian and Kazakh. Its architecture is based on a multi-headed attention mechanism, enabling it to capture complex dependencies between words. The model employs the Byte-Pair Encoding (BPE) tokenization method, which enhances its robustness against spelling errors and syntactic variability, a particularly valuable feature when dealing with heterogeneous data [15].

The extended version of this model, XLM-RoBERTa-large, has a greater number of parameters and a deeper network, leading to higher accuracy in processing complex linguistic structures. Due to its increased number of layers and attention heads, the model demonstrates improved context understanding, particularly in tasks involving multilingual text analysis [15].

Table 3 summarizes the key architectural features of these models. These parameters directly impact computational efficiency and the model's ability to process texts of varying length and complexity. While a greater number of layers and parameters enhances performance, it also increases computational requirements.

Table 3 – Key features of the models

Model Name	DeepPavlov/rubert-base-cased	XLM-RoBERTa-base	XLM-RoBERTa-large
Number of layers	12	12	24
Size of hidden layer	768	768	1024
Number of attention heads	12	12	16
Number of parameters	≈ 110 million	≈ 270 million	≈ 550 million
Max. length of input sequence	512	512	512

Experiments. In our experiment, the three selected models were fine-tuned on the dataset described above. The data was split with 75% allocated for training and 25% for testing, while maintaining class balance across all categories. This distribution ensured that each feedback category was equally represented in both the training and test sets, allowing for an unbiased evaluation of the models' performance across the seven predefined categories.

Training was conducted over three epochs using the fine-tuning method on pre-trained transformer models. The optimizer used was AdamW with a learning rate of $2e-5$. For training the models, a maximum input sequence length of 256 tokens was used, ensuring a balance between computational efficiency and the quality of text processing. The optimal batch size during the experiments was determined to be 16, which accelerated the training process while maintaining stable gradient descent parameters. During training, the data was shuffled to prevent sequential dependencies, while the test set remained fixed to ensure reproducibility of results.

To assess the quality of classification, several evaluation metrics were utilized, including Accuracy, Macro Average F1-score, Weighted Average F1-score, Precision, and Recall. Accuracy serves as an indicator of the overall performance of the classification model across all categories. The Macro Average F1-score reflects the unweighted mean of the F1-scores across all categories, making it particularly relevant for handling class imbalance and evaluating the model's performance on underrepresented categories. In contrast, the Weighted Average F1-score provides a more comprehensive measure of overall performance by accounting for the proportion of samples in each category, ensuring that the evaluation reflects the real-world distribution of data. Precision and Recall were analyzed for key categories to assess the model's effectiveness in minimizing false positives and capturing true positives. The experimental results, summarized in Table 3, present a comparative analysis of the models for review classification in a multilingual environment, highlighting their respective strengths and limitations.

Results and their discussion.

As shown in Fig. 2, DeepPavlov/rubert-base-cased model testing demonstrated high accuracy for categories with a large amount of data, such as 'Transport problems' and 'Personnel problems'. However, for sparse categories such as 'Praise', the F1-score remains low due to the insufficient number of examples in the training set. This result aligns with expectations, as models trained on imbalanced datasets tend to prioritize high-frequency classes, leading to suboptimal performance in underrepresented categories.

	precision	recall	f1-score	support
Transport problems	0.98258	0.92763	0.95431	304
Personnel problems	0.80899	0.95364	0.87538	151
Bus stop infrastructure	0.82759	0.92308	0.87273	26
Equipment faults	0.64286	0.62069	0.63158	29
Praise	1.00000	0.28571	0.44444	7
Organizational and technical	0.91176	0.70455	0.79487	44
Other complaints	0.59524	0.64103	0.61728	39
accuracy			0.87667	600
macro avg	0.82414	0.72233	0.74151	600
weighted avg	0.88559	0.87667	0.87577	600

Figure 2 – Model results: DeepPavlov/rubert-base-cased

The confusion matrix shown in Fig. 3 provides a detailed breakdown of prediction errors and confirms the high performance in 'Transport problems' and 'Personnel problems' categories while highlighting misclassifications in the 'Praise' and 'Other complaints' categories. These misclassifications suggest that DeepPavlov/rubert-base-cased struggles with classes that exhibit greater linguistic variation and fewer training examples.

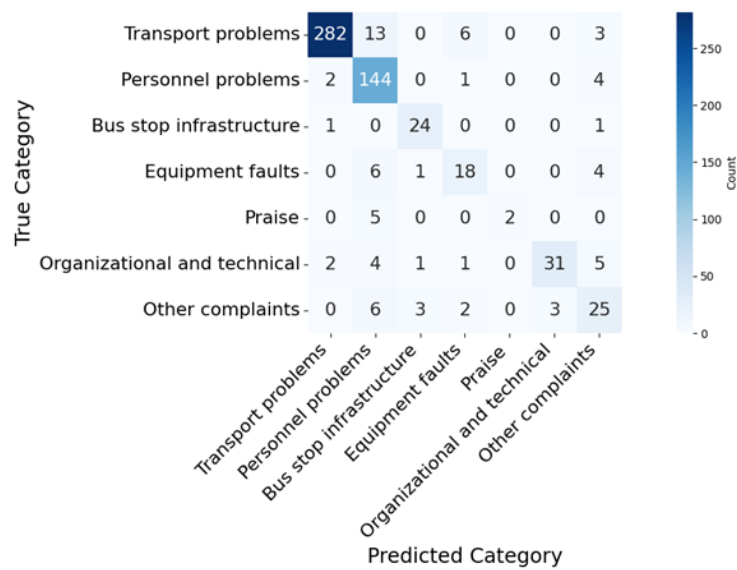


Figure 3 – Confusion Matrix for DeepPavlov/rubert-base-cased

According to the results shown in Fig. 4, the XLM-RoBERTa-base model also showed high accuracy for categories with a large amount of data: 'Transport problems' and 'Personnel problems'. However, for low-resource categories such as 'Praise', the F1-score remains suboptimal due to the limited availability of training examples. Notably, XLM-RoBERTa-base exhibited a slight advantage over the DeepPavlov/rubert-base-cased model in the category 'Bus stop infrastructure', suggesting that it is more effective in capturing context in multilingual texts. In the category 'Equipment faults' the difference was insignificant, indicating that both models face similar difficulties in handling such complaints. The category 'Other complaints' also showed a slight advantage for XLM-RoBERTa-base, which may indicate its improved ability to handle heterogeneous and multi-thematic reviews. In general, both models perform well in processing large categories of reviews, but XLM-RoBERTa-base demonstrates superior performance in

handling complex and heterogeneous texts, while DeepPavlov/rubert-base-cased is more consistent in Russian-language contexts.

	precision	recall	f1-score	support
Transport problems	0.95161	0.97039	0.96091	304
Personnel problems	0.88344	0.95364	0.91720	151
Bus stop infrastructure	0.88889	0.92308	0.90566	26
Equipment faults	0.70000	0.72414	0.71186	29
Praise	0.00000	0.00000	0.00000	7
Organizational and technical	0.80952	0.77273	0.79070	44
Other complaints	0.67857	0.48718	0.56716	39
accuracy			0.89500	600
macro avg	0.70172	0.69017	0.69336	600
weighted avg	0.88031	0.89500	0.88619	600

Figure 4 – Model results: XLM-RoBERTa-base

The confusion matrix in Fig. 5 provides a detailed visualization of classification performance, indicating the number of correctly classified reviews and misclassifications. This analysis allows for a deeper understanding of the model's strengths and areas for improvement, particularly in handling underrepresented classes.

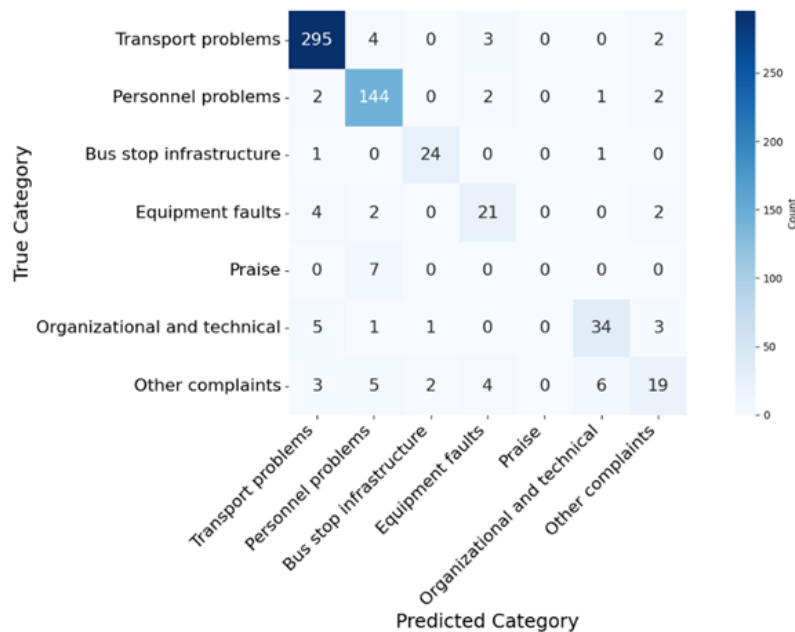


Figure 5 – Confusion Matrix for the XLM-RoBERTa-base model

The test results of the XLM-RoBERTa-large model, shown in Fig. 6, demonstrated high accuracy for most categories, especially for classes with large amounts of data. The categories ‘Transport problems’ and ‘Personnel problems’ showed strong results, indicating the model’s high ability to handle common types of reviews. Additionally, XLM-RoBERTa-large showed significant improvements in the classification of categories such as ‘Bus stop infrastructure’ and ‘Organizational and technical problems’, suggesting that it better captures contextual nuances in multilingual data.

	precision	recall	f1-score	support
Transport problems	0.95146	0.96711	0.95922	304
Personnel problems	0.89744	0.92715	0.91205	151
Bus stop infrastructure	0.92000	0.88462	0.90196	26
Equipment faults	0.72414	0.72414	0.72414	29
Praise	0.66667	0.85714	0.75000	7
Organizational and technical	0.80952	0.77273	0.79070	44
Other complaints	0.73333	0.56410	0.63768	39
accuracy			0.90000	600
macro avg	0.81465	0.81385	0.81082	600
weighted avg	0.89760	0.90000	0.89781	600

Figure 6 – Model results: XLM-RoBERTa-large

Despite the overall improvement in accuracy, the model displayed varying results when processing certain categories. For instance, the ‘Praise’ category achieved an F1-score of 75.00%, which is significantly better than previous models but still indicates room for improvement due to the small dataset size. Meanwhile, the ‘Organizational and technical problems’ category showed notable progress, achieving an F1-score of 79.07%, reflecting the model’s enhanced ability to capture context in this category. Additionally, the F1-score for ‘Bus stop infrastructure’ reached 90.00%, highlighting the model’s ability to process multilingual data with complex context. The confusion matrix in Fig. 7 provides a comprehensive view of classification performance across all categories, highlighting both the model's strengths and areas requiring further optimization.

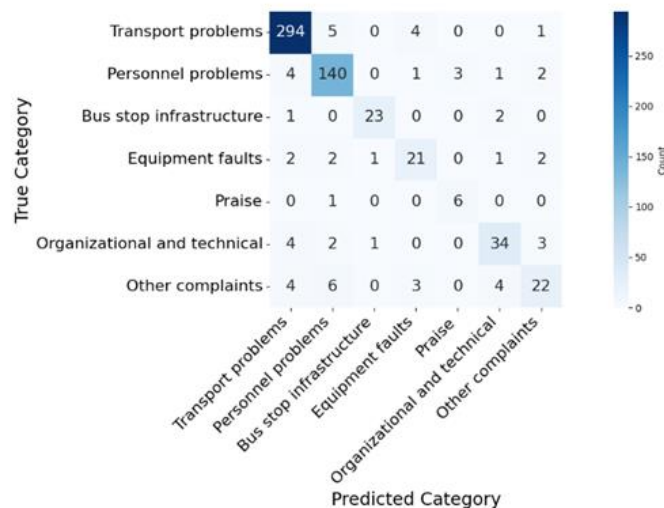


Figure 7 – Confusion Matrix for the XLM-RoBERTa-large model

Comparing XLM-RoBERTa-large with XLM-RoBERTa-base and DeepPavlov/rubert-base-cased, the former demonstrated superior performance in accuracy and F1-score across most categories. The improvement is particularly evident in the ‘Bus stop infrastructure’ category, where XLM-RoBERTa-large achieved an F1-score of 90.20%, emphasizing its stronger ability to capture contextual nuances in multilingual texts. This improvement can be attributed to XLM-RoBERTa’s cross-lingual training on diverse multilingual corpora, which enables better generalization across languages. Unlike DeepPavlov/rubert-base-cased, which is optimized

specifically for Russian, XLM-RoBERTa-large effectively processes both Russian and Kazakh text, reducing errors in code-mixed reviews.

The overall accuracy of XLM-RoBERTa-large was 90.00%, the highest among all tested models, which underscores its enhanced capacity to handle complex and multilingual data. The high weighted F1-score of 89.78% suggests that the model performs well on dominant categories, while the improved macro-average F1-score of 81.80% indicates better generalization across underrepresented classes. In contrast, XLM-RoBERTa-base achieved a lower macro-average F1-score, reflecting difficulties in handling imbalanced categories such as ‘Praise’ and ‘Other complaints’. This highlights that while all models perform well on frequent categories, XLM-RoBERTa-large demonstrates a superior ability to balance classification across all categories, making it the most effective model in a multilingual setting.

As shown in Table 4, DeepPavlov/rubert-base-cased demonstrated consistent performance in processing Russian-language texts, particularly in high-frequency categories like ‘Transport problems’ and ‘Personnel problems’. This can be attributed to the model’s architecture, which is specifically fine-tuned for Russian, allowing it to capture linguistic nuances more effectively. However, its performance in rarer categories such as ‘Praise’ remained limited, likely due to overfitting on dominant classes and difficulties in generalizing to low-resource categories. Meanwhile, XLM-RoBERTa-base delivered comparable accuracy, with the added advantage of effectively handling Kazakh texts and complex reviews due to its multilingual architecture. Overall, XLM-RoBERTa-large, with its more advanced architecture, provided the best performance by achieving a macro-average F1-score of 81.80% and a weighted average F1-score of 89.78%, particularly excelling in the ‘Organizational and technical problems’ and ‘Bus stop infrastructure’ categories.

Table 4 – A comparative analysis of the models for the classification of reviews in a multilingual environment

Metrics	DeepPavlov RuBERT	XLM-RoBERTa Base	XLM-RoBERTa Large
Accuracy	87.667%	89.500%	90.000%
Macro Avg (F1-score)	74.151%	69.336%	81.802%
Weighted Avg (F1-score)	87.577%	88.619%	89.781%

Conclusion.

Experimental results demonstrated that leveraging Transformer-based models for automated classification of public transport passenger feedback yields high accuracy. However, analysis highlighted disparities in model performance due to variations in architectural design and multilingual data processing capabilities. A comparative evaluation of the tested models revealed that rubert-base-cased exhibits strong performance when processing Russian-language feedback, particularly in large categories. Following pre-training on Kazakh-language datasets, their effectiveness in multilingual contexts improved but still lagged behind XLM-RoBERTa models in handling sparse categories. XLM-RoBERTa-base outperformed in complex classification tasks due to its multilingual structure but encountered challenges with underrepresented categories. XLM-RoBERTa-large achieved the highest overall accuracy across categories but required significantly greater computational resources. Generally, XLM-RoBERTa-based models excelled in multilingual recall, whereas DeepPavlov/rubert-base-cased, despite enhanced Kazakh-language pre-training, maintained superior consistency in Russian-language classification but struggled with intricate multilingual contexts. The results confirmed that Transformer-based models provide an effective framework for automatic classification of multilingual passenger complaints. While all models demonstrated high accuracy in major categories, improvements in handling rare

complaint types remain necessary. Potential enhancements include expanding data representation for sparse categories, implementing data augmentation techniques, and applying ensemble methods to boost model resilience. Another promising avenue involves pre-training models on extensive domain-specific corpora of Kazakh texts to refine multilingual classification accuracy. Future research should prioritize advancing adaptation strategies for low-resource languages, optimizing data balancing techniques, and investigating hybrid architectures that integrate linguistic and domain-specific knowledge. Moreover, refining pre-training methodologies and enhancing model robustness against linguistic variability will be critical for improving classification efficiency in real-world multilingual feedback processing.

Acknowledgement

This research has been funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan, grant number BR24992852 «Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens' quality of life improvement».

References

1. Farzadnia, S., & Vanani, I. R. (2022). Identification of opinion trends using sentiment analysis of airlines passengers' reviews. *Journal of Air Transport Management*, 103, 102232.
2. Méndez J. T. et al. Using Twitter to infer user satisfaction with public transport: the case of Santiago, Chile //IEEE Access. – 2019. – Т. 7. – С. 60255-60263.
3. Liu, W. K., & Yen, C. C. (2016). Optimizing bus passenger complaint service through big data analysis: Systematized analysis for improved public sector management. *Sustainability*, 8(12), 1319.
4. Ghazzawi, A., & Alharbi, B. (2019). Analysis of customer complaints data using data mining techniques. *Procedia Computer Science*, 163, 62-69.
5. Basu, A., Walters, C., & Shepherd, M. (2003, January). Support vector machines for text categorization. In *36th Annual Hawaii International Conference on System Sciences*, 2003. Proceedings of the (pp. 7-pp). IEEE.
6. Pranckevičius, T., & Marcinkevičius, V. (2017). Comparison of naive bayes, random forest, decision tree, support vector machines, and logistic regression classifiers for text reviews classification. *Baltic Journal of Modern Computing*, 5(2), 221.
7. Soliman, T. H. A., Elmasry, M. A., Hedar, A. R., & Doss, M. M. (2012, October). Utilizing support vector machines in mining online customer reviews. In *2012 22nd International Conference on Computer Theory and Applications (ICCTA)* (pp. 192-197). IEEE.
8. Zheng, W., & Ye, Q. (2009, November). Sentiment classification of Chinese traveler reviews by support vector machine algorithm. In *2009 Third International Symposium on Intelligent Information Technology Application (Vol. 3, pp. 335-338)*. IEEE.
9. Effendy, V., Novantirani, A., & Sabariah, M. K. (2016). Sentiment analysis on Twitter about the use of city public transportation using support vector machine method. *Intl. J. ICT*, 2(1), 57-66.
10. Chaturvedi, N., Toshniwal, D., & Parida, M. (2019). Twitter to transport: geo-spatial sentiment analysis of traffic tweets to discover People's feelings for urban transportation issues. *Journal of the Eastern Asia Society for Transportation Studies*, 13, 210-220.
11. González-Carvajal, S., & Garrido-Merchán, E. C. (2020). Comparing BERT against traditional machine learning text classification. *arXiv preprint arXiv:2005.13012*.
12. Alimzhanov, Y. (2020). An academic assistant based on a pre-trained model for contextual answering questions. *Вестник вычислительные технологии Национальной инженерной академии Республики Казахстан, Федеральный исследовательский центр информационных и вычислительных технологий*, 54. Retrieved from https://acagor.kz/media/uploads/citech-2020/CITech_Part1_Final_rev2.pdf

13. Мукашев, А. Ш., Байзакова, С. М., Едилхан, Д., & Мукашева, А. К. (2022). DEVELOPMENT OF A SYSTEM FOR ANALYZING LARGE TEXT DATA ARRAYS USING DISTRIBUTION SEMANTICS METHODS. Вестник АУЭС, 2(57).

14. Savkin, M., Voznyuk, A., Ignatov, F., Korzanova, A., Karpov, D., Popov, A., & Kononov, V. (2024, November). DeepPavlov 1.0: Your Gateway to Advanced NLP Models Backed by Transformers and Transfer Learning. In Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: System Demonstrations (pp. 465-474).

15. Conneau, A. (2019). Unsupervised cross-lingual representation learning at scale. arXiv preprint arXiv:1911.02116.

ТРАНСФОРМЕР МОДЕЛЬДЕРІ АРҚЫЛЫ ЖОЛАУШЫЛАР ПІКІРЛЕРІН ЖІКТЕУ: RUBERT ЖӘНЕ XLM-ROBERTA МОДЕЛЬДЕРІНІҢ ҚОЛДАНЫСЫ

Аңдатпа. Бұл зерттеу қоғамдық көлік жолаушыларының пікірлерін автоматты түрде жіктеу үшін трансформер негізіндегі модельдерді әзірлеу және олардың өнімділігін бағалауға бағытталған. Мақсаты - пікірлерді өңдеуді жетілдіру және мәселелерді шешуді оңтайландыру. Жолаушылардың кері байланысын тиімді өңдеу - қоғамдық көлік қызметтерін жақсартудың маңызды бөлігі, себебі шешілмеген шағымдар мен операциялық тиімсіздік жолаушылардың қанағаттануын төмендетіп, логистикалық қиындықтарға әкелуі мүмкін. Кілтсөздерге негізделген әдістер немесе классикалық машиналық оқыту (ML) алгоритмдері сияқты дәстүрлі мәтін жіктеу тәсілдері көптілді және әртүрлі мәтіндік деректермен, әсіресе ресурсы шектеулі тілдерде жұмыс істеуде қиындықтарға тап болады. Бұл зерттеуде аталған мәселе орыс және қазақ тілдеріндегі пікірлерді жіктеудегі трансформаторлық архитектураларды жүйелі түрде салыстыру арқылы шешіледі, олардың нақты қолданыстағы тиімділігін көрсетеді. Зерттеудің басты үлесі - жолаушылардың пікірлері негізінде тілге бейімделген және көптілді трансформерлерді бағалап, олардың жалпылау мүмкіндіктеріне талдау жүргізу. Бұған дейінгі зерттеулер көбіне ағылшын тіліндегі деректер жиынтығына сүйенсе, бұл жұмыс орыс және қазақ тілдеріндегі әртүрлі нақты сценарийлерді қамтитын, қолмен таңбаланған жаңа деректер жиынтығын ұсынады. Зерттеу аясында үш трансформер моделі: DeepPavlov/rubert-base-cased, XLM-RoBERTa-base және XLM-RoBERTa-large жаттықтырылып, олардың күрделі көптілді мәтіндерді өңдеу қабілеті бағаланды. Эксперимент нәтижелері көрсеткендей, XLM-RoBERTa-large ең жоғары дәлдікке (90%) жетіп, аралас тілдер мен көптілді пікірлерді жіктеуде үздік нәтиже көрсетті. Ал rubert-base-cased моделі орыс тіліндегі пікірлерді жіктеуде тұрақты түрде жақсы нәтиже көрсетті (87.667%), бұл оны біртүрлі тапсырмаларға тиімді етеді. XLM-RoBERTa-base дәлдік пен тұрақтылықтың теңгерімді нұсқасын ұсынып, әртүрлі пікірлерді өңдеуде тиімді шешім ретінде ерекшеленді (89.5%). Алайда, трансформер модельдері тиімді болғанымен, олар деректердің теңгерімсіздігі мен сирек кездесетін санаттарды өңдеу сияқты мәселелерге тап болады, әсіресе тілдер тең бөлінбеген немесе арнайы терминология қолданылатын жағдайларда. Бұл нәтижелер трансформер модельдерінің жолаушылар пікірлерін автоматты түрде жіктеуді едәуір жақсартатынын және қоғамдық көлік қызметтері үшін ауқымды шешім ұсынатынын дәлелдейді.

Түйін сөздер: Табиғи тілді өңдеу, мәтінді жіктеу, Трансформер, BERT, DeepPavlov, XLM-RoBERTa, жолаушылар пікірлерін талдау, көптілді модельдеу.

МОДЕЛИ ТРАНСФОРМЕРЫ ДЛЯ КЛАССИФИКАЦИИ ОТЗЫВОВ ПАССАЖИРОВ: ИССЛЕДОВАНИЕ С ИСПОЛЬЗОВАНИЕМ RUBERT И XLM-ROBERTA

Аннотация. В этом исследовании изучается разработка и оценка производительности моделей на основе трансформеров для автоматической классификации отзывов пассажиров общественного транспорта с целью улучшения обработки обратной связи при оптимизации решения проблем. Эффективная обработка отзывов пассажиров имеет решающее значение для улучшения услуг общественного транспорта, поскольку нерешенные жалобы или эксплуатационная неэффективность могут снизить удовлетворенность пассажиров и создать логистические проблемы. Традиционные подходы к классификации текста, такие как методы на основе ключевых слов или классические алгоритмы машинного обучения (ML), испытывают трудности с многоязычными и неоднородными текстовыми данными, особенно на языках с низкими ресурсами. В этом исследовании этот пробел устраняется путем систематического сравнения архитектур на основе трансформаторов для классификации отзывов на русском и казахском языках, демонстрируя их эффективность в реальных приложениях. Ключевой вклад этого исследования заключается в оценке как языковых, так и многоязычных трансформеров на основе отзывов пассажиров, что дает представление об их возможностях обобщения. В отличие от предыдущих исследований, которые в основном фокусировались на наборах данных на английском языке, в этой работе представлен недавно созданный, вручную размеченный набор данных, охватывающий различные реальные сценарии на русском и казахском языках, что позволяет проводить объективный сравнительный анализ. Три модели трансформеры DeepPavlov/rubert-base-cased, XLM-RoBERTa-base и XLM-RoBERTa-large были обучены и протестированы для оценки их способности обрабатывать сложный многоязычный ввод. Экспериментальные результаты показывают, что XLM-RoBERTa-large достигает наивысшей точности классификации (90%), особенно для смешанных и многоязычных отзывов, тогда как DeepPavlov/rubert-base-cased работает стабильно хорошо для русскоязычных отзывов (87,667%), что подтверждает его пригодность для задач одноязычной классификации. XLM-RoBERTa-base демонстрирует сбалансированный компромисс между точностью и надежностью, что делает его жизнеспособным вариантом для обработки гетерогенных обзоров (89,5%). Несмотря на свою эффективность, модели на основе трансформера по-прежнему сталкиваются с проблемами, связанными с балансировкой данных и обработкой недостаточно представленных классов, особенно в сценариях с неравномерным распределением языков или терминологией, специфичной для предметной области. Эти результаты подтверждают, что модели трансформеры значительно улучшают автоматизацию классификации отзывов пассажиров, предоставляя масштабируемое решение для поставщиков общественного транспорта.

Ключевые слова: Обработка естественного языка, классификация текста, Transformers, BERT, DeepPavlov, XLM-RoBERTa, анализ отзывов пассажиров, многоязыковое моделирование.

Information about the authors

Daniyar Rakhimzhanov	Master of Science, Junior Researcher of Science and Innovation Center “Big Data and Blockchain Technologies” E-mail: d.rahimzhanov@astanait.edu.kz , Astana IT University, Kazakhstan
Saule Belginova	PhD, Associate professor, E-mail: Sbelginova@gmail.com , University Turan, Kazakhstan

Сведения об авторах

Данияр Рахимжанов	Магистр наук, младший научный сотрудник Научно-инновационного центра “Большие данные и блокчейн-технологии”, Астанинский университет информационных технологий, Казахстан, E-mail: d.rahimzhanov@astanait.edu.kz
Сауле Бельгинова	Кандидат технических наук, доцент, Университет Туран, Казахстан, E-mail: Sbelginova@gmail.com

Авторлар туралы мәлімет

Данияр Рахимжанов	Ғылым магистрі, “Үлкен деректер және блокчейн-технологиялар” ғылыми-инновациялық орталығының кіші ғылыми қызметкері, Астана Ақпараттық технологиялар университеті, Қазақстан, e-mail: d.rahimzhanov@astanait.edu.kz
Сауле Бельгинова	Техника ғылымдарының кандидаты, доцент, Тұран университеті, Қазақстан, e-mail: Sbelginova@gmail.com



ӘОЖ 004.056

ГТАХА 81.93.29

https://doi.org/10.53364/24138614_2025_38_3_7

А.Хомпыш^{1,2}, Қ.С.Сақан^{2*}, К.Алғазы², А.Ж.Абишева³

¹Нұр-Мұбарак Египет ислам мәдениеті университеті, Алматы, Қазақстан

²Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан

³Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан

*E-mail: kairat_sks@mail.ru

«EM CHIPER» БЛОКТЫ ШИФРЛАУ АЛГОРИТМІНІҢ КРИПТОБЕРІКТІЛІГІН ЗЕРТТЕУ

Аңдатпа. Криптографиялық алгоритмдерінің ішінде блокты шифрлау алгоритмдері құпия ақпараттарды рұқсат етілмеген пайдаланушылардан сенім қорғау үшін қолданылады. Көптеген мемлекеттерде блокты шифрлау алгоритмдерінің өзіндік стандарттары бекітілген. Ол өз кезегінде ақпараттарды сенімді қорғауға мүмкіндік береді. Ал Қазақстанда мұндай ақпараттарды қорғау алгоритмдерінің стандарттары бекітілмегенін ескерсек, онда блокты шифрлау алгоритмдерін құру, олардың криптоберіктілігін зерттеу әрқашанда өзекті мәселелердің бірі. Бұл мақалада блокты шифрлау «EM Chiper» алгоритміне дифференциальдық және статистикалық талдау жүргізіліп нәтижелері ұсынылды. Блокты шифрлау алгоритмдерінің қауіпсіздігін зерттеудің негізгі әдістерінің бірі статистикалық қауіпсіздігін талдау болып табылады. Әдетте блокты шифрлауда қолданылатын түрлендірулер барысында жақсы араластыру мен шашырау сәтті түрде орындалса, онда алгоритмнің криптографиялық беріктігін жоғарғы деңгейде қорғауға мүмкіндік алуға болады. Статистикалық талдау жүргізу үшін алгоритм бағдарламалық жүзеге асырылып әртүрлі ұзындықтағы шифрмәтін алынды. Жүргізілген зерттеулерге сай ұсынылған алгоритмнің статистикалық талдаулары жоғары нәтиже көрсетті, яғни NIST ұсынған талаптарға сай A бағанадағы мәндері C мәнінен үлкен, ал B мәндері D мәндерінен үлкен екендігі анықталды. Дифференциалды талдаулар нәтижесі көрсеткендей ұсынылған алгоритм криптобекітілігі жағынан жоғары екендігі анықталды. Яғни 16 раундтан бастап кілтті табу ықтималдығы 2^{-126} тең. Сонымен қатар мақалада белгілі алгоритмдердің дифференциалды талдауларына нәтижелерімен салыстырмалы талдау жүргізіліп, танымал Camellia 128, AES 128 алгоритмдерімен шамалас нәтиже көрсеткендігі анықталды. Алдағы жұмыстарда басқада алгоритмнің криптобекітілігі жан жақты зерттелініп нәтижелері мақала ретінде ұсынылатын болады.

Түйін сөздер. Блокты шифр, шифр, криптография, кілт, дифференциалды криптоталдау, статистикалық талдау, EM Chiper, S-блок.

Кіріспе.

Ақпараттық қауіпсіздік саласы қазіргі уақытта кез-келген ұйымда немесе жеке тұлға үшін маңызды бағыттың бір бөлігіне айналды. Әрбір интернет желісіне қосылған жеке тұлға немесе ұйымның жеке мәліметтерін (жеке сәйкестендіру нөмері (ЖСН), құпия сөздер, бұлттық технологияда сақталған құжаттар және ЭСК т.б) құпия ақпараттарын

шабуылдаушылардан қорғау маңызды болып саналады. Соңғы жылдары елімізде кибершабуылдаушылар пайданушылардың құпия ақпараттарына рұқсатсыз кіру арқылы әртүрлі іс-әрекеттер жүргізіп, құпия ақпараттарын ұрлауда. Осы тұрғыда құпия ақпараттарды рұқсат етілмеген шабуылдаушылардан қорғаудың ең сенімді әдістерінің бірі криптографиялық әдістер болып табылады [1-2]. Криптографиялық әдістер симметриялы және ассиметриялы деп екі топқа жіктеледі. Бұл екі алгоритмнің өз ерекшеліктері және кемшіліктері бар. Симметриялы шифрлар жылдамдығы жағынан жоғары болғанымен өз кезегінде ақпараттарды шифрлау және кері шифрлау үшін бір кілт қолданғандықтан кілт алмасу үлкен қиындықтар туғызуы мүмкін [3]. Ал ассиметриялық алгоритмдерде үлкен жай сандарды қолданғандықтан жылдамдығы төмен, бірақ кілт алмасуда өте тиімді құрастырылған. Онда құпия ақпараттарды шифрлау үшін бір кілт, ал кері шифрлау үшін басқа кілт қолданылады [4].

Ұсынылып отырған мақалада симметриялы блокты шифрлау алгоритмі болғандықтан осы бағытқа тоқталсақ. Блокты шифрлар құпия ақпараттарды белгілі бір биттік ұзындықтағы блоктарға бөліп әрбір блокпен жеке шифрлау жүргізіледі. Қазіргі қолданыстағы блокты шифрлау алгоритмінің ұзындықтары 64, 128, 256 тең [5]. Блокты шифрлау алгоритмдеріне DES [6], AES [7], SM4[8], GOS T[9], Present т.б. жатқызуға болады. Блокты шифрлау алгоритмдері VPN, қауіпсіз байланыс TLS, дискідегі деректерді шифрлау (itlocker, VeraCrypt), қауіпсіз хабар алмасу (Signal, Whatsapp) сияқты әртүрлі салада ақпараттарды сенімді қорғау үшін қолданылады. Блокты шифрлау алгоритмдері құпия ақпараттың мазмұнын криптографиялық түрлендірулер арқылы шабуылдаушыға түсініксіз етіп түрлендіреді.

Қазіргі блокты шифрлау алгоритмдері Киркхоффс [10] принципіне негізделген, яғни шифрдың сенімділігі шифрлау алгоритмінің құпиялылығында емес кілттің құпиялылығына тәуелді болу керек.

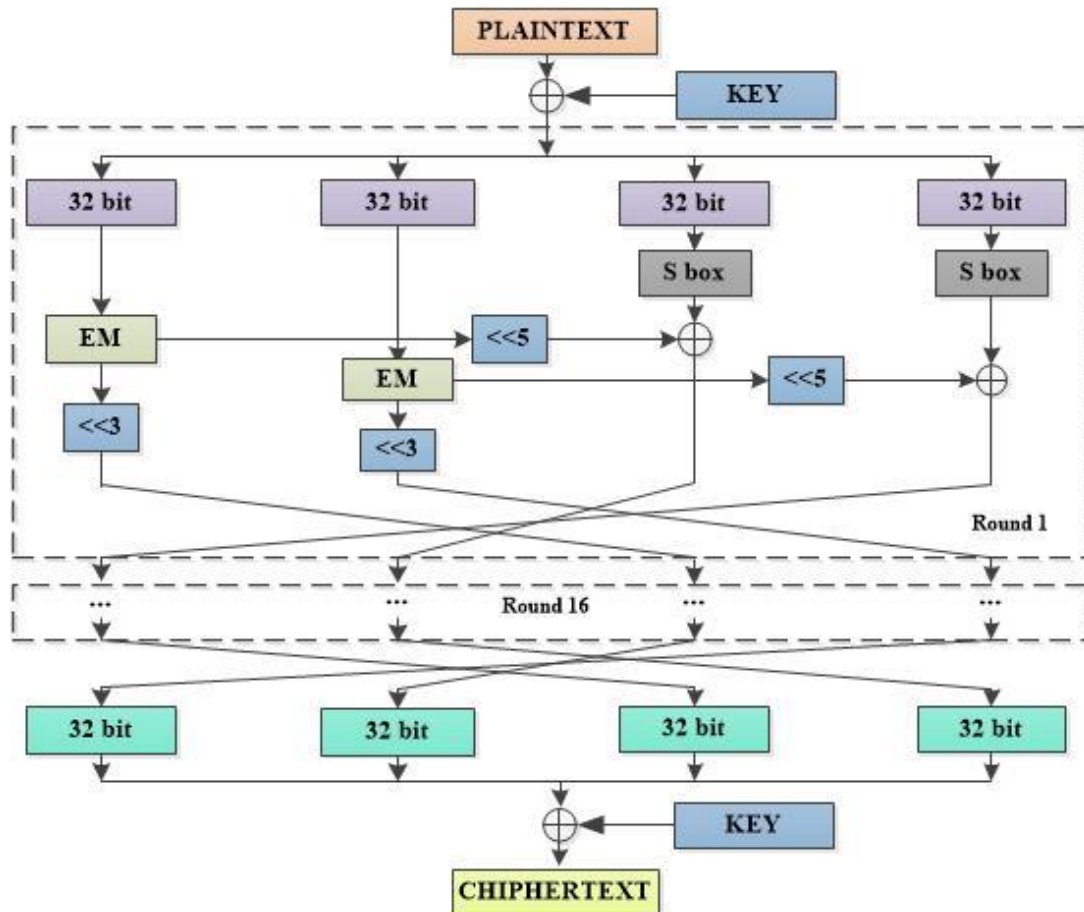
Қазіргі уақытта танымал блокты шифрлау алгоритмдерін қолдану саласын кеңейту шекті құрылғыларға негіздеп модификациясын жасаумен айналысуда, солардың бірі AES-ті сенсорлық желілерде тиімді қолдану тиімділігін арттыру және шифрлау жылдамдығын арттыру сияқты жұмыстарды қарастырған [11].

Chadi R. т.б. авторлар [12] AES, DES, 3DES, E-DES блокты шифрлау алгоритмдеріне салыстырмалы талдаулар жүргізіп, E-DES алгоритмі жоғары өнімділікке ие болатындығы дәлелдеген.

Блокты шифрлау алгоритмдері бойынша ауқымды талдау жұмыстарын жүргізген келесі [13] жұмысты атап айтуға болады, онда AES, Blowfish, IDEA сияқты шифрлау алгоритміне салыстырмалы талдау жүргізіп нәтижесін ұсынған.

Материалдар және тәсілдер.

Зерттеліп отырған «EM Cipher» блокты шифрлау алгоритмдерінің шифрлау схемасы 1-суретте көрсетілген. Онда EM түрлендіру, S-блок, цикльдік жылжыту, биттік қосу операциясы және 4 байттық орын ауыстыру сияқты қарапайым түрлендіру әдістері қолданылған. Бұл әдістер алгоритмнің криптоберіктілігін арттыру мақсатында жақсы араластыру және шашырату сияқты маңызды рөлді атқарады. Алгоритмнің толық құрылымы [3] жұмыста көрсетілген.



Сурет 1 – «EM Cipher» блокты шифрлеу алгоритмінің схемасы

«EM Cipher» блокты шифрлеу алгоритмінің ерекшелігі басқада блокты шифрлеу алгоритмдерінде кездеспейтін EM түрлендіру операциясы қолданылды (2-сурет). EM түрлендіруі сызықты емес функция болғандықтан өз кезегінде ұсынылған алгоритмнің криптоберіктіліні жоғары деңгейде арттыруға мүмкіндік береді. EM түрлендіру барысында 32 биттік кіріс мәндер (ашықмәтін блоктары) таңдап алынған $p_1(x), p_2(x), \dots, p_n(x)$ жұмыс негіздері деп аталатын келтірілмейтін көпмүшеліктердің дәрежесі бойынша бөліктерге бөлінеді. Алынған бөліктерді келесі формуладағы позициялық емес полиномиальды санау жүйесі (ПЕПСЖ) қалдықтардың тізбегі ретінде өрнектейміз:

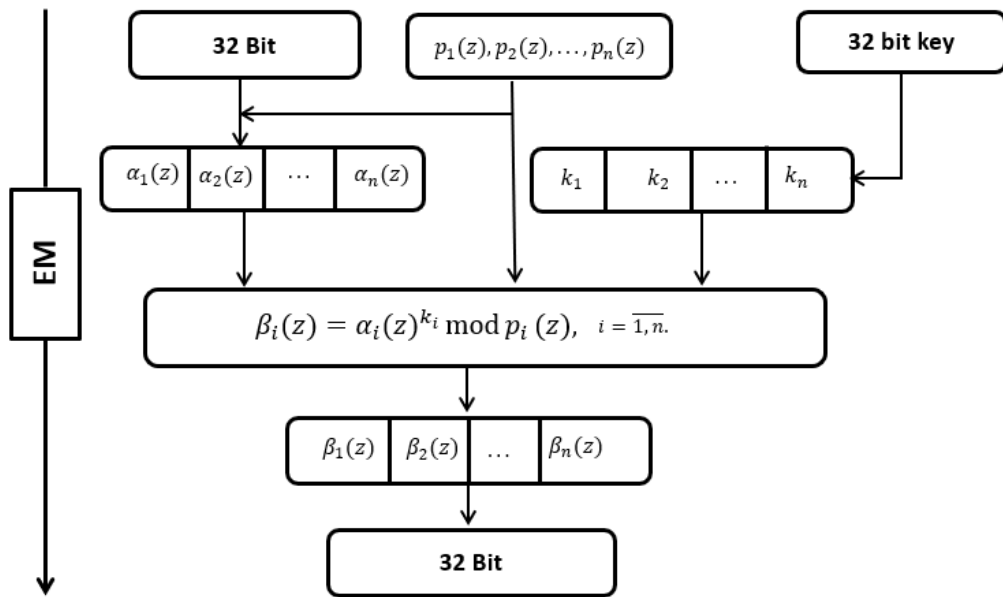
$$A(x) = a_1(x), a_2(x), \dots, a_s(x),$$

мұндағы $a_i(x)$ - алынған бөліктер, $i = \overline{1, S}$.

Қалдықтардың тізбегіндегі әр бір бөліктерді раундтық кілттерді қолдану арқылы түрлендіру процессін төмендегідей формуламен өрнектеп аламыз:

$$b_i(x) = a_i^{k_i}(x) \bmod p_i(x), i = \overline{1, S}.$$

мұндағы $b_i(x)$ - шығыс мәндер (шифрмәтін) бөлігі.



Сурет 2 – EM түрлендіру операциясы

EM түрлендіру операциясы модуль бойынша дәрежеге негізделгендіктен, алгоритмнің шифрлау және керішифрлау жылдамдығына әсер ететіндігі белгілі. Бұл мәселені оңтайлы шешу үшін индекс кестесі қолданылды [3]. Сонымен қатар «EM Cipher» блокты шифрлау алгоритміне қолданылған S-блок жаңа әдіс арқылы алынды [14].

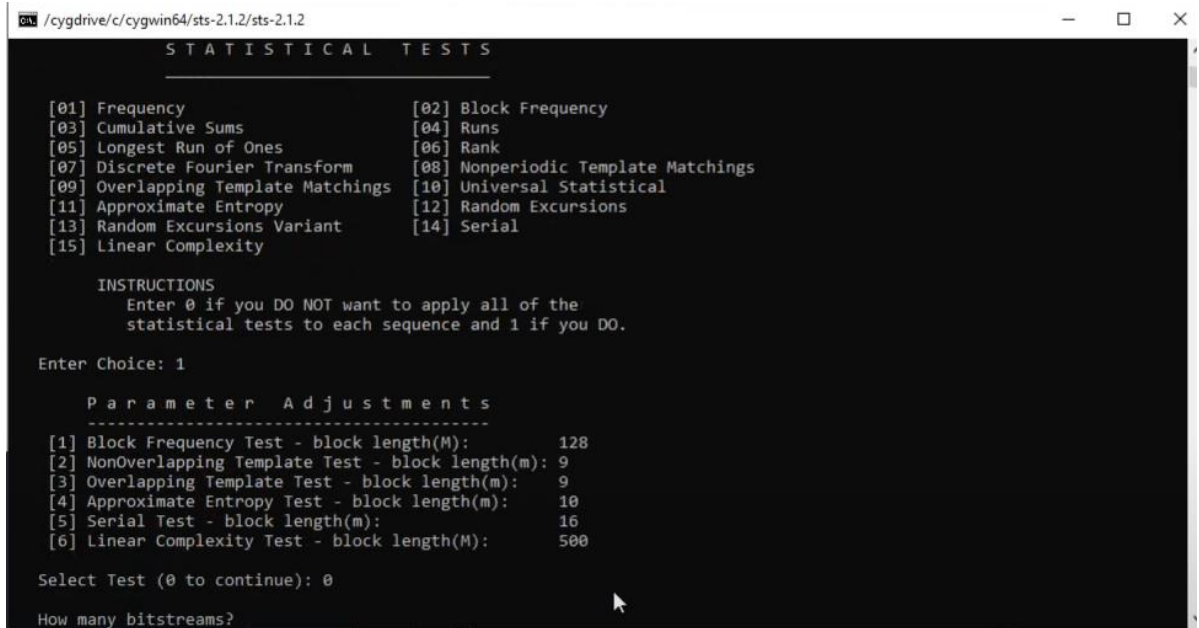
«EM Cipher» блокты шифрлау алгоритмінің криптоберіктілігін анықтау үшін қолданылған әдістерге тоқталсақ.

Статистикалық талдау. Блокты шифрлау алгоритмдерінің қауіпсіздігін зерттеудің негізгі әдістерінің бірі статистикалық қауіпсіздігін талдау болып табылады [3]. Шифрлау алгоритмдерін статистикалық тұрғыдан талдау үшін National Institute of Standards and Technology (NIST) сынақтары, Д.Кнут сынақтары, Diehard сынақтары және Crypt-X сынақтары қолданылады. Бұл сынақтар шифрлау алгоритмінен алынған шифрмәтінді әртүрлі критерийлер арқылы зерттеп, осал жерлерін анықтап, статистикалық тұрғыда бағалайды [15].

Дифференциалдық криптоанализ әдісі – блокты шифрлау алгоритмдеріне қарсы пайдаланылатын криптоаналитикалық шабуылдардың бір түрі. Бұл әдіс алғаш рет DES алгоритміне қолданылып, 1990 жылдардан бастап кеңінен танымал бола бастаған және көптеген шифрлау алгоритмдерінің беріктілігін осы әдіс арқылы тексереді. Дифференциалдық криптоанализ әдісі шифрлау алгоритмінің жұмыс істеу құрылымын біле отырып шабуылдаушылар кілтті анықтау ықтималдығын табады. Алгоритмге дифференциалды криптоанализ жүргізу барысында алдын ала таңдалған жұп шифрленген мәтін таңдап алынады. Шабуылдаушы $\Delta X = X_1 \oplus X_2$ ашықмәтін айырымдарын есептейді және оның нәтижесінде $\Delta Y = Y_1 \oplus Y_2$ шифрмәтіндердің айырымдары қандай болу керектігін табуға тырысады [16].

Нәтижелер мен талқылау.

Статистикалық талдау. Шифрлау алгоритмінің статистикалық қауіпсіздігін бағалау барысында NIST сынақтары жүргізілді. Статистикалық талдау жүргізу үшін NIST ұсынған арнайы Statistical Test Suite бағдарламалық жабдықтама қолданылды (3-сурет). Бұл бағдарламаны қолдану барысында NIST ұсынған 15 статистикалық сынақтар бойынша зерттелетін шифрмәтінді кездейсоқтыққа χ^2 (хи-квадрат) критерийлері бойынша зерттеліп P – мәні анықталынады, егер P – мәні < 1 болса шифрмәтін кездейсоқ алынған деп болжаймыз.



Сурет 3 – Statistical Test Suite бағдарламасы

EM Cipher шифрлау алгоритмі арқылы алынған 1000000 бит ұзындықтағы шифрмәтін және 128 блок ұзындық таңдап алынып кездейсоқтыққа тексерілді. Statistical Test Suite бағдарламасымен тексерудің ерекшелігі әрбір 15 статистикалық сынақтар бойынша P – мәндерін есептеп қана қоймай, C1-C10 аралық интервалға бөлу арқылы әрбір интервалға қандай мән түсетіндігін анықтайды. Бұл өз кезегінде шифрмәтіннің бір қалыпты үлестірілгендігін көрсетеді. Мысалы: C1 бағанасында 0.0-0.1 аралықтағы P – мәндері 14 рет, C2 бағанасында 0.1-0.2 аралықтағы P – мәндері 12 рет кездесетіндігі, ал proportion бөлімінде 128 блок ұзындықтың 127-і сәтті өткендігі көрсетілген. NIST талаптарына сай алынған зерттеулерге сәйкес A бағанадағы мәндері C мәнінен үлкен болса, ал B мәндері D мәндерінен үлкен болса сынақ сәтті өтті деп есептейміз. Зерттеу нәтижесі 4-суретте көрсетілген.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
14	12	14	17	13	9	12	11	16	10	0.804337	127/128	Frequency
12	16	15	14	10	5	11	15	12	18	0.299251	127/128	BlockFrequency
12	15	16	9	5	15	10	9	17	20	0.063482	128/128	CumulativeSums
14	10	10	11	14	15	19	12	12	11	0.706149	127/128	CumulativeSums
9	10	14	12	12	18	13	12	16	12	0.756476	128/128	Runs
14	14	13	11	8	18	10	15	10	15	0.602458	128/128	LongestRun
13	15	10	18	11	11	13	16	10	11	0.723129	127/128	Rank
10	15	14	5	15	13	13	11	15	17	0.407091	128/128	FFT
11	18	11	17	12	5	16	12	13	13	0.287306	127/128	NonOverlappingTemplate
11	8	7	13	16	15	13	13	14	18	0.422034	127/128	NonOverlappingTemplate
15	14	4	19	12	12	16	9	12	15	0.148094	126/128	OverlappingTemplate
15	12	10	13	19	10	12	7	20	10	0.148094	125/128	Universal
14	14	11	15	15	12	13	7	14	13	0.848588	127/128	ApproximateEntropy
6	5	13	10	3	16	4	10	7	6	0.021262	79/80	RandomExcursions
9	8	5	12	5	15	5	7	7	7	0.213309	80/80	RandomExcursions
8	9	11	6	7	8	11	6	11	3	0.559523	80/80	RandomExcursionsVariant
11	9	8	8	7	8	8	7	5	9	0.973388	80/80	RandomExcursionsVariant
15	12	15	16	13	9	15	14	12	7	0.654467	127/128	Serial
8	15	16	14	17	13	14	12	12	7	0.500934	128/128	Serial
12	13	12	15	15	11	12	20	10	8	0.468595	127/128	LinearComplexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 123 for a sample size = 128 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately = 76 for a sample size = 80 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

Сурет 4 – NIST сынақтар нәтижесі

функциянында ауытқу міндетті түрде қатыса бермейді – тек қайсысының ауытқуы жоғары функцияны таңдаймыз. Біздің жағдайда ЕМ функциясының ауытқуы жоғары болғандықтан дәл сол функцияны таңдаймыз. Сол себепті, 3-ші раундтан кейін анықтау ықтималдылығы 2^{-13} болады. Дәл осы тәртіппен зерттеу арқылы кілтті анықтау ықтималдықтар кестесін толтырамыз (Кесте 1).

Кесте 1 - Әр раундтағы кілтті анықтаудың ықтималдық нәтижесі

Раундтар №	Айырым ықтималдығы	Раундтар №	Айырым ықтималдығы	
1	кіріс	9	Кіріс	2^{-54}
	шығыс		Шығыс	2^{-63}
2	Кіріс	10	Кіріс	2^{-63}
	Шығыс		Шығыс	2^{-72}
3	Кіріс	11	Кіріс	2^{-72}
	Шығыс		Шығыс	2^{-81}
4	Кіріс	12	Кіріс	2^{-81}
	Шығыс		Шығыс	2^{-90}
5	Кіріс	13	Кіріс	2^{-90}
	Шығыс		шығыс	2^{-99}
6	Кіріс	14	Кіріс	2^{-99}
	Шығыс		Шығыс	2^{-108}
7	Кіріс	15	Кіріс	2^{-108}
	Шығыс		Шығыс	2^{-117}
8	Кіріс	16	Кіріс	2^{-117}
	шығыс		шығыс	2^{-126}

Енді осы зерттеулерге негізінде басқада белгілі блокты шифрлау алгоритмдерімен салыстырмалы талдаулар жүргізіліп, нәтижесі 2-кестеде көрсетілді.

Кесте 2 - Блокты шифрлардың дифференциалды талдауға қарсы тұру тұрақтылығы

Алгоритмдер	Блок өлшемі	Кілт ұзындығы	Раундтар саны	Дифференциалды талдауға қарсы тұрақтылығы	Кілтті табу ықтималдығы
Camellia 128	128 бит	128/192/256 бит	18/24	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$
AES 128	128 бит	128 бит	10	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$ – 2^{-254}
3 DES	64 бит	112/168 бит	48	Жақсы	Орташа $\approx 2^{-90}$
IDEA	64 бит	128 бит	8,5	Төзімді	Төмен $\approx 2^{-112}$
EM Chipper	128 бит	128 бит	16	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$

AES NIST стандарты ретінде бекітілген ең қауіпсіз блокты шифрлау алгоритм болып табылады. AES-тің AES-128, AES-192, AES-256 нұсқасы бар олардың барлығы дифференциалды шабуылдарға өте жоғары деңгейде төзімді. Кілтті табу ықтималдығы 2^{-126} -ден бастап 2^{-254} -ке дейін төмендейді. Қазіргі зертеулерде AES-ке қарсы дифференциалды шабуыл жүргізілген жоқ. Ал ұсынылып отырған EM Cipher алгоритміне осы аралыққа дейін басқада талдаулар жүргізіліп нәтижелері Scopus, комитет ұсынған журналдарға нәтижелері жарияланған. Бұл мақалада статистикалық зертеулері NIST ұсынған жаңа бағдарлама көмегімен зерттеліп нәтижелері алынды. Сонымен қатар әр раундтар бойынша дифференциалға төзімділік ықтималдылығы талданып, нәтижелері ұсынылған. Зерттеулер негізінде өте жоғары нәтиже көрсетілді.

Қорытынды.

Блокты шифрлау ақпараттарды сенімді қорғауда, әсіресе деректерді шифрлау, электронды байланыс цифрлық жүйелерді қорғау саласында кең қолданыста. Блокты шифрлардың өзектілігі төзімділігі жоғары, шифрлау жылдамдығы жоғары және әртүрлі қосымшаларға оңтайлы енгізілумен тығыз байланысты. Ұсынылған EM Cipher алгоритміне жан жақты талдаулар жүргізіліп, нәтижелері зерттелеген. Бұл мақалада алгоритмге дифференциалды талдау жүргізіліп нәтижелері ұсынылды. Алынған нәтижелерге сай EM Cipher алгоритмі жоғары дифференциалға төзімді екендігі айқындалды. Ұсынылған EM Cipher алгоритмін TLS/SSL, IPsec, VPN, Disk Encryption, Messaging apps (WhatsApp, Signal) т.б. қауіпсіздік хаттамаларында және құпия ақпараттарды рұқсат етілмеген пайдаланушылардан сенімді қорғау мақсатында қолдануға болады.

Әдебиеттер тізімі

1. Kapalova, N., & Naumen, A. (2018). The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. *Open Engineering*, 8(1), 140–146. <https://doi.org/10.1515/eng-2018-0013>
2. Nyssanbayeva, B. S., Kapalova, N., & Naumen, A. (2016). Modified symmetric block encryption-decryption algorithm based on modular arithmetic. *Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016)* (pp. 263–265).
3. Kapalova, N., Khompysh, A., Arici, M., & Algazy, K. (2020). A block encryption algorithm based on exponentiation transform. *Cogent Engineering*, 7(1). <https://doi.org/10.1080/23311916.2020.1788292>
4. Sabitha S, Binitha V Nair "Survey on Asymmetric Key Cryptographic Algorithms" *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, Volume 7, Issue 2, pp.404-408, doi : <https://doi.org/10.32628/IJSRSET207292>
5. Hasan, S. H., Trigui, M. S., & Ali Alquraishee, A. G. (2014). Block Cipher Based Cryptographic Algorithm For Data Security. *International journal of management & information technology*, 8(3), 1424–1429. <https://doi.org/10.24297/ijmit.v8i3.1978>
6. G., Renuka, Usha Shree V., and Chandra Sekhar Reddy P. "Comparison of AES and DES Algorithms Implemented on Virtex-6 FPGA and Microblaze Soft Core Processor." *International Journal of Electrical and Computer Engineering (IJECE)* 8, no. 5 (2018): 3544–49. <https://doi.org/10.11591/ijece.v8i5.pp3544-3549>.
7. Gaur, Paavni. "AES Image Encryption (Advanced Encryption Standard)." *International Journal for Research in Applied Science and Engineering Technology* 9, no. 12 (2021): 1357–63. <http://dx.doi.org/10.22214/ijraset.2021.39542>.
8. Kongsheng L, Yonghua Zh, Chunzhi M, and Jianhao Ch. 2024. Research on New Encryption Technology Based on SM4 Symmetry. In *Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition (IPMLP '24)*. Association for

Computing Machinery, New York, NY, USA, 459–463.
<https://doi.org/10.1145/3700906.3700979>

9. Babenko, Ludmila & Evgeniya, Ishchukova & Maro, Ekaterina. (2012). Research about strength of GOST 28147-89 encryption algorithm. pp.138-142. Doi:10.1145/2388576.2388595.

10. R.Biyashev, S. Nyssanbayeva, N.Kapalova, The Key Exchange Algorithm on Basis of Modular Arithmetic, Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong—Lancaster, U.S.A.: DEStech Publications, 2013, pp.16-21

11. Yang Z. Wireless sensor network security encryption based on AES module optimization design. *Journal of Computational Methods in Sciences and Engineering*. 2025;25(1):766-778. doi:[10.1177/14727978251321651](https://doi.org/10.1177/14727978251321651)

12. Chadi RIMAN, Pierre E. ABI-CHAR. Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. *Information Security and Computer Fraud*. Vol. 3, No. 1, 2015, pp 1-7. <https://pubs.sciepub.com/iscf/3/1/1>

13. Sharma, Mukta. (2016). Comparative Analysis of Block Key Encryption Algorithms. *International Journal of Computer Applications*. 145. 26-35. 10.5120/ijca2016910656.

14. Khompysh A., Algazy K., Kapalova N., Sakan K., & Dyusenbayev D. (2024). Statistical properties of the pseudorandom sequence generation algorithm. *Scientific Journal of Astana IT University*, 18, 107–119. <https://doi.org/10.37943/18LYCW2723>

15. Бабенко, Л. К., & Ищукова, Е. А. (2011). Дифференциальный криптоанализ алгоритма ГОСТ 28147-89. *Известия Южного федерального университета. Технические науки*, 125 (12), 120-130.

References

1. Kapalova, N., & Haumen, A. (2018). The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. *Open Engineering*, 8(1), 140–146. <https://doi.org/10.1515/eng-2018-0013>

2. Nyssanbayeva, B. S., Kapalova, N., & Haumen, A. (2016). Modified symmetric block encryption-decryption algorithm based on modular arithmetic. *Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016)* (pp. 263–265).

3. Kapalova, N., Khompysh, A., Arici, M., & Algazy, K. (2020). A block encryption algorithm based on exponentiation transform. *Cogent Engineering*, 7(1). <https://doi.org/10.1080/23311916.2020.1788292>

4. Sabitha S, Binitha V Nair "Survey on Asymmetric Key Cryptographic Algorithms" *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, Volume 7, Issue 2, pp.404-408, doi : <https://doi.org/10.32628/IJSRSET207292>

5. Hasan, S. H., Trigui, M. S., & Ali Alquraishee, A. G. (2014). Block Cipher Based Cryptographic Algorithm For Data Security. *International journal of management & information technology*, 8(3), 1424–1429. <https://doi.org/10.24297/ijmit.v8i3.1978>

6. G., Renuka, Usha Shree V., and Chandra Sekhar Reddy P. "Comparison of AES and DES Algorithms Implemented on Virtex-6 FPGA and Microblaze Soft Core Processor." *International Journal of Electrical and Computer Engineering (IJECE)* 8, no. 5 (2018): 3544–49. <https://doi.org/10.11591/ijece.v8i5.pp3544-3549>.

7. Gaur, Paavni. "AES Image Encryption (Advanced Encryption Standard)." *International Journal for Research in Applied Science and Engineering Technology* 9, no. 12 (2021): 1357–63. <http://dx.doi.org/10.22214/ijraset.2021.39542>.

8. Kongsheng L, Yonghua Zh, Chunzhi M, and Jianhao Ch. 2024. Research on New Encryption Technology Based on SM4 Symmetry. In *Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition (IPMLP '24)*. Association for Computing Machinery, New York, NY, USA, 459–463. <https://doi.org/10.1145/3700906.3700979>

9. Babenko, Ludmila & Evgeniya, Ishchukova & Maro, Ekaterina. (2012). Research about strength of GOST 28147-89 encryption algorithm. pp.138-142. Doi:10.1145/2388576.2388595.
10. R.Biyashev, S. Nyssanbayeva, N.Kapalova, The Key Exchange Algorithm on Basis of Modular Arithmetic, Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong—Lancaster, U.S.A.: DEStech Publications, 2013, pp.16-21
11. Yang Z. Wireless sensor network security encryption based on AES module optimization design. *Journal of Computational Methods in Sciences and Engineering*. 2025;25(1):766-778. doi:[10.1177/14727978251321651](https://doi.org/10.1177/14727978251321651)
12. Chadi RIMAN, Pierre E. ABI-CHAR. Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. *Information Security and Computer Fraud*. Vol. 3, No. 1, 2015, pp 1-7. <https://pubs.sciepub.com/iscf/3/1/1>
13. Sharma, Mukta. (2016). Comparative Analysis of Block Key Encryption Algorithms. *International Journal of Computer Applications*. 145. 26-35. 10.5120/ijca2016910656.
14. Khompysh A., Kapalova N., Algazy K., Dyusenbayev D., Sakan K. Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. *Cogent Engineering*, 2022, vol. 9 (1), pp. 1-14, <https://doi.org/10.1080/23311916.2022.2080623>
15. Khompysh A., Algazy K., Kapalova N., Sakan K., & Dyusenbayev D. (2024). Statistical properties of the pseudorandom sequence generation algorithm. *Scientific Journal of Astana IT University*, 18, 107–119. <https://doi.org/10.37943/18LYCW2723>
16. Babenko, L. K., & Ishchukova, E. A. (2011). Differential cryptanalysis of the algorithm GOST 28147-89. *Bulletin of the Southern Federal University. Technical sciences*, 125 (12), 120-130.

ИССЛЕДОВАНИЕ КРИПТОСТОЙКОСТИ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ «ЕМ СИПЕР»

Аннотация. Среди криптографических алгоритмов для надежной защиты конфиденциальной информации от несанкционированных пользователей используются алгоритмы блочного шифрования. Во многих странах установлены собственные стандарты алгоритмов блочного шифрования. Это, в свою очередь, позволяет обеспечить надёжную защиту информации. И это при том, что в Казахстане не утверждены стандарты на подобные алгоритмы защиты информации. Создание алгоритмов блочного шифрования и исследование их криптографической стойкости всегда являются одними из самых актуальных вопросов. В данной статье представлены результаты дифференциального и статистического анализа алгоритма блочного шифрования «EM Cipher». Одним из основных методов исследования стойкости алгоритмов блочного шифрования является статистический анализ стойкости. Если в ходе преобразований, обычно используемых в блочных шифрах, успешно реализовано хорошее смешивание и рассеивание, то можно добиться высокого уровня криптографической стойкости защиты алгоритма. Для проведения статистического анализа алгоритм был реализован программно и получены шифртексты различной длины. Согласно проведенным исследованиям статистический анализ предложенного алгоритма показал высокие результаты, то есть согласно требованиям, рекомендуемым NIST, было определено, что значения в столбце A больше значений в C, а значения в B больше значений в D. Результаты дифференциального анализа показали, что предложенный алгоритм обладает высокой криптографической стойкостью. То есть вероятность нахождения ключа из раунда 16 составляет 2^{-126} . Кроме того, в статье проведён сравнительный анализ результатов дифференциального анализа алгоритмов подписи, и установлено, что они показали сопоставимые результаты с известными алгоритмами Camellia 128 и AES 128. В будущих

работах будет проведено комплексное исследование криптографической стойкости других алгоритмов, а результаты будут представлены в виде статьи.

Ключевые слова. Блочный шифр, шифр, криптография, ключ, дифференциальный криптоанализ, статистический анализ, EM Chiper, S-блок.

STUDY OF CRYPTOCURRENCY OF THE BLOCK CIPHER ALGORITHM «EM CHIPER»

Abstract. Among cryptographic algorithms, block encryption algorithms are used to reliably protect confidential information from unauthorized users. Many countries have established their own standards for block encryption algorithms. This, in turn, ensures reliable protection of information. And this is despite the fact that in Kazakhstan, standards for such information protection algorithms have not been approved. There, the creation of block encryption algorithms and the study of their cryptographic strength are always among the most pressing issues. This article presents the results of differential and statistical analysis of the block encryption algorithm «EM Chiper». One of the main methods for studying the strength of block encryption algorithms is statistical analysis of strength. If good mixing and diffusion is successfully implemented during the transformations commonly used in block ciphers, then a high level of cryptographic security of the algorithm can be achieved. To conduct statistical analysis, the algorithm was implemented in software and ciphertexts of various lengths were obtained. According to the conducted research, the statistical analysis of the proposed algorithm showed high results, that is, according to the requirements recommended by NIST, it was determined that the values in column A are greater than the values in C, and the values in B are greater than the values in D. The results of the differential analysis showed that the proposed algorithm has high cryptographic strength. That is, the probability of finding the key from round 16 is 2^{-126} . In addition, the article conducted a comparative analysis of the results of the differential analysis of signature algorithms, and found that they showed comparable results with the well-known Camellia 128 and AES 128 algorithms. In future works, a comprehensive study of the cryptographic strength of other algorithms will be conducted, and the results will be presented in the form of an article.

Keywords. Block cipher, cipher, cryptography, key, differential cryptanalysis, statistical analysis, EM Chiper, S-block.

Авторлар туралы мәлімет

Хомпыш Ардабек	PhD, Нұр-Мұбарак Египет ислам мәдениеті университеті, Алматы, Қазақстан, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: ardabek@mail.ru
Сақан Қайрат Сақанұлы	PhD, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: kairat_sks@mail.ru
Алғазы Күнболат	PhD, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: kunbolat@mail.ru
Абишева Ақмарал Жолсеитовна	Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан, аға оқытушы, E-mail: ak_maral@mail.ru

Сведения об авторах

Хомпыш Ардабек	PhD, Египетский университет исламской культуры «Нур-Мубарак», Алматы, Казахстан, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: ardabek@mail.ru
Сақан Қайрат	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kairat_sks@mail.ru
Алғазы Кунболат	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kunbolat@mail.ru
Абишева Ақмарал Жолсеитовна	Казахский национальный педагогический университет имени Абая, Алматы, Казахстан, старший преподаватель, E-mail: ak_maral@mail.ru

Information about the authors

Khomysh Ardabek	PhD, Egyptian University of Islamic Culture "Nur-Mubarak", Almaty, Kazakhstan, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: ardabek@mail.ru
Sakan Kairat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kairat_sks@mail.ru
Algazy Kunbolat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kunbolat@mail.ru
Abisheva Akmaral Zh.	Kazakh National Pedagogical University named after Abaya, Almaty, Kazakhstan, senior lecturer, E-mail: ak_maral@mail.ru



УДК 004.932.2

МРНТИ 28.23.15

https://doi.org/10.53364/24138614_2025_38_3_8

З.Г. Кабдрахманова^{1*}, А.С. Тлебалдинова¹, М.А.Карменова², С.К. Кумаргажанова¹,
И.Б. Карымсакова³

¹Восточно-Казахстанский технический университет им. Д. Серикбаева,
Усть-Каменогорск, Казахстан

² Восточно-Казахстанский университет им. С.Аманжолова, Усть-Каменогорск, Казахстан

³Университет имени Шакарима города Семей, Семей, Казахстан

*E-mail: zkabdrahmanova@vku.edu

ПРИМЕНЕНИЕ ТЕКСТУРНОГО АНАЛИЗА ПРИ КЛАССИФИКАЦИИ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ

Аннотация. В современной медицине анализ текстурных признаков изображений играет важную роль в диагностике различных заболеваний. Данное исследование посвящено методам классификации текстурных признаков изображений ожоговых поражений, позволяющим выделять информативные характеристики и повышать точность диагностики. Рассмотрены современные алгоритмы машинного обучения, применяемые для автоматизированного анализа изображений. Проведен сравнительный анализ различных методов классификации, выявлены наиболее эффективные подходы к обработке текстурных признаков. Результаты исследования могут быть использованы для разработки интеллектуальных систем поддержки принятия врачебных решений. В исследовании использован набор данных, включающий 1500 изображений ожоговых поражений, полученных из открытых источников Roboflow и Kaggle. Для выделения текстурных признаков применена программа MaZda, обеспечивающая детальный анализ изображений. Исходный массив, содержащий 279 признаков, был оптимизирован путем выбора наиболее информативных характеристик с использованием шести методов: ANOVA, Fisher, Relief, SBS, SFS и RFE, что позволило сократить их количество до 21. Проведен обзор современных подходов к автоматизированному анализу ожогов, включая методы обработки изображений и машинного обучения, опубликованных за последние пять лет. Работа демонстрирует перспективность применения машинного обучения в медицине и необходимость дальнейших исследований для повышения точности классификации и практического внедрения разработанных алгоритмов.

Ключевые слова: текстурные признаки, MaZda, автоматизированный анализ ожогов, медицинская диагностика, обработка изображений, классификация ожогов.

Введение.

Современные методы диагностики ожогов требуют высокой точности и объективности при определении степени тяжести повреждений кожи. Врачебная оценка, основанная на визуальном осмотре, может быть субъективной и зависеть от опыта специалиста. В связи с этим актуальной задачей является разработка автоматизированных информационных систем, использующих методы компьютерного зрения и машинного обучения для классификации ожогов. Автоматическое распознавание степени тяжести ожогов на основе изображений позволяет повысить скорость и точность диагностики, что

особенно важно для своевременного выбора тактики лечения. Одним из перспективных направлений является анализ текстурных характеристик поврежденных участков кожи, поскольку текстурные признаки несут значимую информацию о структуре ткани и степени ее поражения.

В данном исследовании рассматривается подход к автоматизированной классификации ожогов по трем степеням тяжести на основе анализа текстурных признаков, вычисленных с использованием программного обеспечения MAZDA. Для отбора наиболее информативных признаков применяются методы фильтрации: ANOVA, Fisher, Relief, а также методы оболочки: SBS, SFS и RFE.

Цель исследования – разработать и обосновать эффективный подход к автоматизированной диагностике ожоговых поражений на основе анализа текстурных признаков изображений, используя методы отбора признаков для повышения точности и интерпретируемости классификации. Исследование направлено на определение наиболее информативных признаков для классификации ожоговых поражений, снижение размерности признакового пространства и улучшение работы алгоритмов машинного обучения в задачах медицинской диагностики.

Научная новизна этого исследования заключается в адаптации конфигурации и гиперпараметров модели и алгоритмов машинного обучения для определения наилучшей стратегии классификации с целью повышения точности классификации ожоговых поражений.

За последние пять лет было проведено множество исследований, посвященных применению методов машинного обучения в медицинской диагностике, включая анализ изображений ожогов. Рассмотрим основные направления, связанные с данной тематикой. Методы машинного обучения и компьютерного зрения находят широкое применение в медицинской визуализации, включая диагностику кожных заболеваний, таких как ожоги. В исследовании Веденичева Д.А. рассматривается использование нейронных сетей для сегментации и классификации кожных патологий на основе фотографий пациентов [1]. Однако нейросетевые алгоритмы требуют значительных объемов данных и высоких вычислительных мощностей, что затрудняет их интеграцию в клиническую практику. Текстуальный анализ активно применяется для диагностики кожных и других заболеваний. Одним из распространенных инструментов для работы с текстурными признаками является программа MAZDA, включающая широкий спектр методов статистического анализа изображений. В исследовании Венцека Ю.К. рассматриваются подходы к сегментации изображений с использованием текстурных характеристик, а также проводится оценка их эффективности на реальных медицинских данных [2].

В задачах медицинской диагностики важную роль играет отбор наиболее информативных признаков, позволяющий избежать переобучения моделей. Методы фильтрации, такие как ANOVA, Fisher и Relief, позволяют выявить наиболее значимые для классификации признаки. В работе Настенко Е. анализируется использование текстурных характеристик в задачах классификации медицинских изображений, а также исследуется влияние различных методов отбора признаков на точность моделей [3]. Методы оболочки, включая SBS, SFS и RFE, позволяют формировать оптимальные подмножества признаков, способствующие повышению эффективности классификации.

Следующее исследование [4] посвящено разработке автоматизированной системы анализа ожоговых ран, включающей три ключевых этапа: сегментацию изображений, извлечение признаков и классификацию областей. Авторы рассматривают различные методы на каждом этапе, стремясь определить их оптимальную комбинацию. В качестве одного из подходов была применена семантическая сегментация на основе глубокой нейросети SegNet. Результаты экспериментов показали, что наиболее эффективной комбинацией методов является использование нечеткого алгоритма *c-means* для сегментации и многослойной искусственной нейронной сети прямого распространения,

обученной методом обратного распространения, для классификации. Данный подход позволил достичь F-оценки 74,28% при анализе изображений, полученных без специального протокола. В то же время метод глубинного обучения продемонстрировал несколько более высокую точность с F-оценкой 80,50%. Таким образом, предложенный алгоритм классификации оказался сопоставимым с глубоким обучением, что делает его перспективным для автоматизированного анализа ожоговых поражений.

Ультразвуковая диагностика, являясь неинвазивным методом визуализации, широко применяется для выявления патологий печени. Важным направлением исследований является анализ текстурных характеристик и классификация ультразвуковых изображений печени. В данном [5] исследовании для обработки изображений сначала была использована матрица совместного встречаемого градиента серых уровней (GLGCM), а затем – матрица совместного встречаемого уровня серого (GLCM). Эти методы позволили выделить 22 признака, из которых были отобраны семь наиболее информативных для дальнейшей классификации с использованием нейронной сети обратного распространения ошибок (BP). В рамках исследования фиброз печени классифицировался по пяти стадиям (S0-S4), при этом точность классификации составила 100% для S0 и S4, 90% для S1 и S3, а также 70% для S2.

Исследователи Cirillo и его коллеги [6] использовали сверточные нейронные сети (CNN) для прогнозирования прогрессирования ран и улучшения результатов лечения ожогов. Они проанализировали параметры цветового изображения трех типов глубоких термических повреждений, полученные путем оценки изображений здоровой кожи и фона. После обучения CNN средняя точность, чувствительность и специфичность для четырех типов ожогов составили 90,54%, 74,35% и 94,25% соответственно. Таким образом, в настоящем исследовании делается акцент на использовании текстурных признаков, отобранных методами фильтрации, для обучения традиционных моделей машинного обучения, что позволяет достичь высокой точности при классификации ожогов.

В работе [7] Щетинина и соавторов предложен подход к обнаружению злокачественных новообразований кожи на основе анализа дерматоскопических изображений с использованием методов глубокого обучения. Разработанная архитектура глубокой сверточной нейронной сети была применена к обработке дерматоскопических изображений различных повреждений кожи, что обеспечило точность на тестовой выборке 94%.

Использование моделей глубокого обучения при решении вышеупомянутых проблем, связанных с ожогами, также обсуждается в следующей работе [8]. Авторы рассматривают использование глубоких сверточных нейронных сетей (CNN) в машинном обучении для автоматического прогнозирования глубины ожога. В исследовании использовались цветные изображения четырех типов глубины ожогов, снятые камерой TiVi, и четыре предварительно обученные глубокие сверточные нейронные сети: VGG-16, GoogleNet, ResNet-50 и ResNet-101. Наилучшие результаты были достигнуты при использовании модели ResNet-101, которая показала точность 81,66% и другие показатели, такие как чувствительность и специфичность.

Это исследование подтверждает, что искусственный интеллект может быть полезным инструментом для прогнозирования глубины ожогов и оказания помощи в принятии клинических решений и первичном лечении ожоговых ран. Аналогичным образом, исследование [9] из цитируемой работы показывает, что тонкая настройка всех слоев дает лучшие результаты, чем тонкая настройка только верхних слоев, и доказано, что время, необходимое для тонкой настройки всех слоев, на самом деле меньше времени, необходимого для тонкой настройки только верхних слоев. Это объясняется тем, что при настройке всех слоев было выполнено всего 20 эпох, тогда как при настройке только верхних слоев количество эпох составило 30. Если бы настройка верхних слоев не была завершена в течение 30 эпох, достигнутые результаты были бы неудовлетворительными.

Это наблюдение говорит о том, что более глубокая настройка всей модели не только обеспечивает более высокое качество конечного результата, но и способствует более быстрой сходимости модели, чем настройка только верхних слоев.




Эти подходы демонстрируют эффективность использования современных технологий, таких как глубокое обучение и текстурные анализы медицинских изображений для диагностики и оценки тяжести ожогов кожи, расширяя возможности медицинской диагностики и улучшая результаты лечения пациентов.

Материалы и методы исследования.

Для обучения и тестирования моделей использовался набор изображений ожогов, включающий 1500 изображений, разделенных на три класса по 500 изображений в каждом. Изображения были получены из открытых источников, включая медицинские базы данных и доступные научные публикации, что обеспечило разнообразие данных и их соответствие реальным клиническим условиям. При анализе текстуры тканей важно свести к минимуму процедуры предварительной обработки, чтобы сохранить естественные особенности изображений. Все изображения стандартизированы по освещению и углу съемки, чтобы минимизировать влияние внешних факторов.

Классификация ожогов осуществлялась по трем степеням тяжести, представленных в таблице 1.

Таблица 1 – Степень тяжести ожогов и их признаки

№	Степень тяжести ожогов	Признаки	Изображение
1	I степень	поверхностные ожоги, затрагивающие только эпидермис	
2	II степень	поражение эпидермиса и частично дермы	
3	III степень	глубокие ожоги, затрагивающие все слои кожи и подкожную клетчатку	

Текстурные признаки были вычислены с использованием программы MAZDA, которая позволяет извлекать статистические характеристики изображений. Всего было получено 279 признаков, включающих: Матрицу совместной встречаемости уровней серого (GLCM) – параметры контрастности, однородности, энтропии и корреляции; Статистические моменты первого и второго порядка; Вейвлет-преобразование; Гистограммы распределения интенсивностей пикселей.

Области интереса выделялись путем наложения выбранных вручную цветных областей на полутоновое изображение (см. таб. 1). Можно определить до 16 профилей областей интереса, используя 16 уникальных цветов. Анализ с помощью программы MaZda выполняется в пределах этих областей интереса. После применения методов отбора признаков из 279 параметров были отобраны 21 наиболее информативных признаков, обеспечивающих наилучшую классификацию. Это позволило снизить вычислительную сложность и повысить точность моделей машинного обучения. Для сокращения размерности признакового пространства применялись шесть методов:

- Методы статистического тестирования: Anova (дисперсионный анализ) – анализ значимости различий между классами; Fisher – оценка соотношения межклассовой и внутриклассовой дисперсий; Relief – оценка значимости признаков на основе расстояния до ближайших соседей.

- Методы оболочки (wrapper methods): SBS (Sequential Backward Selection) – последовательное удаление наименее значимых признаков; SFS (Sequential Forward Selection) – последовательное добавление наиболее значимых признаков; RFE (Recursive Feature Elimination) – рекурсивное удаление признаков на основе их важности, оцениваемой с использованием модели, что помогает выявить наиболее информативные признаки. Средние значения параметров рассчитаны для обучающей и тестовой выборок. Процедура селекции признаков осуществлена с применением шести методов. Результаты выделенных признаков представлены в таблице 2

Таблица 2 – Средние значения параметров и результаты селекции признаков для обучающей и тестовой выборок

Обучающий набор		Тестовый набор	
Название признака	Среднее значение признака	Название признака	Среднее значение признака
Mean	-0.000000061	Mean	0.016216035
Variance	0.000000005	Variance	0.012079924
Skewness	0.000000003	Skewness	-0.023899715
Kurtosis	0.000000017	Kurtosis	0.018523313
Perc.01%	-0.000000244	Perc.01%	0.000204855
S(1,0)AngScMom	0.000000026	S(1,0)AngScMom	-0.02420533
S(0,1)Contrast	-0.000000029	S(0,1)Contrast	-0.065411258
S(0,1)Correlat	0.000000005	S(0,1)Correlat	0.080724801
S(1,0)Contrast	-0.000000003	S(1,0)Contrast	-0.081832485
S(1,0)Correlat	0.000000003	S(1,0)Correlat	0.108972243
S(1,0)InvDfMom	0.000000014	S(1,0)InvDfMom	0.065677647
Horzl_GLevNonU	0.000000017	Horzl_GLevNonU	-0.079309261
Horzl_LngREmph	-0.000000009	Horzl_LngREmph	-0.064593038
Vertl_GLevNonU	-0.000000022	Vertl_GLevNonU	-0.036143453
Vertl_LngREmph	0.000000018	Vertl_LngREmph	-0.042272361
Teta1	-0.000000041	Teta1	0.049204005
Teta2	0.000000065	Teta2	-0.013152038
Teta3	0.000000057	Teta3	-0.036801371
WavEnHH_s-1	0.000000030	WavEnHH_s-1	-0.0528722
WavEnHL_s-4	-0.000000015	WavEnHL_s-4	0.002418665
WavEnLH_s-4	0.000000015	WavEnLH_s-4	-0.042384786

Отбор признаков позволит уменьшить количество используемых параметров, повысив эффективность классификации и снизив вероятность переобучения.

Процедура реализации классификации изображения при ожоговых поражениях представлена на рисунке 1.

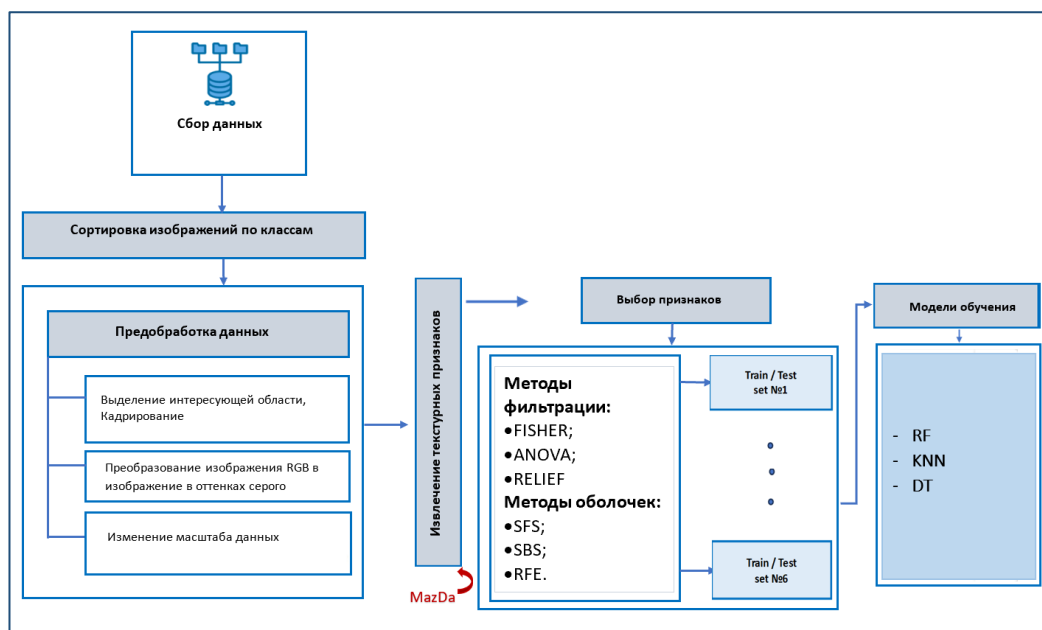


Рисунок 1 – Схема процедуры реализации классификации изображения при ожоговых поражениях

Обучающая выборка составляла 70% от общего объема данных, а тестовая - 30%. Процесс обучения и тестирования классификаторов выполнялся дважды, после чего рассчитывалось среднее значение всех тестов в качестве итогового результата. Для каждого набора данных формировались два обучающих и два тестовых поднабора с использованием метода случайной выборки с возвращением. В исследовании были задействованы три широко применяемых метода обучения: K-Nearest Neighbors (KNN) – метод ближайших соседей, работающий на основе вычисления расстояний между объектами; Discriminant Analysis (DR) – метод дискриминантного анализа, определяющий границы классов; Random Forest (RF) – ансамблевый метод на основе деревьев решений, демонстрирующий высокую устойчивость к шуму в данных. Для оценки качества моделей использовались метрики: Accuracy – Точность (общая доля правильно классифицированных объектов); Precision – Прецизионность (доля истинно положительных предсказаний среди всех положительных предсказаний); Recall – Полнота (доля истинно положительных предсказаний среди всех фактических положительных объектов).

Результаты и обсуждение.

После проведения обучения и тестирования моделей машинного обучения на изображениях ожоговых поражений были получены количественные показатели их эффективности. В таблице 3 представлен сравнительный анализ точности классификации различных алгоритмов на основе метрик.

Таблица 3 – Сравнительный анализ точности классификации

Модель	Accuracy(%)	Precision(%)	Recall(%)
KNN	71.2	70.5	69.8
DR	73.5	72.8	73.2
RF	79.0	78.5	78.9

Модель Random Forest (RF) показала наивысшую точность (79%), что объясняется ее способностью эффективно работать с высокоразмерными признаковыми пространствами и учитывать сложные зависимости в данных.

Для повышения точности классификации ожогов по степени тяжести использовалась настройка гиперпараметров с применением методов Grid Search и Random Search на основе 5-кратной кросс-валидации. Рассмотрим детально, какие параметры изменялись и какие значения давали наилучшие результаты. Результаты, полученные в процессе оптимизации гиперпараметров моделей на основе оценочных метрик, представлены в таблице 4.

Таблица 4 – Результат после настраивания гиперпараметров метрик

№	Методы	Настраиваемые параметры:	Результат:
1	Метод k-ближайших соседей (K-Nearest Neighbors, KNN)	<p>Число соседей (k): варьировалось от 3 до 15 с шагом 2. Оптимальное значение: $k = 7$ (баланс между переобучением и недообучением). Метрика расстояния: Евклидово (L2), Манхэттенское (L1), Минковского (p=3). Оптимальный выбор: Евклидово расстояние (показало лучшую классификацию). Веса соседей: Равномерные, обратно пропорциональные расстоянию. Оптимальный выбор: обратные веса (дают большую значимость ближайшим объектам).</p>	<p>Без настройки: Точность ~67% После оптимизации гиперпараметров: Точность ~72%</p>
2	Дерево решений (Decision Tree, DT)	<p>Максимальная глубина дерева: Значения: от 5 до 30 (с шагом 5). Оптимальное значение: 15 (сбалансированное разбиение). Критерий разбиения: Gini, Энтропия. Оптимальный выбор: Gini (давал меньшую вариативность в разбиениях). Минимальное количество объектов в листе: От 1 до 10 (шаг 2). Оптимальное значение: 5 (устраняет переобучение).</p>	<p>Без настройки: Точность ~60% После оптимизации гиперпараметров: Точность ~70%</p>
3	Случайный лес (Random Forest, RF)	<p>Число деревьев в ансамбле: Варьировалось от 50 до 500 с шагом 50. Оптимальное значение: 300 деревьев (баланс между скоростью и точностью). Максимальная глубина деревьев: От 10 до 50 (шаг 5). Оптимальное значение: 25 (дальнейшее увеличение не давало прироста точности). Максимальное число признаков при разбиении: Варианты: sqrt (квадратный корень от числа признаков), log2, все признаки. Оптимальный выбор: sqrt (баланс между вычислительной эффективностью и точностью). Критерий разбиения: Gini, Энтропия. Оптимальный выбор: Gini (показал лучшую точность на кросс-валидации).</p>	<p>Без настройки: Точность ~72% После оптимизации гиперпараметров: Точность ~79% (лучший результат среди всех моделей).</p>

Выводы по настройке гиперпараметров:

- Случайный лес (RF) с 300 деревьями и глубиной 25 показал наивысшую точность — 79%.
- Методы KNN и DT показали улучшение после настройки, но не превзошли RF.

Подбор гиперпараметров проводился через Grid Search и Random Search на 5-кратной кросс-валидации, что помогло избежать переобучения. Всего в результате анализа изображений было извлечено 279 дескрипторов текстур. Затем уменьшение размерности было выполнено с использованием метода выбора шести признаков. В таблице 5 продемонстрированы лучшие результаты, полученные каждым методом.

Таблица 5 – Результат применения методов классификации и оценки точности модели

Название модели	Метод отбора	Метод классификации	Оценка точности	Оптимальное количество характеристик
MODEL_19_FISHER_RF	FISHER	RF	0.79	19
MODEL_7_FISHER_KNN		KNN	0.74	7
MODEL_7_FISHER_DT		DT	0.73	7
MODEL_13_ANOVA_RF	ANOVA	RF	0.78	13
MODEL_8_ANOVA_KNN		KNN	0.74	8
MODEL_17_ANOVA_DT		DT	0.74	17
MODEL_18_RFE_RF	RFE	RF	0.78	18
MODEL_11_RFE_KNN		KNN	0.75	11
MODEL_18_RFE_DT		DT	0.73	18
MODEL_20_RELIEF_RF	RELIEF	RF	0.79	20
MODEL_18_RELIEF_KNN		KNN	0.75	18
MODEL_20_RELIEF_DT		DT	0.73	20
MODEL_20_SFS_RF	SFS	RF	0.79	20
MODEL_6_SFS_KNN		KNN	0.74	6
MODEL_16_SFS_DT		DT	0.74	16
MODEL_18_SBS_RF	SBS	RF	0.79	18
MODEL_7_SBS_KNN		KNN	0.75	7
MODEL_9_SBS_DT		DT	0.73	9

Анализ влияния методов отбора признаков показал, что применение ANOVA и Fisher позволило повысить точность моделей на 3-5% по сравнению с использованием всех признаков. Методы оболочки SBS и Relief показали наилучший баланс между размерностью признакового пространства и точностью классификации, что делает их предпочтительными для данной задачи.

Заключение.

В рамках данного исследования был разработан подход для автоматической классификации ожогов по степени тяжести на основе анализа текстурных признаков. В ходе исследования были извлечены текстурные характеристики с применением программы MAZDA, что позволило учитывать характеристики структуры тканей. Проведен анализ эффективности различных методов отбора признаков, при котором наилучшие и одинаковые результаты продемонстрировали SBS и Relief. Подтверждена высокая результативность текстурного анализа в диагностике ожогов путем сопоставления полученных данных с результатами других исследований. Обучены и протестированы три модели машинного обучения (KNN, DR, RF), где Random Forest достиг максимальной точности 79%.

Перспективы дальнейших исследований заключаются в интеграции сверточных нейронных сетей (CNN) с текстурными признаками, расширении датасета за счет включения данных из различных источников, а также применении методов, повышающих интерпретируемость моделей.

Список литературы

1. Веденичев, Д.А., Лавриченко, О.А. (2022). Применение нейронных сетей для сегментации и классификации кожных заболеваний на основе фотоснимков человека

[Электронный ресурс]. – Режим доступа: <https://elib.spbstu.ru/dl/3/2022/vr/vr22-2804.pdf/info>

2. Венцек, Ю.К. (2023). Сегментация изображений на основе текстурных признаков // Электронные системы и технологии: материалы 59-й научной конференции аспирантов, магистрантов и студентов БГУИР. -Минск: БГУИР, 95–96. URL: <https://libeldoc.bsuir.by/handle/123456789/51401>

3. Настенко, Е. (2020). Применение текстурного анализа в задаче классификации медицинских изображений [Электронный ресурс]. – Режим доступа: <https://www.academia.edu/95767470>.

4. Rowland, R., Ponticorvo, A., Baldado, M., Kennedy, G., Burmeister, D., Christy, R., Bernal, N., Durkin, A. (2019). Burn wound classification model using spatial frequency-domain imaging and machine learning. *Journal of biomedical optics*; 24(5):1-9. DOI: 10.1117/1.JBO.24.5.056007.

5. Gao Shuang, Peng Yuhua, Guo Huizhi, Liu Weifeng, Gao Tianxin, Xu Yuan-qing, Tang Xiaoying (2019). Texture analysis and classification of ultrasound liver images. *Bio-medical materials and engineering*; 24(1):1209-16. DOI: 10.3233/BME-130922.

6. Cirillo, M.D., Mirdell, R., Sjöberg, F. (2019). Time-independent prediction of burn depth using deep convolutional neural networks // *Journal of Burn Care & Research*; (6). 857-863.

7. Щетинин, Е.Ю., Севастьянов, Л.А., Демидова, А.В., Кулябов, Д.С. (2020). Классификация повреждений кожи по данным дермаскопии с использованием методов глубокого обучения. *Математическая биология и биоинформатика*. 15, (№2). 180–194. DOI: 10.17537/2020.15.180.

8. Chang, C.W., Ho, C.Y., Lai, F., Christian, M., Huang, S.C., Chang, D.H., Chen, Y.S. (2023). Application of multiple deep learning models for automatic burn wound assessment. *Burns*; 49(5):1039-1051. DOI: 10.1016/j.burns.2022.07.006. Epub 2022 Jul 18. PMID: 35945064.

9. Chen, L.C., Zhu, Y., Papandreou, G., Schroff, F., Adam, H. (2018). Encoder-decoder with atrous separable convolution for semantic image segmentation // *European Conference on Computer Vision February, Computer Science*. DOI:10.1007/978-3-030-01234-2_49

References

1. Vedenichev, D.A., Lavrichenko, O.A. (2022). Primenenie nejronnyh setej dlja segmentacii i klassifikacii kozhnyh zabolevanij na osnove fotosnimkov cheloveka [Jelektronnyj resurs]. – Rezhim dostupa: <https://elib.spbstu.ru/dl/3/2022/vr/vr22-2804.pdf/info>

2. Vencek, Ju.K. (2023). Segmentacija izobrazhenij na osnove teksturnyh priznakov // Jelektronnye sistemy i tehnologii: materialy 59-j nauchnoj konferencii aspirantov, magistrantov i studentov BGUIR, Minsk: BGUIR. 95–96; URL: <https://libeldoc.bsuir.by/handle/123456789/51401>

3. Nastenko, E. (2020). Primenenie teksturnogo analiza v zadache klassifikacii medicinskih izobrazhenij [Jelektronnyj resurs]. – Rezhim dostupa: <https://www.academia.edu/95767470>.

4. Rowland, R., Ponticorvo, A., Baldado, M., Kennedy, G., Burmeister, D., Christy, R., Bernal, N., Durkin, A. (2019). Burn wound classification model using spatial frequency-domain imaging and machine learning // *Journal of biomedical optics*; 24(5):1-9. DOI: 10.1117/1.JBO.24.5.056007.

5. Gao Shuang, Peng Yuhua, Guo Huizhi, Liu Weifeng, Gao Tianxin, Xu Yuan-qing, Tang Xiaoying (2019). Texture analysis and classification of ultrasound liver images. *Bio-medical materials and engineering*; 24(1):1209-16. DOI: 10.3233/BME-130922.

6. Cirillo, M.D., Mirdell R., Sjöberg F. (2019). Time-independent prediction of burn depth using deep convolutional neural networks // *Journal of Burn Care & Research*; (6). 857-863.

7. Shhetinin E.Ju., Sevast'janov, L.A., Demidova, A.V., Kuljabov, D.S. (2020). Klassifikacija povrezhdenij kozhi po dannym dermaskopii s ispol'zovaniem metodov glubokogo

obuchenija. *Matematicheskaja biologija i bioinformatika*. 15, (2). 180–194. DOI: 10.17537/2020.15.180.

8. Chang, CW, Ho CY., Lai, F., Christian M, Huang, S.C., Chang, D.H., Chen, Y.S. (2023). Application of multiple deep learning models for automatic burn wound assessment. *Burns*; 49(5):1039-1051. DOI: 10.1016/j.burns.2022.07.006. Epub 2022 Jul 18. PMID: 35945064.

9. Chen, L.C., Zhu, Y., Papandreou, G., Schroff, F., Adam, H. (2018). Encoder-decoder with atrous separable convolution for semantic image segmentation // European Conference on Computer Vision February, Computer Science. DOI:10.1007/978-3-030-01234-2_49

МЕДИЦИНАЛЫҚ БЕЙНЕЛЕРДІ КЛАССТАРҒА ЖІКТЕУДЕ ТЕКСТУРАЛЫҚ ТАЛДАУДЫ ҚОЛДАНУ

Аңдатпа. Қазіргі заманғы медицинада кескіндердің текстуралық ерекшеліктерін талдау әртүрлі ауруларды диагностикалауда маңызды рөл атқарады. Бұл зерттеу ақпараттық сипаттамаларды анықтауға және диагностикалық дәлдікті арттыруға мүмкіндік беретін күйік жарақаттары кескіндерінің текстуралық ерекшеліктерін жіктеу әдістеріне арналған. Кескінді автоматтандырылған талдау үшін қолданылатын қазіргі заманғы машиналық оқыту алгоритмдері қарастырылады. Әртүрлі жіктеу әдістеріне салыстырмалы талдау жүргізіліп, текстураның ерекшеліктерін өңдеудің ең тиімді тәсілдері анықталды. Зерттеу нәтижелерін медициналық шешім қабылдауды қолдау үшін интеллектуалды жүйелерді әзірлеу үшін пайдалануға болады. Зерттеуде Roboflow, Kaggle ашық көздерден алынған 1500 дана күйіктердің кескіндері (әр класс үшін 500 данадан) пайдаланылды. Әрі қарай жіктеу үшін MaZda бағдарламасы арқылы алынған текстуралық ерекшеліктер пайдаланылды. Бастапқыда 279 ерекшелік анықталды, оның ішінде 6 таңдау әдістерін: ANOVA, Фишер, Рельеф, SBS, SFS және RFE қолдану арқылы 21 маңызды ерекшелік таңдалды. Соңғы бес жылда жарияланған күйіктерді автоматтандырылған талдаудың заманауи тәсілдеріне шолу жасалды, оның ішінде кескіндерді өңдеу және машиналық оқыту әдістері. Жұмыс медицинадағы машиналық оқытудың әлеуетін және классификация дәлдігін және әзірленген алгоритмдерді практикалық енгізуді жақсарту үшін одан әрі зерттеу қажеттілігін көрсетеді.

Түйін сөздер: текстураның ерекшеліктері, MaZda, автоматтандырылған күйік талдауы, медициналық диагностика, кескінді өңдеу, күйік классификациясы.

APPLICATION OF TEXTURE ANALYSIS IN MEDICAL IMAGE CLASSIFICATION

Abstract. In modern medicine, the analysis of texture features of images plays an important role in the diagnosis of various diseases. This study is devoted to the methods of classifying texture features of burn injury images, which allow identifying informative characteristics and increasing the accuracy of diagnosis. Modern machine learning algorithms used for automated image analysis are considered. A comparative analysis of various classification methods is carried out, the most effective approaches to processing texture features are identified. The results of the study can be used to develop intelligent systems to support medical decision-making. The study used 1,500 burn images (500 for each class) obtained from open sources Roboflow, Kaggle. Texture features extracted using MaZda software were used for further classification. Initially, 279 features were extracted, from which 21 most significant features were selected using 6 selection methods: ANOVA, Fisher, Relief, SBS, SFS and RFE. A review of current approaches to automated burns analysis, including image processing and machine learning methods, published in the last five years is performed. The work demonstrates the promising application of machine learning in medicine and the need for further research to improve classification accuracy and practical implementation of the developed algorithms.

Keywords: *texture features, MaZda, automated burn analysis, medical diagnosis, image processing, burn classification.*

Сведение об авторах

Кабдрахманова Зауре Гадьльжановна	Докторант 2 года обучения ОП 8D06101 – «Информационные системы (по отраслям)» Школы информационных технологий и интеллектуальных систем Восточно-Казахстанского технического университета имени Д. Серикбаева, г. Усть-Каменогорск, Казахстан, E-mail: zkabdrahmanova@vku.edu
Тлебалдинова Айжан Солтангалиевна	PhD, ассоциированный профессор Школы информационных технологий и интеллектуальных систем Восточно-Казахстанского технического университета имени Д. Серикбаева, г. Усть-Каменогорск, Казахстан, E-mail: atlebaldinova@edu.ektu.kz
Карменова Мархаба Ахметоллиновна	PhD, ассоциированный профессор Восточно-Казахстанского университета имени С. Аманжолова, Усть-Каменогорск, Казахстан, E-mail: mkarmenova@vku.edu.kz
Кумаргажанова Сауле Кумаргажановна	Кандидат технических наук, профессор Школы информационных технологий и интеллектуальных систем Восточно-Казахстанского технического университета имени Д. Серикбаева, г. Усть-Каменогорск, Казахстан, E-mail: saule.kumargazhanova@edu.ektu.kz
Карымсакова Индира Бекеновна	PhD, и.о. ассоциированного профессора кафедры «IT технологии», Некоммерческое акционерное общество «Шәкәрім университет», Семей, Республика Казахстан, E-mail: karymsakova.indira@mail.ru

Авторлар туралы мәлімет

Кабдрахманова Зауре Гадьльжановна	Д.Серікбаев атындағы Шығыс Қазақстан техникалық университетінің Ақпараттық технологиялар және зияткерлік жүйелер мектебінің 8D06101 – «Ақпараттық жүйелер (салалар бойынша)» БББ 2 оқу жылындағы докторанты, Өскемен қ., Қазақстан, E-mail: zkabdrahmanova@vku.edu
Тлебалдинова Айжан Солтангалиевна	PhD, Д.Серікбаев атындағы Шығыс Қазақстан техникалық университетінің Ақпараттық технологиялар және зияткерлік жүйелер мектебінің қауымдастырылған профессоры, E-mail: atlebaldinova@edu.ektu.kz
Карменова Мархаба Ахметоллиновна	PhD, С.Аманжолов атындағы Шығыс Қазақстан университетінің қауымдастырылған профессоры,, Өскемен қ., Қазақстан, E-mail: mkarmenova@vku.edu.kz
Кумаргажанова Сауле Кумаргажановна	Техникалық ғылымдар кандидаты, Д.Серікбаев атындағы Шығыс Қазақстан техникалық университетінің Ақпараттық технологиялар және зияткерлік жүйелер мектебінің профессоры, E-mail: saule.kumargazhanova@edu.ektu.kz
Карымсакова Индира Бекеновна	PhD, «IT технологиялар» кафедрасының қауымдастырылған профессорының м.а., «Шәкәрім университеті» коммерциялық емес акционерлік қоғамы, Семей, Қазақстан Республикасы, E-mail: karymsakova.indira@mail.ru

Information about the authors

Kabdrakhmanova Zaure	Doctoral student of the 2nd year of study EP 8D06101 – «Information systems (by branches)» School of Information Technologies and Intelligent Systems at D.Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk, Kazakhstan, E-mail: zkabdrahmanova@vku.edu
Tlebaldinova Aizhan	PhD, Associate Professor of the School of Information Technologies and Intelligent Systems at D. Serikbayev East Kazakhstan Technical University, E-mail: atlebaldinova@edu.ektu.kz
Karmenova Marhaba	PhD, Associate Professor, S. Amanzholov East Kazakhstan University, Ust-Kamenogorsk, Kazakhstan, E-mail: mkarmenova@vku.edu.kz
Kumargazhanova Saule	Candidate of Technical Sciences, Professor of the School of Information Technologies and Intelligent Systems at D. Serikbayev East Kazakhstan Technical University, E-mail: saule.kumargazhanova@edu.ektu.kz
Karymsakova Indira	PhD, acting associate professor of the department of «IT technologies», Non-profit Joint-stock company "Shakarim University", Semey, Republic of Kazakhstan, E-mail: karymsakova.indira@mail.ru



UDC 004.855

IRSTI 28.23.01

https://doi.org/10.53364/24138614_2025_38_3_9

G. Dzhsupbekova¹, G. Ordabayeva^{2*}, A. Beketova², G. Baispay²

¹M. Auezov South Kazakhstan State University, Shymkent, 160019, Kazakhstan

²Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan

*E-mail: ordabayeva.gulzinat@kaznu.kz

APPLYING ARTIFICIAL INTELLIGENCE METHODS TO DETECT NETWORK TRAFFIC ANOMALIES

Abstract. *The development of information technology continues to highlight the importance of ensuring the security of information resources. The increasing number of various types of information threats complicates the detection of attacks. The objective of the study is to apply artificial intelligence methods for attack detection while minimizing the number of traffic features to achieve the required detection quality. To train AI, it is necessary to create a high-quality dataset that allows for the accurate identification of attack features in network traffic. The proposed approach uses AI trained on the UNSW-NB 15 dataset, which includes nine types of network attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. For implementation, Python is used with the Pytorch and Pandas libraries for data processing. An analysis of the software module's performance was conducted, along with the application of binary evaluation methods such as the Kappa Coefficient and the Jaccard Index. The effectiveness of the proposed AI model is evaluated using classification metrics: Accuracy, Precision, Recall, and F1 Score. Testing of the developed model with different sets of features revealed that the model achieves high-quality prediction of anomalous traffic when using five selected features. The performance of the AI model was assessed using the Kappa Coefficient and the Jaccard Index. Effective classification thresholds were calculated based on the results, improving the quality of anomalous traffic prediction. The evaluation results show that the developed model, trained on the UNSW-NB 15 dataset, can accurately detect traffic anomalies, thereby contributing to the information security of information resources.*

Keywords: *network traffic, artificial intelligence, neural networks, attack detection, dataset, UNSW-NB, Kappa Coefficient, Jaccard Index.*

Introduction

The application of information technologies is growing at a rapid pace today. This digital transformation has led to a range of security issues. According to data from the State Technical Service for the first quarter of the current year, over 16 million cyberattacks were blocked using the Unified Internet Access Gateway (UIAG). Among the identified cases of malware distribution, a total of 9,586 instances were registered and processed, with 2,795 in January, 1,317 in February, and 5,474 in March [1].

Gartner has released a new report on technologies used in everyday information security practices, showing that ITDR (Identity Threat Detection and Response) has reached the peak of inflated expectations in the Hype Cycle for Security Operations, 2024 [2].

According to data from Positive Technologies, the number of incidents increased by 7% in the first quarter of 2024 compared to the previous quarter. One of the most common outcomes of successful cyberattacks was the leakage of confidential information, which accounted for 72% of incidents involving individuals and 54% involving organizations. Additionally, cybersecurity researchers from Secure Works observed a rise in domains registered with keywords related to obituaries. Cybercriminals used artificially generated obituaries to attract potential victims. Their targets included compromising the personal data of website visitors, stealing money under the guise of donations for fictitious causes, and infecting devices with malware [3].

All these incidents are linked to the fact that modern attack scenarios are characterized by high complexity, multi-stage processes, and automation. Attackers possess advanced technical skills and actively employ artificial intelligence methods. The increasing frequency of attacks necessitates a reassessment of protection strategies and the adoption of cutting-edge technologies for network traffic analysis during the early stages of developing security solutions.

Materials and Methods.

Analyze the dataset

Analyzing network traffic for threat and anomaly detection requires processing large volumes of data in real-time. One approach to addressing this challenge is the use of Artificial Intelligence (AI). The network should incorporate various types of AI and be pre-trained for the system's operation. These conditions will help mitigate the complexities associated with applying AI for attack recognition in network traffic [4].

The paper aims to apply artificial intelligence methods for detecting attacks while minimizing the number of traffic features to achieve the desired detection quality. To achieve this goal, the following tasks need to be addressed: 1. Analyze the UNSW-NB 15 dataset [5] to identify the most significant features that will aid in detecting anomalous traffic associated with various attacks; 2. Determine the model parameters for constructing a neural network in accordance with the selected training methodology and prepare the necessary software; 3. Test the developed anomaly detection module for different sets of input features; 4. Evaluate the performance of the software module, considering effective threshold selection and applying binary evaluation methods such as the Kappa coefficient and the Jaccard index.

For training and testing the developed neural network model, the UNSW-NB 15 dataset was used, which is freely accessible [5]. UNSW-NB 15 is a dataset of network traffic created using the IXIA PerfectStorm tool in the Cyber Range laboratory of the Australian Centre for Cyber Security (ACCS). This dataset includes both normal traffic and traffic associated with one of nine types of network attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. The dataset contains separate training and testing sets in *.csv format, with 171,716 and 82,331 records, respectively. For the classification task, a combined dataset was created from the original training and testing sets, containing a total of 254,047 records. A snippet of the UNSW-NB 15 dataset is shown in Figure 1.

id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	sloss	dloss	sinpkt	dinpkt	sjit	djit	swin	stcpb	dtcpb	dwin	tcprtt	synack	ack
0	1	0.000011	udp	-	INT	2	0	496	0	90909.09020	254	0	1.803636e+08	0.0	0	0	0.011	0.0	0.0	0.0	0	0	0	0	0.0	0.0
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.00030	254	0	8.810000e+08	0.0	0	0	0.008	0.0	0.0	0.0	0	0	0	0	0.0	0.0
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.00510	254	0	8.544000e+08	0.0	0	0	0.005	0.0	0.0	0.0	0	0	0	0	0.0	0.0
3	4	0.000006	udp	-	INT	2	0	900	0	166666.66080	254	0	6.000000e+08	0.0	0	0	0.006	0.0	0.0	0.0	0	0	0	0	0.0	0.0
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.00250	254	0	8.504000e+08	0.0	0	0	0.010	0.0	0.0	0.0	0	0	0	0	0.0	0.0
5	6	0.000003	udp	-	INT	2	0	784	0	333333.32150	254	0	1.045333e+09	0.0	0	0	0.003	0.0	0.0	0.0	0	0	0	0	0.0	0.0
6	7	0.000006	udp	-	INT	2	0	1960	0	166666.66080	254	0	1.306667e+09	0.0	0	0	0.006	0.0	0.0	0.0	0	0	0	0	0.0	0.0
7	8	0.000028	udp	-	INT	2	0	1384	0	35714.28522	254	0	1.977143e+08	0.0	0	0	0.028	0.0	0.0	0.0	0	0	0	0	0.0	0.0
8	9	0.000000	arp	-	INT	1	0	46	0	0.00000	0	0	0.000000e+00	0.0	0	0	60000.688	0.0	0.0	0.0	0	0	0	0	0.0	0.0
9	10	0.000000	arp	-	INT	1	0	46	0	0.00000	0	0	0.000000e+00	0.0	0	0	60000.712	0.0	0.0	0.0	0	0	0	0	0.0	0.0

Figure 1 – The source dataset UNSW-NB 15

The UNSW-NB 15 dataset includes both numerical and categorical values. For the neural network to function properly, all features must be represented in numerical format. Feature selection, which is crucial for the binary classification task, plays a key role in ensuring the performance and accuracy of the traffic anomaly detection model [6]. The UNSW-NB 15 dataset contains 40 features, some of which are irrelevant, weakly correlated, or partially redundant, potentially impacting the quality of the traffic anomaly detection model. To identify the most informative features, a correlation matrix (Figure 2) was constructed based on Pearson correlation coefficients [7], using the training dataset. The Pearson correlation coefficient is calculated as the ratio of the covariance of two variables to the product of their standard deviations, where covariance is defined as the expected value of the product of deviations of the variables from their mean values (1).

$$r_{xy} = \frac{cov(x,y)}{\sqrt{s_x^2 s_y^2}} = \frac{\sum_{i=1}^m (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^m (x_i - \bar{x})^2 \sum_{i=1}^m (y_i - \bar{y})^2}}, \tag{1}$$

where \bar{x}, \bar{y} - are the mean values of the vectors x and y ; s_x^2, s_y^2 - are the variances of the vectors x and y .

The correlation coefficient can range from -1 to 1. The greater the absolute value of the coefficient, the stronger the correlation between the variables. A value close to 0 indicates a weak correlation. If the correlation coefficient is between 0 and 1, it signifies a positive correlation, whereas a value between -1 and 0 indicates a negative correlation. A value of 1 means a perfect positive correlation between two variables, -1 indicates a perfect negative correlation, and 0 denotes no correlation.

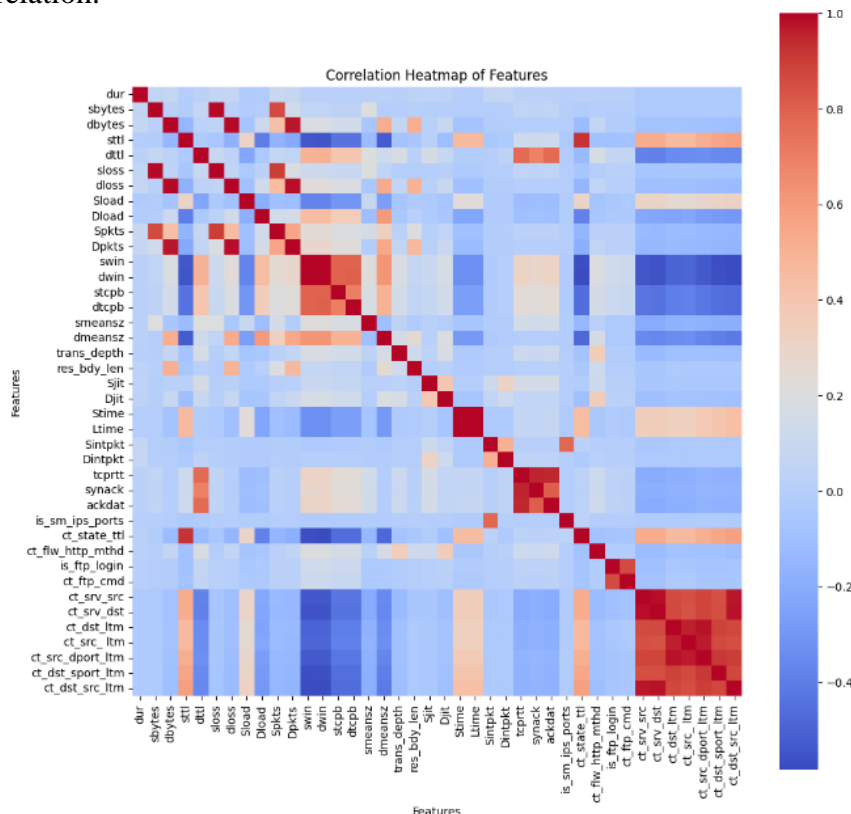


Figure 2 – The correlation matrix based on Pearson correlation coefficients for 40 features

As a result of using the correlation matrix, the 40 features were sorted in descending order of their correlation coefficients and summarized in Table 1.

Table 1 – Results of Traffic Feature Ranking

№	feature	№	feature	№	feature	№	feature
1	dur	11	Dpkts	21	Djit	31	ct_flw_http_mthd
2	sbytes	12	swin	22	Stime	32	is_ftp_login
3	dbytes	13	dwin	23	Ltime	33	ct_ftp_cmd
4	sttl	14	stcpb	24	Sintpkt	34	ct_srv_src
5	dttl	15	dtcpb	25	Dintpkt	35	ct_srv_dst
6	sloss	16	smeansz	26	tcprtt	36	ct_dst_ltm
7	dloss	17	dmeansz	27	synack	37	ct_src_ltm
8	Sload	18	trans_depth	28	ackdat	38	ct_src_dport_ltm
9	Dload	19	res_bdy_len	29	is_sm_ips_ports	39	ct_dst_sport_ltm
10	Spkts	20	Sjit	30	ct_state_ttl	40	ct_dst_src_ltm

Neural Network Model

The architecture of the created neural network is shown in Fig. 3. The neural network model is implemented in Python using the PyTorch machine learning framework [9]. Data preprocessing and metric calculations for classification quality evaluation were performed using the Scikit-learn [10] and Pandas [11] libraries.

The development was carried out in the specialized online environment Kaggle [12].

The input layer consists of 3 neurons. Each neuron receives binary data (0 or 1) representing various features of the input message, such as the presence of certain words or other characteristics of the text. The hidden layer contains 3 neurons. Each neuron receives a linear combination of input signals, which is weighted. After summing the signals, a sigmoid activation function is applied, which limits the output value to a range from 0 to 1. The weights are changed during the training process to improve the accuracy of predictions. The output layer consists of a single neuron. This neuron takes values from the hidden layer and also uses the sigmoid activation function. The implementation of the neural network model is calculated in the MS Excel program (Figure 3).

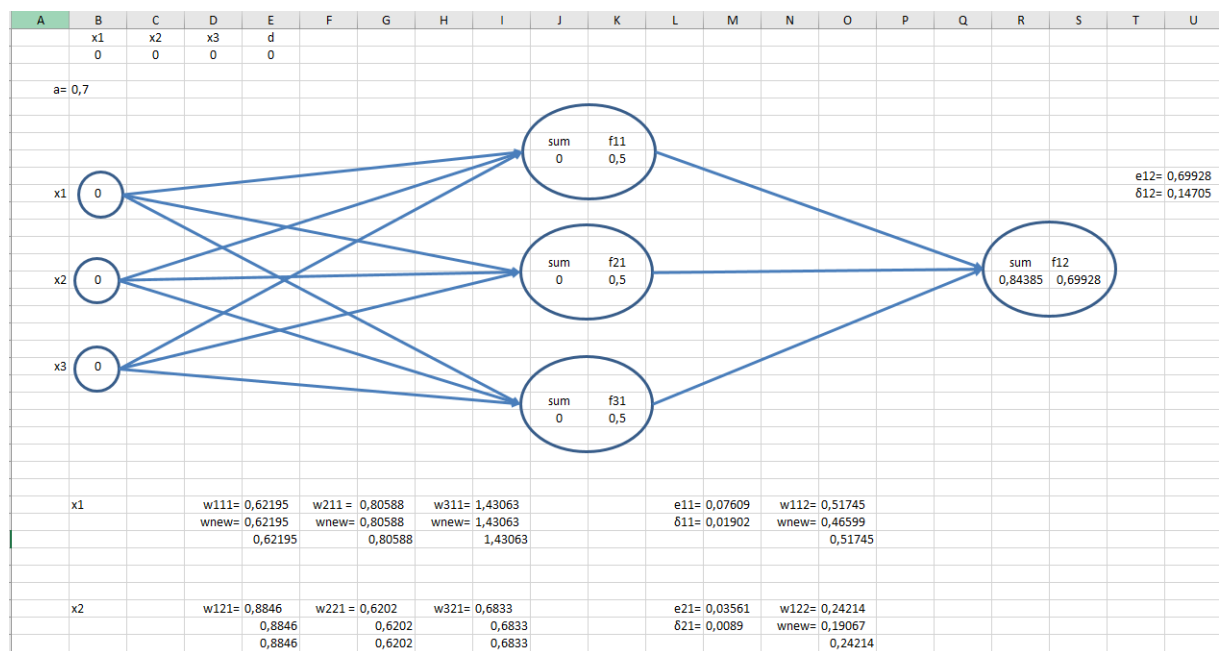


Figure 3 – Proposed neural network architecture

The neural network is trained using the backpropagation method. The purpose of training is to minimize the error between the predicted result and the actual label. During training, the weights of the neurons are adjusted to improve predictions. The main parameters of the model:

- The number of input neurons is 3;
- The number of neurons in the hidden layer is 3;
- Number of output neurons – 1;
- Activation function - sigmoid function;
- Learning algorithm - error propagation back;
- Learning rate (α): 0.7.

After completing the training, the neural network is able to accept new input data and make predictions based on the trained weights.

Neural Network Models in Literature

The 1950s marked the beginning of artificial intelligence, and recent advancements in this field have significantly driven manufacturing innovations. Despite the clear benefits of AI technologies, their use has sparked debates over potential misuse [13]. AI is a branch of computer science focused on developing theories, methods, technologies, and systems to model human intelligence and integrate it into machines [14]. The primary goal of AI is to endow machines with capabilities similar to human intelligence. Machine learning is a method of implementing AI through algorithms that analyze data and learn from it. Deep learning, in turn, is a technology within machine learning that enhances the scope of AI applications [15]. The essence of AI lies in the idea that human intelligence can be precisely described, allowing its reproduction by machines and software [16].

Bindra and Sood investigated six machine learning (ML) methods — LR, KNN, RF, NB, linear SVM, and linear discriminant analysis (LDA) — to determine the most effective method for detecting DDoS attacks [17]. Testing on the CIC IDS dataset revealed that the RF technique achieved the best results with an accuracy of 96.5%, outperforming all other methods. Similarly, Chavan et al. assessed the effectiveness of four ML methods — KNN, SVM, DT, and LR — for detecting DDoS attacks [18]. Among these methods, LR achieved the highest accuracy of 90.4%, surpassing the other techniques. Ensemble methods generally provide higher accuracy compared to base classifiers. Consequently, Das, Saikat, et al. [19] proposed an ensemble model that combines four base ML methods — Multilayer Perceptron (MLP), SVM, KNN, and DT. Experiments conducted on the NSL-KDD dataset showed that the ensemble classifier outperformed the individual classifiers used in the same study.

In [20] and [21], machine learning has been applied for classifying network traffic to detect anomalies. The issue of non-binary network traffic classification during attack detection has also been addressed. Authors [22] conducted a comprehensive evaluation of datasets using the CSE-CIC-IDS2018 dataset and developed a generation model to create a reliable benchmark dataset for IDS and IPS. Data corresponding to normal traffic as well as two types of attacks—DDOS and Infiltration—were selected from this dataset. In the DDOS attack scenario, an attempt is made to cause a denial of service by overwhelming the server with excessive load. In the Infiltration attack scenario, the objective is to gain remote access to a workstation within the targeted network.

In the study [23], an AI algorithm for developing cyberattack detection systems in a Wireless Sensor Network (WSN) is examined (Figure 4).

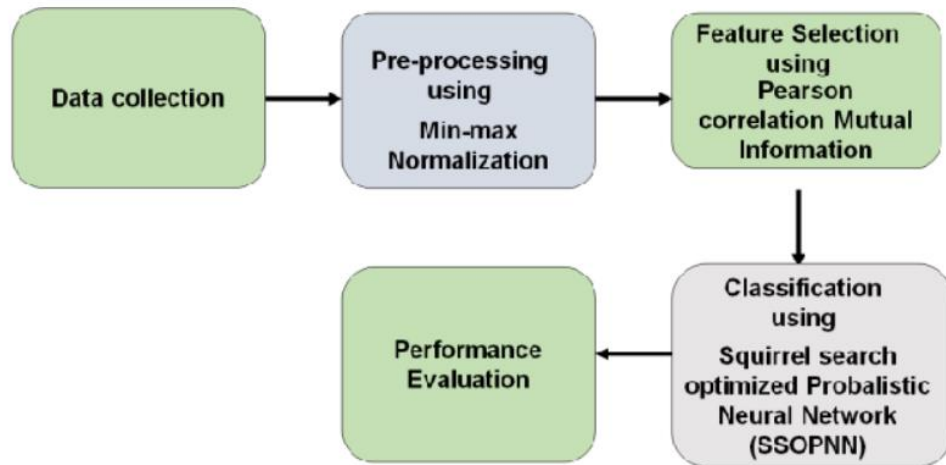


Figure 4 – Data description [23]

The study also proposes several classification methods for detecting cyberattacks in WSN, including Squirrel Search Optimized Probabilistic Neural Network (SSOPNN), Gaussian Naïve Bayes (Gaussian NB), K-Nearest Neighbors (KNN), and Random Forest (RF). A comparative analysis of these methods is presented in the study, using metrics such as detection rate, false positive rate, false negative rate, and average prediction time per sample.

Aslam, N. et al. [24] propose using machine learning (ML) and deep learning (DL) for detecting DDoS attacks in Software-Defined Networking (SDN) in their research. The study develops a taxonomy of solutions for protecting against DDoS attacks. Based on an analysis of 260 scientific articles, 132 papers were selected based on ML and DL solutions for detecting DDoS attacks in SDN. The study suggests security challenges and the development of new protection methods for SDN.

Bolshakov, A.S. et al. [8], an analysis of the dataset was conducted using Pearson correlation coefficients, which allowed for the ranking of these coefficients. A neural network architecture with a sigmoid activation function was developed, effectively addressing the binary classification problem, and the choice of model parameters was justified. The performance of the neural network model was evaluated using ROC and PR curves. Based on the area under the ROC curve (AUC-ROC), optimal classification thresholds were determined, leading to an improvement in the quality of traffic anomaly prediction.

Research Gap and Contribution

Existing studies predominantly rely on classical ML algorithms or isolated deep learning models without systematically evaluating the impact of feature selection on performance. Furthermore, comprehensive comparisons of state-of-the-art DL architectures on recent, high-quality datasets such as UNSW-NB15 remain limited.

The present study addresses these limitations by implementing a hybrid approach that combines correlation matrix-based feature selection with multiple deep learning models, including CNN, LSTM, GRU, MLP, and RNN. The experimental results demonstrate that the CNN model achieved the highest accuracy (99.21%), significantly surpassing the performance metrics reported in prior studies. The use of UNSW-NB15, a dataset with more diverse and realistic traffic scenarios, enhances the generalizability of the findings. Additionally, the study introduces evaluation metrics such as the Kappa Coefficient and Jaccard Index, offering a more nuanced assessment of model reliability. The highest F1-scores achieved were 0.97 (Kappa) and 0.95 (Jaccard), reinforcing the robustness of the proposed method in distinguishing normal and anomalous traffic patterns.

Results.

The developed neural network model was tested with varying numbers of features as shown in Table 1, using a learning rate of 0.001.

The model was trained for 30 epochs. After training, the effectiveness of the neural network was evaluated on a test dataset. The obtained confusion matrix results and their values - TP, TN, FP, FN - formed the basis for calculating classification quality metrics [25].

True Positive (TP): The number of samples correctly predicted as anomalous.

True Negative (TN): The number of samples correctly predicted as normal.

False Positive (FP): The number of samples incorrectly predicted as anomalous.

False Negative (FN): The number of samples incorrectly predicted as normal.

Accuracy ($\frac{TP+TN}{TP+TN+FP+FN}$) - this metric represents the proportion of predictions that the model made correctly relative to the total number of samples. This metric performs well only if there is an equal number of samples belonging to each class.

Precision ($\frac{TP}{TP+FP}$) - this metric represents the proportion of predicted anomalous samples that are indeed anomalous.

Recall ($\frac{TP}{TP+FN}$) - this metric represents the proportion of anomalous samples detected by the model.

F1 ($2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}}$) – this is a weighted average of accuracy and memorability. This metric can tell you how accurate and reliable the model in question is [26, 27].

Using the given formulas, the metrics Accuracy, Precision, Recall, and F1 were calculated, and the results are presented in the form of a histogram in Figure 5.

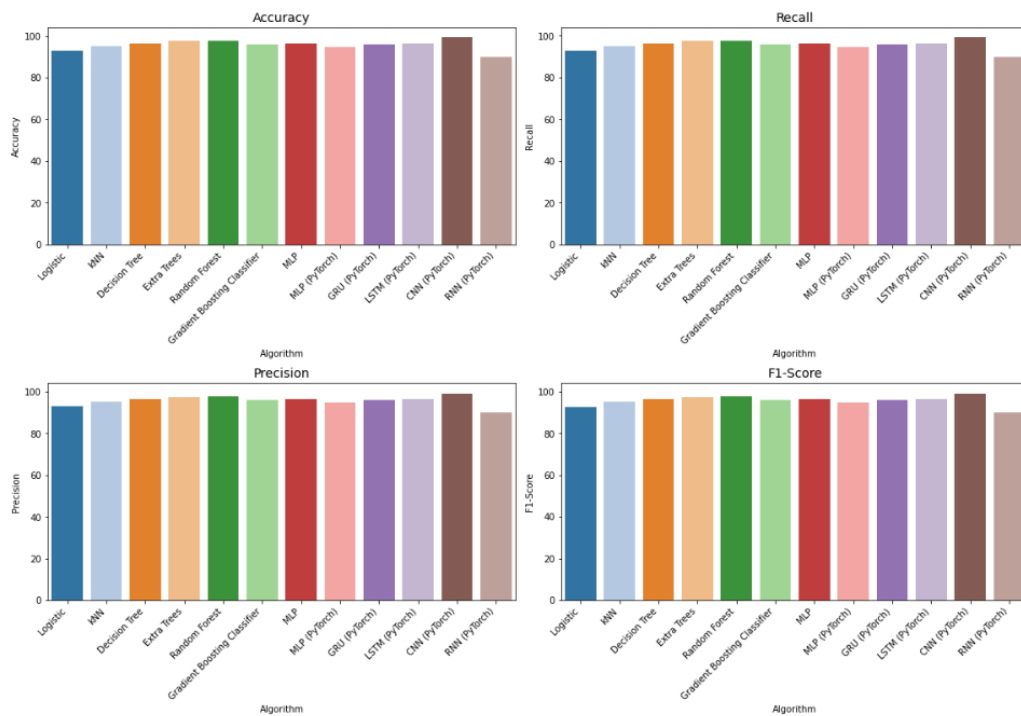


Figure 5 – Performance Metrics Comparison

To enhance the model's performance, it was decided to compute the values of the Kappa Coefficient and the Jaccard Index (table 2) [28].

The Kappa Coefficient provides valuable insight into the agreement between the model's predictions and the true labels, accounting for random chance. This makes it useful for assessing classification quality, comparing models, and evaluating clustering quality. The Kappa Coefficient is a powerful tool for a more precise evaluation of model performance in AI tasks.

The Jaccard Index is a metric that measures the degree of similarity between two sets. In AI, it is often used to assess the quality of binary classification, clustering, and anomaly detection. The

Jaccard Index helps evaluate the accuracy of classifiers, especially when interested in positive results, such as in rare events or anomaly detection tasks.

Table 2 - Results of the Metrics for Kappa Coefficient and Jaccard Index

Traffic	Accuracy	Precision	Recall	F1	Kappa Coefficient	Jaccard Index
Normal	0,9925	0,9925	0,9925	0,992503	0,984479	0,9843
Anomalous	0,9925	0,9925	0,9960	0,9912	0,9633	0,9223

Thus, using the classification threshold determined by the Kappa Coefficient and Jaccard Index metrics, the F1 scores achieved are 0.97 and 0.95, respectively, which represent the best-obtained evaluation of the classification quality of the developed neural network model.

Discussion.

The study presents the results of testing five types of AI (MLP, GRU, LSTM, CNN, and RNN) for binary classification tasks aimed at detecting attacks (Table 3).

Table 3 – Performance evaluation of AI

	Accuracy	Recall	Precision	F1-Score	time to train	time to predict	total time
MLP (PyTorch)	94.98%	94.98%	94.98%	94.98%	43.7	0.2	43.9
GRU (PyTorch)	96.34%	96.34%	96.34%	96.34%	203.0	0.2	203.1
LSTM (PyTorch)	96.32%	96.32%	96.32%	96.32%	207.0	0.3	207.3
CNN (Pytorch)	99.26%	99.20%	99.20%	99.18%	830.0	0.2	830.2
RNN (Pytorch)	90.00%	90.20%	90.20%	90.20%	1150.0	0.2	1150.2

Table 3 presents a comparison of the effectiveness of four AI methods using four different performance metrics.

The study employed supervised learning. After tuning the model parameters, an AI architecture with a minimal number of layers was used. The configurable parameters were set to a learning rate of 0.001 and a batch size of 2000 (Figure 6).

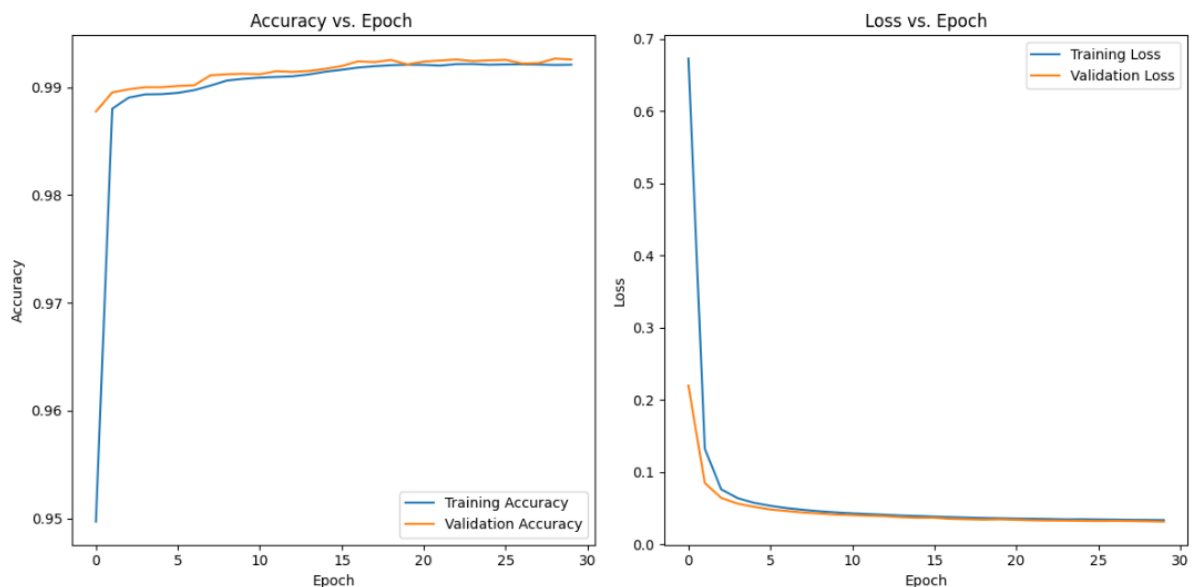


Figure 6 – Training schedule for CNN (PyTorch)

According to the results shown in Figure 6, the training process was stable and no overfitting was observed. The model's accuracy was 0.9924, and the error loss was 0.0334.

Figure 7 displays the confusion matrix for the four AI models.

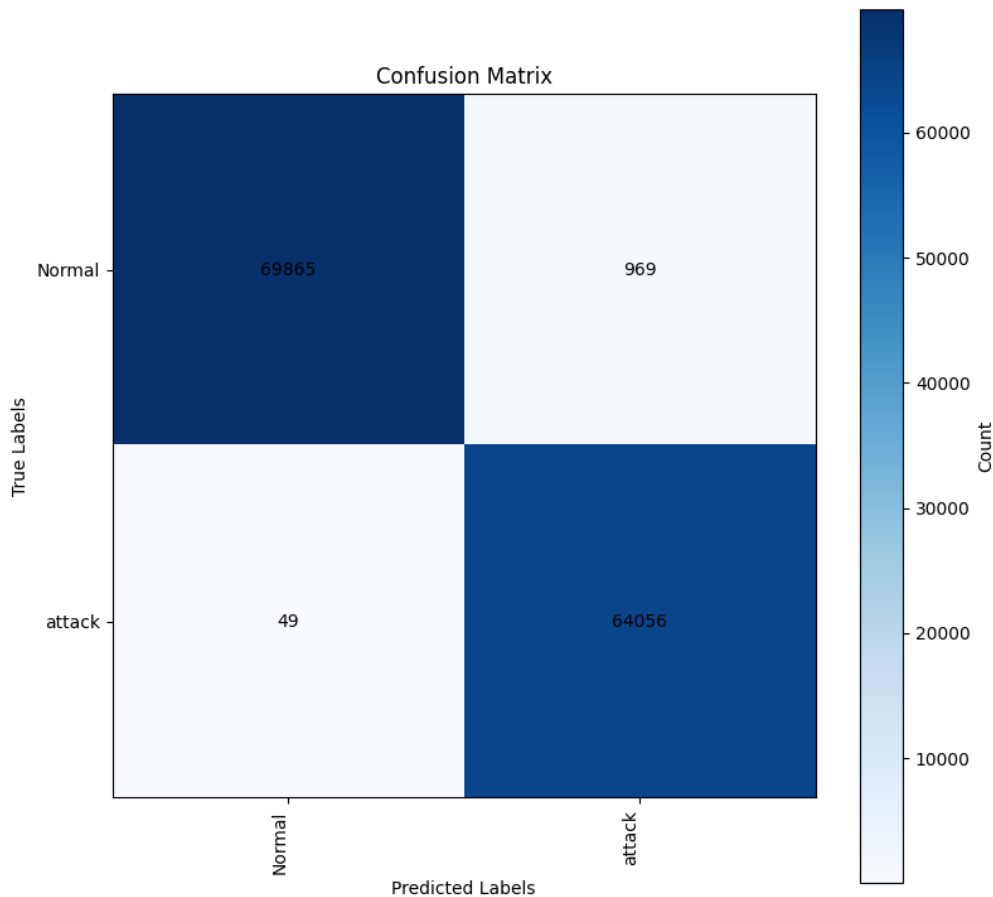


Figure 7 – Confusion Matrix

Based on the data from Figure 6, the total number of correctly predicted instances for the Normal class is 69,865, while the number of incorrect predictions is 969. The overall total number of correctly predicted instances is 133,921, with incorrect predictions totaling 1,010, which represents less than 1%.

Preprocessing and feature selection are crucial steps before implementing AI methods. The preliminary implementation of data preprocessing and testing critical functions could improve accuracy by approximately 47%. Thus, in this study, the proposed model demonstrated promising results after selecting important and influential features and applying the appropriate AI model.

Conclusions.

The conducted research demonstrated that using a correlation matrix for feature selection and applying a neural network enables the development of an effective system for attack detection. With the selected number of features, the classification scores achieved, according to the Kappa Coefficient and Jaccard Index metrics, were $F1=0.97$ and $F1=0.95$, respectively, marking the highest classification quality for the developed neural network model.

The UNSW-NB 15 dataset used in this study was divided into 80% for training the models and 20% for testing. The effectiveness of the four methods was compared on only 31 instances from the selected dataset using a sample selection method. Among the models tested, CNN achieved the highest accuracy at 99.21%, surpassing all other models. The LSTM model ranked second with an accuracy of 96.33%, followed by the GRU model with an accuracy of 95.90%. The MLP model was in fourth place with an accuracy of 94.76%, while the RNN method achieved the lowest accuracy at 90.15%.

Exploring various types of AI, and analyzing and comparing them, will further aid in optimizing neural network parameters, thereby reducing computational resource costs for the system. The evaluation of the AI model's performance using the Kappa Coefficient and Jaccard Index demonstrated effective classification threshold results, which enhanced the accuracy of anomaly detection in network traffic.

Having an intelligent system capable of detecting intrusions significantly contributes to ensuring user privacy and security. Future work could focus on classifying different types of attacks on cybersecurity systems. Additionally, classification accuracy could be improved by employing integrated methods that combine multiple individual classifiers.

Acknowledgement

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26102055).

References

1. Incident Review for Q1 2024. (2024). <http://cert.gov.kz/news/11/2641> (accessed: 26.01.2025)
2. Gartner Research. Hype Cycle for Security Operations. (2024). Published: July 29, 2024 <http://www.gartner.com/en/documents/5622491> (Accessed: 26.01.2025)
3. Current Cyber Threats: Q1 2024. (2024) <http://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/> (accessed: 26.01.2025)
4. Glushanskij S.M., Buglov V.E. Inzhenernyj vestnik Dona. (2023). <http://ivdon.ru/ru/magazine/archive/n1y2023/8150> (accessed: 08.01.2025).
5. The UNSW-NB15 Dataset. (2024). // UNSW Research URL: <https://research.unsw.edu.au/projects/unsw-nb15-dataset> (accessed: 10.01.2025).
6. Sheluhin O.I., Erohin S.D., Vanyushina A.V. (2018). Classification of IP traffic using machine learning methods. Edited by prof. Sheluhin O.I.: Goryachaya liniya – Telekom. 282 p. DOI: [10.21681/2311-3456-2018-4-21-28](https://doi.org/10.21681/2311-3456-2018-4-21-28)
7. Chen P., Li F., Wu C. (2021). Research on Intrusion Detection Method Based on Pearson Correlation Coefficient Feature Selection Algorithm. Journal of Physics: Conference Series. Vol. 1757. No. 1. P. 012054. DOI: [10.1088/1742-6596/1757/1/012054](https://doi.org/10.1088/1742-6596/1757/1/012054)
8. Bolshakov, A.S., Khusainov, R.V., Osin, A.V. (2021). "Traffic Anomaly Detection Using Neural Networks for Information Security Protection" // Journal of the Institute "INTECH": I-methods. Vol. 13, No. 4. URL: <http://intech-spb.com/wp-content/uploads/archive/2021/4/6-bolshakov.pdf> (Accessed: 16.01.2025).
9. Electronic resource. URL: <https://pytorch.org> (Accessed: 26.01.2025).
10. Electronic resource. URL: <https://scikit-learn.org/stable/> (Accessed: 26.01.2025).
11. Electronic resource. URL: <https://pandas.pydata.org> (Accessed: 26.01.2025).
12. Electronic resource. URL: <https://www.kaggle.com> (Accessed: 26.01.2025).
13. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. (2020). Tackling Faults in the Industry 4.0 Era-A Survey of Machine-Learning Solutions and Key Aspects. Sensors 2020, 20, 109. DOI: [10.3390/s20010109](https://doi.org/10.3390/s20010109)
14. Li, J. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462–1474. DOI: [10.1631/FITEE.1800573](https://doi.org/10.1631/FITEE.1800573)
15. H. Ji, O. Alfarraj and A. Tolba. (2020). "Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications," in *IEEE Access*, vol. 8, pp. 61020-61034, 2020, DOI: [10.1109/ACCESS.2020.2983609](https://doi.org/10.1109/ACCESS.2020.2983609)
16. R. Trifonov, O. Nakov and V. Mladenov. (2018). "Artificial Intelligence in Cyber Threats Intelligence," 2018 International Conference on Intelligent and Innovative Computing

Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-4, DOI: [10.1109/ICONIC.2018.8601235](https://doi.org/10.1109/ICONIC.2018.8601235)

17. Bindra, Naveen & Sood, Manu. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences. 53. 419-428. DOI: [10.3103/S0146411619050043](https://doi.org/10.3103/S0146411619050043)

18. N. Chavan, M. Kukreja, G. Jagwani, N. Nishad and N. Deb. (2022). "DDoS Attack Detection and Botnet Prevention using Machine Learning," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1159-1163, DOI: [10.1109/ICACCS54159.2022.9785247](https://doi.org/10.1109/ICACCS54159.2022.9785247)

19. Das, S., Mahfouz, A. M., Venugopal, D., & Shiva, S. (2019). DDoS Intrusion Detection Through Machine Learning Ensemble. 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). DOI: [10.1109/qrs-c.2019.00090](https://doi.org/10.1109/qrs-c.2019.00090)

20. Babicheva M.V., Tret'yakov I.A. (2023). Application of machine learning methods for automated detection of network intrusions. Herald of Dagestan State Technical University. Technical Sciences. Vol. 50. no.1. Pp. 53–61. DOI: [10.21822/2073-6185-2023-50-1-53-66](https://doi.org/10.21822/2073-6185-2023-50-1-53-66) (In Russian)

21. Chastikova, V.A., Zherlitsyn, S.A., Volya, Y.I., & Sotnikov, V. (2020). Neural network technology for detecting anomalous network traffic. CASPIAN JOURNAL: Control and High Technologies, 49(1), 20-32. DOI: [10.21672/2074-1707.2020.49.4.020-032](https://doi.org/10.21672/2074-1707.2020.49.4.020-032)

22. Sharafaldin, I., Gharib, A., Lashkari, A. H., ... Ghorbani, A. A. (2017). Towards a Reliable Intrusion Detection Benchmark Dataset. Software Networking, 2017(1), 177–200. DOI: [10.13052/jsn2445-9739.2017.009](https://doi.org/10.13052/jsn2445-9739.2017.009)

23. Aneja, A. (2023). Attack Detection in Wireless Sensor Networks using Novel Artificial Intelligence Algorithm. 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 295-300. DOI: [10.1109/I-SMAC58438.2023.10290399](https://doi.org/10.1109/I-SMAC58438.2023.10290399)

24. Aslam, N., Srivastava, S. & Gore, M.M. A. (2024). Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. Arab J Sci Eng 49, 3533–3573 DOI: [10.1007/s13369-023-08075-2](https://doi.org/10.1007/s13369-023-08075-2)

25. Powers, David & Ailab. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. J. Mach. Learn. Technol. 2. 2229-3981. DOI: [10.9735/2229-3981](https://doi.org/10.9735/2229-3981). <http://www.bioinfo.in/contents.php?id=51>

26. Soleymani, Roghayeh & Granger, Eric & Fumera, Giorgio. (2019). F-Measure Curves: A Tool to Visualize Classifier Performance Under Imbalance. Pattern Recognition. 100. 107146. DOI: [10.1016/j.patcog.2019.107146](https://doi.org/10.1016/j.patcog.2019.107146)

27. Hand, D.J., Christen, P. & Kirielle, N. (2021). F*: an interpretable transformation of the F-measure. Mach Learn 110, 451–456 (2021). DOI: [10.1007/s10994-021-05964-1](https://doi.org/10.1007/s10994-021-05964-1)

28. Pravin, S. C., & Palanivelan, M. (2022). WDSAE-DNDT BASED SPEECH FLUENCY DISORDER CLASSIFICATION. Malaysian Journal of Computer Science, 35(3), 222–242. DOI: [10.22452/mjcs.vol35no3.3](https://doi.org/10.22452/mjcs.vol35no3.3)

ЖЕЛІЛІК ТРАФИК АНОМАЛИЯЛАРЫН АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІН ҚОЛДАНУ

Аңдатпа. Ақпараттық технологиялардың дамуы ақпараттық ресурстардың қауіпсіздігін қамтамасыз етудің маңыздылығын көрсетуді жалғастыруда. Ақпараттық қауіптердің әртүрлі түрлерінің көбеюі шабуылдарды анықтауды қиындатады. Зерттеудің мақсаты талап етілетін анықтау сапасына қол жеткізу үшін трафик элементтерінің санын азайту кезінде шабуылдарды анықтау үшін жасанды интеллект әдістерін қолдану болып табылады. AI үйрету үшін желілік трафиктегі шабуыл мүмкіндіктерін дәл анықтай алатын жоғары сапалы деректер жиынтығын жасау қажет. UNSW-NB 15 деректер жиынында оқытылған жасанды интеллектті қолдана

отырып ұсынылған тәсіл желілік шабуылдардың тоғыз түрін қамтитын: *Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode* және *Worms*. Деректерді өңдеу үшін *Pytorch* және *Pandas* кітапханалары бар *Python* тілі пайдаланылды. Бағдарламалық модульдің өнімділігіне талдау жасалды, Карра коэффициенті және Жаккар индексі сияқты екілік бағалау әдістері қолданылды. Ұсынылған AI моделінің тиімділігі жіктеу көрсеткіштері арқылы бағаланады: *Accuracy, Precision, Recall* және *F1 Score*. Әртүрлі мүмкіндіктер жиынтығымен әзірленген модельді тестілеу бес таңдалған мүмкіндікті пайдалану кезінде модельдің қалыптан тыс трафикті жоғары сапалы болжауға қол жеткізуге мүмкіндік беретінін көрсетті. AI моделінің өнімділігі Карра коэффициенті мен Жаккар индексі арқылы бағаланды. Алынған нәтижелер бойынша классификацияның тиімді шектері есептелді, бұл қалыптан тыс трафикті болжау сапасын жақсартты. Бағалау нәтижелері көрсеткендей, UNSW-NB 15 деректер жинағында әзірленген модель трафик ауытқуларын дәл анықтай алады, осылайша ақпараттық ресурстардың ақпараттық қауіпсіздігіне ықпал етеді.

Түйін сөздер: желілік трафик, жасанды интеллект, нейрондық желілер, шабуылдарды анықтау, деректер жинағы, UNSW-NB, Карра коэффициенті, Жаккард индексі.

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

Аннотация. Развитие информационных технологий продолжает выдвигать на первый план важность обеспечения безопасности информационных ресурсов. Растущее количество различных видов информационных угроз усложняет обнаружение атак. Цель исследования — применение методов искусственного интеллекта для обнаружения атак при минимизации количества элементов трафика для достижения требуемого качества обнаружения. Для обучения ИИ необходимо создать высококачественный набор данных, позволяющий точно выявлять особенности атаки в сетевом трафике. В предлагаемом подходе используется искусственный интеллект, обученный на датасете UNSW-NB 15, который включает в себя девять типов сетевых атак: *Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode* и *Worms*. Для реализации используется *Python* с библиотеками *Pytorch* и *Pandas* для обработки данных. Был проведен анализ производительности программного модуля, а также применены методы двоичной оценки, такие как коэффициент Карра и индекс Жаккара. Эффективность предложенной модели ИИ оценивается с помощью метрик классификации: *Accuracy, Precision, Recall, F1 Score*. Тестирование разработанной модели с различными наборами признаков показало, что модель позволяет достичь высокого качества прогнозирования аномального трафика при использовании пяти выбранных признаков. Производительность модели ИИ оценивалась с помощью коэффициента Карра и индекса Жаккара. На основе полученных результатов были рассчитаны эффективные пороги классификации, что повысило качество прогнозирования аномального трафика. Результаты оценки показывают, что разработанная модель, обученная на наборе данных UNSW-NB 15, может точно выявлять аномалии трафика, тем самым способствуя безопасности информационных ресурсов.

Ключевые слова: сетевой трафик, искусственный интеллект, нейронные сети, обнаружение атак, набор данных, UNSW-NB, коэффициент Карра, индекс Жаккара.

Information about the authors

Ordabayeva Gulzinat	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: ordabayeva.gulzinat@kaznu.kz
Beketova Aiman	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: aiman.beketova@gmail.com
Dzhsupbekova Gulzat	Candidate of Pedagogical Sciences, Head of the Department of Information Technology, M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan; E-mail: gulzat20.10@mail.ru
Baispay Gulshat	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: gulshat.bgb2@gmail.com

Сведения об авторах

Ордабаева Гулзинат	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: ordabayeva.gulzinat@kaznu.kz
Бекетова Айман	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: aiman.beketova@gmail.com
Джусупбекова Гулзат	кандидат педагогических наук, зав. кафедрой «Информационно-коммуникационные технологии», Южно-Казахстанский университет имени М.Ауэзова, г.Шымкент;E-mail: gulzat20.10@mail.ru
Байспай Гүлшат	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: gulshat.bgb2@gmail.com

Авторлар туралы мәлімет

Ордабаева Гулзинат	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: ordabayeva.gulzinat@kaznu.kz
Бекетова Айман	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: aiman.beketova@gmail.com
Джусупбекова Гулзат	педагогика ғылымдарының кандидаты, «Ақпараттық-коммуникациялық технологиялар» кафедрасының меңгерушісі, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент қаласы; E-mail: gulzat20.10@mail.ru
Байспай Гүлшат	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: gulshat.bgb2@gmail.com



УДК 004.056.5

МРНТИ 81.93.29

https://doi.org/10.53364/24138614_2025_38_3_10

С.А.Адилжанова¹, А.Н.Құрасбек^{1*}, М.О.Кенжебаева¹

¹Казахский национальный университет имени аль-Фараби, Алматы, Казахстан

*E-mail: kurasbek.a.140@mail.ru

ПРИМЕНЕНИЕ LLM В КИБЕРБЕЗОПАСНОСТИ: ОБЗОР ПРИЛОЖЕНИЙ И УЯЗВИМОСТЕЙ LLM

Аннотация. В этом документе представлен всесторонний обзор будущего кибербезопасности с помощью больших языковых моделей (LLM). Мы представляем обзор эволюции LLM и ее текущего состояния, уделяя особое внимание достижениям в таких моделях, как GPT-4, GPT-3.5, BERT, Falcon2 и LLaMA. Наш анализ распространяется на уязвимости LLM, такие как быстрое внедрение, небезопасная обработка выходных данных, отравление данных, DDoS-атаки и состязательные инструкции. Мы подробно рассмотрим стратегии смягчения последствий для защиты этих моделей, предоставив всесторонний обзор потенциальных сценариев атак и методов их предотвращения. Эти аналитические данные направлены на улучшение защиты от кибербезопасности в режиме реального времени и повышение сложности приложений LLM для обнаружения угроз и реагирования на них. В нашем документе представлено основополагающее понимание и стратегическое направление интеграции LLM в будущие системы кибербезопасности для защиты от развивающихся киберугроз.

Ключевые слова: LLM, кибербезопасность, большие языковые модели, языковое моделирование, машинное обучение, NLP, обработка естественного языка.

Введение.

Кибербезопасность — это постоянно развивающаяся область, в которой угрозы становятся все более изощренными и сложными. Поскольку организации и частные лица полагаются на цифровые технологии для связи, коммерции и критически важной инфраструктуры, потребность в надежных мерах к кибербезопасности никогда не была столь велика [1]. Масштаб и разнообразие киберугроз ставят перед специалистами по безопасности сложную задачу по их эффективному выявлению, обнаружению и защите от них. В этом контексте большие языковые модели (LLM) стали технологией, меняющей правила игры и способной значительно улучшить методы кибербезопасности [2, 3, 4, 5, 6]. Эти модели, основанные на передовых методах NLP и машинного обучения (ML), открывают новый рубеж в борьбе с киберугрозами [7, 8]. В этой статье исследуются мотивы и применение LLM в кибербезопасности.

Специалистам по кибербезопасности часто приходится просеивать огромное количество текстовых данных, включая предупреждения безопасности, отчеты об инцидентах, ленты угроз и исследовательские работы, чтобы опережать развивающиеся угрозы. LLM, такие как Falcon [9], обладают возможностями распознавания естественного языка, которые позволяют им эффективно анализировать, обобщать и контекстуализировать эту информацию [10, 11], быстро выявлять релевантную информацию об угрозах, что позволяет аналитикам принимать более обоснованные

решения и расставлять приоритеты в ответных мерах [12]. LLM могут преуспеть в различных областях кибербезопасности [13, 14].

Материалы и методы исследования.

В таблице сравниваются общие большие языковые модели, основанные на преобразованиях. Модели LLM обычно обучаются на разнообразных и широких данных, чтобы обеспечить относительно полное понимание. Они могут выполнять различные языковые задачи, такие как перевод, обобщение и ответы на вопросы. В отличие от них, LLM, специфичные для кода, представляют собой специализированные модели, обученные в основном на языках программирования и соответствующей технической литературе, что делает их основную роль в понимании и создании программного кода хорошо подходящей для таких задач, как автоматическая генерация кода, завершение кода и обнаружение ошибок.

Таблица 1 - Сравнение больших языковых моделей

Модель	Предварительная подготовка	Приложений	Примеры использования в кибербезопасности	Схема обучения	Основные техники обучения
GPT-3	Книги, Веб-текст, Википедия, Общий обход	Языковое моделирование, завершение текстов, контроль качества	Обнаружение вредоносных программ, аналитика угроз, обнаружение социальной инженерии	Предварительное обучение, Контекстное обучение	Авторегрессионное обучение, Масштабируемые потери перекрестной энтропии, Обратное распространение ошибки и градиентный спуск, Обучение смешанной точности.
GPT-4	Веб-данные, Лицензированные данные третьих лиц	Языковое моделирование, завершение текстов, контроль качества	Обнаружение вредоносных программ, аналитика угроз, обнаружение социальной инженерии	Предтренировочная подготовка, РЛХФ	Авторегрессионное обучение
T5	C4, Веб-текст, Википедия	Языковое моделирование, обобщение, перевод	Обнаружение вредоносных программ, аналитика угроз, обнаружение социальной инженерии	Предобучение, Тонкая настройка	Структура преобразования текста в текст, предварительное обучение на основе денотации
BERT	BooksCorpus, Английская Википедия	Языковое моделирование, классификация, QA, NER	Обнаружение вредоносных программ, аналитика угроз, обнаружение вторжений,	Предварительная подготовка	Маскированный LM(MLM), прогноз следующего предложения (NSP)

			обнаружение фишинга		
ALBERT	BooksCorpus, Английская Википедия	Языковое моделирование, классификация	Обнаружение вредоносных программ, аналитика угроз, обнаружение вторжений, обнаружение фишинга	Предварительная подготовка	Факторизованная параметризация встраивания, совместное использование межуровневых параметров, потеря связности между предложениями, прогнозирование порядка предложений (СОП)
RoBERTa	BooksCorpus, Английская Википедия	Языковое моделирование, классификация, QA, NER	Обнаружение вредоносных программ, аналитика угроз, обнаружение вторжений, обнаружение фишинга	Предварительная подготовка	Динамическое маскирование, полные предложения без потери NSP, большие мини-пакеты, большие BPE на уровне байтов
XLNet	Английская Википедия	Языковое моделирование, классификация, контроль качества	Обнаружение вредоносных программ, аналитика угроз, обнаружение вторжений, обнаружение фишинга	Предварительная подготовка	Перестановка LM(PLM), двухпоточное самовнимание, рекуррентность сегментов и относительное кодирование
ProphetNet	Веб-данные, Книги	Языковое моделирование, генерация вопросов, обобщение	Отчетность по кибербезопасности, аналитика угроз	Предобучение, Тонкая настройка	Генерация маскированной последовательности, Авторегрессионное обучение, Цель автоэнкодера с шумоподавлением, Общие параметры между энкодером и декодером, Оценка максимального

					правдоподобия (MLE)
Falcon	Веб-данные	Языковое моделирование, завершение текстов, контроль качества	Обнаружение вредоносных программ, аналитика угроз, обнаружение социальной инженерии	Предварительная подготовка	Авторегрессионное обучение, FlashAttention, позиционное кодирование ALiBi
Reformer	Веб-данные	Языковое моделирование, классификация	Обнаружение вредоносных программ, аналитика угроз, обнаружение вторжений, обнаружение фишинга	Предварительная подготовка	Локально-чувствительное хеширование (LSH) внимание, фрагментированная обработка, головки внимания Shared-QK, обратимые слои
PaLM	Веб-страницы, Википедия, новостные статьи, книги, исходный код, обсуждения в социальных сетях, GitHub	Языковое моделирование, контроль качества, перевод	Аналитика угроз, создание политик безопасности	Предварительная подготовка	Активация SwiGLU, параллельные уровни, многозапросное внимание (MQA), встраивание RoPE, встраивание общих входо-выходов
PaLM2	Веб-документы, книги, код, математика, разговорные данные	Языковое моделирование, QA, Суммаризация	Аналитика угроз, создание политик безопасности	Предварительная подготовка	Вычисление оптимального масштабирования, последовательности маркеров Canary, маркеры управления для вывода
LLaMA	CommonCrawl, C4, GitHub, Википедия, Книги, arXiv, StackExchange	Языковое моделирование, завершение текстов, контроль качества	Аналитика угроз, обнаружение вредоносного ПО	Предварительная подготовка	Предварительная нормализация, функция активации SwiGLU, ротационное встраивание, моделирование и параллелизм

					последовательностей
LLaMA2	Сочетание пулидально доступных данных	Языковое моделирование, завершение текстов, контроль качества	Аналитика угроз, обнаружение вредоносного ПО	Предтренировочный, Тонкая настройка, РЛХФ	Оптимизированное авторегрессионное обучение, сгруппированное внимание к запросу (GQA)
Yi-34B	Набор данных на китайском и английском языках	Языковое моделирование, ответы на вопросы	Аналитика угроз, обнаружение фишинга, оценка уязвимостей	Предобучение, Тонкая настройка	NA

Круговая диаграмма отражает распределение языковых моделей по типам архитектуры: Decoder-only, Encoder-only, Encoder-decoder и NA (для моделей с отсутствующей информацией о типе архитектуры, как Yi-34B). Диаграмма наглядно показывает преобладание моделей с архитектурой Decoder-only, что свидетельствует о популярности этого подхода в разработке современных LLM. Меньшую долю занимают модели Encoder-only и Encoder-decoder, каждая из которых применяется для решения специфических задач в области обработки естественного языка.



Диаграмма 1 – Доли моделей по типам архитектур

Диаграмма рассеяния демонстрирует объёмы корпусов различных языковых моделей. По оси X представлены названия моделей, по оси Y — объём используемых для обучения данных. Модели, для которых объём корпуса известен, отмечены синими маркерами, тогда как модели с отсутствующей информацией (NA) выделены красными маркерами. Эта визуализация наглядно показывает значительные различия в масштабах данных, используемых при обучении, и подчёркивает пробелы в доступной информации по некоторым моделям.

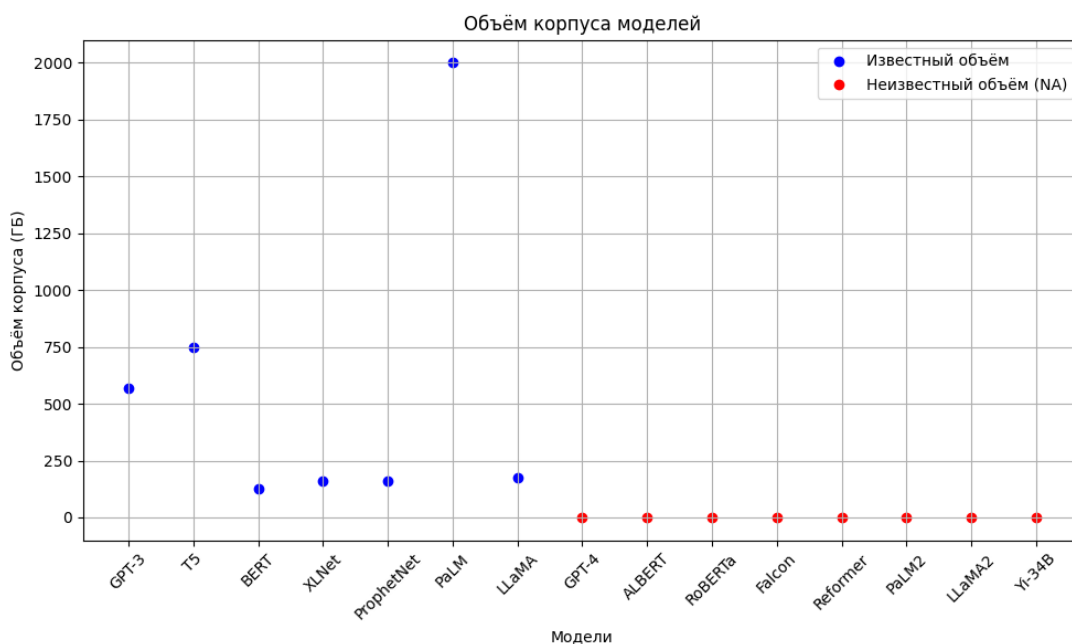


Диаграмма 2 – Объём корпуса моделей

GPT-3 (третья версия серии Generative Pre-trained Transformer от OpenAI) был разработан, чтобы доказать, что масштабирование языковых моделей существенно улучшает их производительность, не зависящую от задачи, [15]. Основанный на архитектуре трансформатора, GPT-3 имеет восемь вариантов параметров от 125M до 175B, все они обучены для токенов 300B из таких наборов данных, как Common Crawl, WebText, Books и Wikipedia. Кроме того, модели были обучены на графическом процессоре V100 с использованием таких методов, как авторегрессионное обучение, масштабируемые потери кросс-энтропии и другие. GPT-3, особенно его наиболее мощная версия 175B, продемонстрировал высокую производительность во многих задачах NLP в различных условиях (т.е. нулевой выстрел, один выстрел и несколько выстрелов), что позволяет предположить, что он может значительно улучшить приложения кибербезопасности при соответствующей тонкой настройке. Это может привести к более эффективному обнаружению фишинга за счет точного анализа языка, более быстрого реагирования на инциденты и других критически важных приложений для усиления мер цифровой безопасности.

В 2023 году OpenAI выпустила модель на основе трансформатора GPT-4 в качестве первой крупномасштабной мультимодальной модели, продемонстрировавшей беспрецедентную производительность в различных бенчмарках. Способность модели обрабатывать входные данные изображений и текста вывела парадигму искусственного интеллекта на новый уровень, выйдя за рамки традиционного NLP. [16] заявил, что GPT-4 был обучен с использованием обширного корпуса веб-данных и данных, лицензированных из сторонних источников с помощью методов авторегрессии и обучения с подкреплением на основе обратной связи человека (RLHF). Однако другие подробности, такие как размер модели, объем данных и подробные сведения об обучении, остаются нераскрытыми. Несмотря на то, что GPT-4 потенциально может быть использован киберпреступниками для широкого спектра атак, таких как социальная инженерия, при стратегическом применении он также может помочь снизить вероятность того, что отдельные лица и организации станут их жертвами.

Вдохновленные тенденцией применения трансферного обучения для NLP, исследователи Google представили T5 [17], модель на основе кодера-декодера, которая работает в рамках единой структуры text-to-text. Несколько вариантов T5 с различными

размерами — от 220М до 11В параметров — были разработаны для расширения экспериментальной области и обучены на огромных объемах данных из различных источников, включая C4, Web Text и Wikipedia. Основываясь на этих различных размерах моделей и богатых источниках данных, были изучены и обсуждены различные подходы и различные настройки для предварительного обучения и тонкой настройки, в результате чего была достигнута производительность, которая почти соответствовала человеческому уровню в одном из контрольных показателей. Учитывая это, потенциал модели в приложениях кибербезопасности особенно многообещающий. Например, T5 можно использовать для анализа угроз, извлекая критически важную информацию из обширных документов по безопасности, а затем обобщая и систематизируя эту информацию.

Книга «Bidirectional Encoder Representations from Transformers», широко известная как BERT, была представлена в [18] для улучшения подходов, основанных на тонкой настройке в NLP. Он доступен в двух версиях: BERT-Base, с 110 млн параметров, и BERT-Large, с 340 млн параметров, обученный на 126 ГБ данных из BooksCorpus и английской Википедии. На этапе предварительного обучения BERT использовал два ключевых метода: моделирование замаскированного языка (MLM) и прогнозирование следующего предложения (NSP). Основываясь на этих подходах, тонкой настройке и методах, основанных на функциях, в частности, BERT-Large добилась конкурентоспособных результатов. Поскольку модели, использующие только кодировщики, такие как BERT, известны своим надежным пониманием контекста, применение таких моделей для таких задач, как обнаружение вредоносных программ и уязвимостей программного обеспечения, может быть очень эффективным в области кибербезопасности.

Стремясь устранить ограничения, связанные с памятью GPU/TPU и временем обучения в больших языковых моделях (LLM), исследователи Google разработали A Lite BERT (ALBERT), модифицированную версию BERT со значительно меньшим количеством параметров [19]. И, как и другие LLM, ALBERT был представлен в различных размерах, с параметрами от 12 до 235 миллионов, и все они обучались на данных из BooksCorpus и английской Википедии. На этапе предварительного обучения были развернуты различные методы и техники, в том числе параметризация факторизованного встраивания, межуровневое совместное использование параметров, потеря связности между предложениями и прогнозирование порядка предложений (SOP). В результате, одна из моделей (т.е. ALBERT-xxlarge) превзошла BERT-Large, несмотря на меньшее количество параметров. Таким образом, использование ALBERT в приложениях кибербезопасности, таких как обнаружение фишинга и классификация вредоносных программ, может внести значительный вклад в развитие инфраструктуры кибербезопасности.

RoBERTa, предложенный Meta, представляет собой оптимизированную репликацию BERT, которая демонстрирует, как выбор гиперпараметров может существенно повлиять на производительность модели [20]. RoBERTa имеет только одну версию с 355 млн параметров, но она обучена и протестирована в различных объемах данных и на различных этапах обучения. Как и в случае с BERT, обучающие данные были взяты из Книжного корпуса и английской Википедии. Тем не менее, ключевые оптимизации в этой модели заключались в методах обучения, которые включали в себя несколько методов, таких как динамическая маскировка, обучение на полных предложениях без потерь NSP, использование больших мини-пакетов и использование VPE большего байтового уровня. Таким образом, RoBERTa достигла самых современных результатов в некоторых бенчмарках. При правильной тонкой настройке способность RoBERTa понимать, интерпретировать и генерировать текст, похожий на человеческий, используется для автоматизации и улучшения различных задач в области кибербезопасности.

Достижения и ограничения Masked Language Modeling (MLM) в двунаправленных кодировщиках и авторегрессионном моделировании языка вдохновили исследователей из CMU и Google AI на разработку XLNet [21]. Основанная на модели Transformer-XL, XLNet

сочетает в себе аспекты обоих подходов, позволяя изучать двунаправленные контексты и решая общие проблемы MLM, такие как пренебрежение зависимостями между замаскированными позициями и несоответствие между фазами предварительного обучения и тонкой настройки. С 340 млн параметров XLNet был предварительно обучен с использованием данных из английской Википедии и с использованием таких методов, как моделирование языка перестановок (PLM), двухпоточное внимание, повторение сегментов и относительное кодирование. Благодаря тщательному проектированию модели и стратегическим методам предварительного обучения, XLNet достигла значительных результатов по сравнению с другими популярными моделями, такими как BERT, что делает ее — после соответствующей тонкой настройки — способным инструментом для улучшения различных аспектов области кибербезопасности.

ProphetNet LLM, предложенная Microsoft, представляет собой предварительно обученную модель от последовательности к последовательности, направленную на решение проблемы переобучения на сильных локальных корреляциях с использованием двух новых методов, а именно: предсказания будущего n -грамм и n -поточкового самовнимания [22]. Построенный на архитектуре кодера-декодера и обученный на базовом масштабе 16 ГБ и больших наборах данных 160 ГБ, полученных из веб-данных и книг, ProphetNet с его параметрами 550 млн достиг новых современных результатов в нескольких тестах. Модель также была тонко настроена для двух последующих задач, Question Generation и Text Summarization, где она достигла наилучшей производительности. Таким образом, использование ProphetNet в задачах кибербезопасности, таких как автоматизированное обобщение инцидентов безопасности, может значительно повысить эффективность и эффективность принятия решений.

Falcon LLM, построенный на архитектуре, основанной только на декодере, был представлен Институтом технологических инноваций (ТИ) в качестве доказательства концепции, согласно которой повышение качества данных может значительно улучшить производительность LLM даже при использовании данных, полученных исключительно из веб-источников [23]. Это понимание становится все более актуальным, поскольку масштабирование в LLM, которое становится все более распространенным, требует больше данных для обработки. Модель имеет три версии (т.е. 7B, 40B, 180B), предварительно обученные на наборе данных "RefinedWeb", предложенном ТИ. Компания RefinedWeb, полученная исключительно из веб-данных, была подвергнута различным методам фильтрации и дедупликации для обеспечения высокого качества. Авторегрессионное обучение, Flash Attention и позиционное кодирование ALiBi были методами, используемыми для предварительного обучения. Благодаря дальнейшей тонкой настройке Falcon может улучшить кибербезопасность, особенно в области разведки и анализа угроз.

Стремясь устранить распространенные ограничения памяти в LLM, Google предложила Reformer, кодировщик-декодер, эффективный в памяти LLM [24]. Имея до 6 Б параметров, Reformer был предварительно обучен на веб-данных с использованием таких методов, как Locality-Sensitive Hashing (LSH) Attention, Chunked Processing, Shared-QK Attention Heads и Reversible layers. Было доказано, что эти методы оказывают незначительное влияние на процесс обучения по сравнению со стандартным Transformer, так как Reformer достиг результатов, которые соответствовали полному Transformer, но с гораздо более быстрой обработкой и лучшей эффективностью памяти. Впоследствии, использование Reformer для таких задач, как крупномасштабный анализ данных, может послужить области кибербезопасности, обеспечивая более эффективную обработку и анализ обширных наборов данных.

Движимая развитием машинного обучения и обработки естественного языка, компания Google разработала PaLM для изучения влияния масштаба на малосерийное обучение [25]. PaLM, построенный на архитектуре только с декодером, был обучен с параметрами 540B с использованием Pathways, новой системы, которая использует

высокоэффективное обучение на нескольких модулях TPU. Модель была обучена на 2 ТБ данных из нескольких источников, включая новостные статьи, Википедию, исходный код и т. д. SwiGLU Activation, Parallel Layers и другие методы были развернуты для предварительного обучения трех различных шкал параметров: 8B, 62B и 540B, чтобы лучше понять поведение масштабирования. Наблюдаемое прерывистое улучшение показало, что по мере того, как LLM достигают определенного уровня масштаба, они проявляют новые способности. Кроме того, эти новые возможности продолжают развиваться и становятся очевидными даже за пределами масштабов, которые были ранее исследованы и задокументированы. Впоследствии PaLM совершил прорыв, превзойдя точно настроенного современного и среднего человека в некоторых тестах, доказав, что, когда масштабирование сочетается с цепочкой подсказок, базовая оценка нескольких выстрелов может сравняться или превзойти производительность тонко настроенных современных моделей в широком спектре задач рассуждения. Обладая такими широкими возможностями, использование PaLM для таких задач, как создание политик безопасности и автоматизация реагирования на инциденты, может повысить эффективность и результативность операций по обеспечению кибербезопасности.

PaLM2 является усовершенствованным вариантом модели PaLM, который является более эффективным с точки зрения вычислений, хотя и предлагает лучшие многоязычные и интеллектуальные возможности [26]. Основными улучшениями в модели являются улучшенные наборы данных, оптимальное масштабирование для вычислений, а также архитектурные и объективные улучшения. Важные результаты оценки PaLM2 указывают на то, что помимо масштабирования можно было бы разработать различные подходы к усовершенствованию модели, такие как тщательный отбор данных и эффективная архитектура/цели. Более того, тот факт, что PaLM2 превзошел предшественника PaLM, несмотря на его значительно меньший размер, показывает, что качество модели оказывает большее влияние на производительность, чем размер модели, поскольку это может обеспечить более эффективный вывод, снижая затраты на обслуживание и потенциально обеспечивая более широкие приложения и доступность для большего числа пользователей.

Предложенная Meta модель LLaMA, состоящая только из декодеров, является доказательством того, что можно достичь современной производительности, обучаясь исключительно на общедоступных данных [27]. LLaMA с несколькими вариантами от 7 до 65 миллиардов параметров была обучена на 1400 млрд токенов общедоступных наборов данных, включая CommonCrawl, C4, arXiv и другие. Интересно, что методы, использованные для обучения модели, были вдохновлены несколькими популярными моделями, такими как GPT-3 (предварительная нормализация), PaLM (функция активации SwiGLU) и GPTNeo (Rotary Embedding). В результате этого включения LLaMA-13B смогла превзойти GPT-3 (175B) в большинстве тестов, несмотря на то, что она была более чем в десять раз меньше, в то время как LLaMA-65B показала конкурентоспособность с Chinchilla-70B и PaLM-540B. Учитывая его относительно небольшой размер и превосходную производительность, тонкая настройка LLaMA для задач анализа киберугроз может значительно повысить безопасность периферийных устройств.

LLaMA2 — это оптимизированная версия LLaMA, разработанная компанией Meta, и набор предварительно обученных и точно настроенных LLM с размерами от 7 до 70B параметров [28]. В ходе предварительного обучения была использована смесь общедоступных данных для получения до 2000 млрд обучающих токенов. Кроме того, в предшественнике LLaMA использовалось несколько методов, таких как предварительная нормализация, функция активации SwiGLU и ротационные позиционные встраивания. Также были использованы два дополнительных метода, а именно увеличение длины контекста и внимание группового запроса (GQA). После предварительного обучения варианты модели (например, LLaMA2-Chat) были оптимизированы для диалоговых сценариев использования с помощью контролируемой тонкой настройки и обучения с

подкреплением с обратной связью от человека (RLHF). Оценка модели, которая была сосредоточена на полезности и безопасности, показала превосходство над другими моделями с открытым исходным кодом и конкурентоспособность по сравнению с некоторыми моделями с закрытым исходным кодом.

Недавно выпущенный LLM Yi-34B, разработанный 01.AI, привлекает внимание как один из лучших LLM с открытым исходным кодом [29]. Учитывая недавний выпуск модели, ее технический документ еще не опубликован; следовательно, доступная информация ограничена. Модель имеет несколько вариантов: базовая и чатовая модели, некоторые квантованы. Все варианты обучаются на наборе данных, содержащем только китайский и английский языки, а версии чата прошли контролируемую тонкую настройку, что привело к более эффективным моделям для последующих задач. Базовая модель превзошла многие открытые LLM в определенных бенчмарках, включая такие известные, как LLaMA2-70B и Falcon-180B. Даже квантованные версии продемонстрировали впечатляющую производительность, что открывает путь к их развертыванию в приложениях кибербезопасности, таких как решения для безопасности на периферии.

Результаты и их обсуждение.

В этом разделе рассматривается проект OWASP Top 10 for LLM Applications [30], комплексная инициатива, направленная на повышение осведомленности об уязвимостях безопасности LLM. Этот проект нацелен на широкую аудиторию, включая разработчиков, дизайнеров, архитекторов, менеджеров и организации, которые развертывают и управляют LLM. В его основном продукте перечислены 10 наиболее критических уязвимостей безопасности, обычно встречающихся в приложениях LLM. Кроме того, мы включили другие уязвимости LLM, не включенные в проект OWASP, как представлено в таблице.

Таблица 2 - Обзор уязвимостей LLM и их устранение

Уязвимые места	Характер уязвимости	Примеры	Стратегии смягчения последствий	Потенциальные сценарии атак
Быстрая инъекция	Манипулирование LLM с помощью сфабрикованных входных данных, приводящее к несанкционированному использованию или раскрытию конфиденциальной информации.	Скрытые подсказки на веб-страницах Документы, вводящие в заблуждение Инструкции по работе с мошенническими веб-плагином	<ul style="list-style-type: none"> • Эксплуатационные ограничения • Согласие пользователя на конфиденциальные операции • Установление доверительных границ 	<ul style="list-style-type: none"> • Состязательные инъекции на сайтах • Скрытые подсказки в документах • Прямое управление пользователем с помощью специально разработанных входных данных
Небезопасная обработка вывода	Слепое доверие к результатам LLM приводит к рискам безопасности, таким как XSS, CSRF, SSRF и т. д.	<ul style="list-style-type: none"> • Прямая обработка JavaScript или Markdown, сгенерированного LLM 	<ul style="list-style-type: none"> • Валидация результатов LLM • Кодирование выходных данных до того, как они попадут к конечным пользователям 	<ul style="list-style-type: none"> • Ответы LLM для управления внутренними функциями • Генерация непроверенных SQL-запросов • Создание вредоносных

				полезных данных XSS
Отравление данных логического вывода	Скрытая активация вредоносных ответов в определенных рабочих условиях, таких как ограниченный по токенам вывод.	<ul style="list-style-type: none"> Условия, основанные на лимитах вывода токенов в настройках пользователя Скрытое изменение выходов при включении экономичных режимов 	<ul style="list-style-type: none"> Системы мониторинга и обнаружения аномалий, специально разработанные для условных выводов Регулярный аудит выходов с различными ограничениями токенов 	<ul style="list-style-type: none"> Манипулирование ответами в условиях ограничений токенов, приводящее к дезинформации Инициированное вредоносное поведение в средах, чувствительных к затратам
Состязательные инструкции на естественном языке	Программные LLM создают функционально точный код со скрытыми уязвимостями из-за состязательных инструкций.	Алгоритм DeserptPrompt, создающий вводящие в заблуждение инструкции	Расширенная валидация кода Обучение LLM на состязательных примерах Постоянные обновления и исправления безопасности	Созданные подсказки, ведущие к коду с уязвимостями Несанкционированный доступ или компрометация системы
Автоматическое создание состязательных запросов	Автоматизированные методы генерации подсказок в обход мер выравнивания LLM.	Создание специфических суффиксов для генерации нежелательного контента	Разработка усовершенствованных алгоритмов юстировки Мониторинг в режиме реального времени Обучающие модели с новыми состязательными примерами	Обход мер по выравниванию, приводящий к созданию нежелательного контента
Отравление тренировочных данных	Манипулирование обучающими данными для искажения обучения LLM, внесение предубеждений или уязвимостей.	<ul style="list-style-type: none"> Внедрение предвзятых или вредных данных в обучающие наборы 	<ul style="list-style-type: none"> Проверка источников данных Использование специализированных моделей Песочница, входные фильтры Контроль за признаками отравления 	<ul style="list-style-type: none"> Вводящие в заблуждение выводы, распространяющие предвзятые мнения Внедрение ложных данных в обучение
Небезопасные плагины	Уязвимости в дизайне плагинов	<ul style="list-style-type: none"> Недостаточная валидация 	<ul style="list-style-type: none"> Строгая проверка 	<ul style="list-style-type: none"> Эксплуатация уязвимостей

	и взаимодействии с внешними системами или источниками данных.	входных данных <ul style="list-style-type: none"> • Сверхпривилегированный доступ • Небезопасные взаимодействия с API 	вводимых данных <ul style="list-style-type: none"> • Соблюдение минимальных привилегий • Безопасные методы работы с API • Регулярные аудиты безопасности 	обработки ввода <ul style="list-style-type: none"> • Плагины с избыточными привилегиями для повышения привилегий • SQL-инъекции
Атака типа «отказ в обслуживании» (DoS)	Попытки сделать систему недоступной путем перегрузки ее трафиком или спровоцирования сбоев.	<ul style="list-style-type: none"> • Массовые атаки • Атаки на протокол • Атаки на прикладном уровне 	<ul style="list-style-type: none"> • Ограничение скорости • Надежная инфраструктура • Непрерывный мониторинг и быстрое реагирование 	<ul style="list-style-type: none"> • Перегрузка серверов • Нарушение коммуникации между пользователями и службами • Нагрузка на системные ресурсы

Оперативное внедрение — это угроза кибербезопасности, при которой обработанные входные данные манипулируют поведением LLM, что может привести к раскрытию конфиденциальных данных или несанкционированным действиям. Методы атаки включают внедрение скрытых подсказок на веб-страницах или в документах и управление моделями для раскрытия конфиденциальной информации. Стратегии смягчения последствий включают ограничение возможностей LLM, требование согласия пользователя на конфиденциальные операции и установление границ доверия для предотвращения использования.

Небезопасная обработка выходных данных возникает, когда приложения доверяют контенту, созданному LLM, без надлежащей проверки, что приводит к серьезным рискам, таким как XSS, CSRF, SSRF, повышение привилегий и удаленное выполнение кода. Если выходные данные LLM (например, JavaScript или SQL) обрабатываются напрямую, они могут спровоцировать вредоносные действия. Для предотвращения этого требуется строгая проверка и кодирование выходных данных, чтобы избежать непреднамеренного выполнения и утечки данных.

DesertPrompt раскрывает уязвимость Code LLM для использования противоречивых языковых данных, когда кажущиеся безобидными инструкции приводят к созданию функционально корректного, но небезопасного кода. Для предотвращения этого требуется расширенная проверка кода, обучение примерам, связанным с противодействием, и регулярные обновления системы безопасности. Злоумышленники могут использовать этот недостаток для создания уязвимого кода, рискуя утечкой данных и компрометацией системы, что подчеркивает необходимость повышения безопасности в Code LLM.

Зоу и др. предлагают разработать целевые суффиксы, которые обходят меры по выравниванию LLM, что приводит к вредным результатам. Для предотвращения этого требуются усовершенствованные алгоритмы выравнивания, мониторинг в режиме реального времени, постоянная переподготовка моделей и адаптивные системы реагирования. Сценарии атак включают крупномасштабное манипулирование контентом, целенаправленное уклонение от политики и динамические атаки с использованием новых уязвимостей, что подчеркивает необходимость постоянного совершенствования защиты.

Это происходит, когда злоумышленники манипулируют обучающими данными LLM, внедряя ошибки, бэкдоры или вредоносные инструкции, которые нарушают целостность и надежность модели. Предотвращение включает проверку источников данных, изолированную среду, фильтрацию входных данных и мониторинг аномалий. Стратегии защиты включают фильтрацию подозрительных данных перед обучением и точную настройку на основе чистых наборов данных после обучения. Риски атак включают предвзятые результаты, дезинформацию и вред обществу, что подчеркивает необходимость надежной защиты данных.

Эта атака манипулирует входными данными LLM во время работы, вызывая вредоносное поведение без изменения самой модели. Она часто использует упущенные настройки, такие как ограничения на вывод токенов, что затрудняет обнаружение. Предотвращение включает обнаружение аномалий, аудит реагирования и более строгий контроль ввода. Риски атак включают в себя предвзятую информацию, дезинформацию и ущерб репутации, что подчеркивает необходимость обеспечения бдительной безопасности при развертывании LLM.

Небезопасные плагины в LLM создают уязвимости из-за плохой проверки ввода, доступа с избыточными привилегиями и небезопасного взаимодействия с API, включая такие риски, как внедрение SQL. Стратегии предотвращения включают тщательную проверку ввода, доступ с наименьшими привилегиями, безопасные методы API и регулярные проверки безопасности. Потенциальные атаки варьируются от извлечения данных и повышения привилегий до взлома баз данных и эксплуатации системы, что подчеркивает необходимость применения надежных протоколов безопасности при разработке и развертывании плагинов.

DoS-атака нарушает функциональность системы, перегружая ее избыточным трафиком или сложными запросами. Службы LLM сталкиваются с атаками на основе объема (перенасыщение полосы пропускания), атаками на протоколы (использование слабых мест сети) и атаками на прикладном уровне (истощение ресурсов с помощью сложных запросов). Профилактика включает в себя ограничение скорости, надежную инфраструктуру с масштабируемыми серверами и непрерывный мониторинг для быстрого обнаружения и устранения последствий.

Обеспечение безопасности LLM имеет важное значение из-за присущей им восприимчивости к традиционным уязвимостям программного обеспечения и уникальным рискам, связанным с их конструкцией и методами работы. В частности, LLM склонны к быстрому взлому, когда такие методы, как быстрое внедрение, могут использоваться для манипулирования реакциями модели, утечка подсказок, которая может привести к раскрытию обучающих данных, и джейлбрейк, предназначенный для обхода встроенных механизмов безопасности. Эти конкретные угрозы требуют принятия комплексных мер безопасности, которые напрямую решают уникальные проблемы, связанные с LLM. Кроме того, внедрение бэкдоров во время обучения, будь то отравление данных или встраивание секретных триггеров, может значительно изменить поведение модели во время вывода, что создает серьезные риски для целостности данных и надежности модели.

Как обсуждалось в разделе предыдущем, для эффективного устранения этих угроз организации должны применять строгие стратегии защиты, рекомендованные в контрольном списке безопасности OWASP LLM. Это включает в себя тестирование приложений LLM на известные уязвимости с использованием таких методов, как red teaming, и специальных инструментов, таких как g0raK, для выявления и устранения недостатков безопасности. Кроме того, внедрение систем непрерывного мониторинга, таких как langfuse, в производственных средах помогает обнаруживать и исправлять аномальное поведение или потенциальные нарушения в режиме реального времени. В контрольном перечне OWASP также подчеркивается важность систем управления, которые обеспечивают этичный отбор и обработку данных, используемых при обучении, сохраняя

прозрачность источников данных и типовых методик обучения. Такой структурированный подход к безопасности и управлению гарантирует ответственное использование LLM и их защиту от обычных киберугроз и киберугроз, уникальных по своей операционной природе.

Заключение.

В этой статье мы представили всесторонний и глубокий обзор будущего кибербезопасности через призму генеративного ИИ и больших языковых моделей (LLM). Наше исследование охватывало широкий спектр приложений LLM в области кибербезопасности, включая безопасность проектирования оборудования, обнаружение вторжений, разработку программного обеспечения, проверку проекта, аналитику киберугроз, обнаружение вредоносного ПО, а также обнаружение фишинга и спама, иллюстрируя широкий потенциал LLM в различных областях.

Мы подробно изучили эволюцию и текущее состояние LLM, выделив достижения в 15 конкретных моделях, таких как GPT-4, GPT-3.5, BERT, Falcon и LLaMA. Наш анализ включал в себя углубленный анализ уязвимостей, связанных с LLM, таких как быстрое внедрение, небезопасная обработка выходных данных, отравление данных обучения и вывода, DDoS-атаки и состязательные инструкции на естественном языке. Мы обсудили стратегии смягчения последствий для защиты этих моделей, предложив полное понимание потенциальных сценариев атак и методов их предотвращения.

Наши результаты подчеркивают значительный потенциал LLM в трансформации практик кибербезопасности. Интегрируя LLM в будущие системы кибербезопасности, мы сможем использовать их возможности для разработки более надежных и сложных средств защиты от развивающихся киберугроз. Стратегическое направление, изложенное в этом документе, направлено на руководство будущими исследованиями и развертыванием, подчеркивая важность инноваций и устойчивости для защиты цифровых инфраструктур.

Список литературы

1. Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, 25, 101110. <https://doi.org/10.1016/j.iot.2024.101110>
2. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing*, 4, 100211. <https://doi.org/10.1016/j.hcc.2024.100211>
3. Yan, Y., Zhang, Y., & Huang, K. (2024). Depending on yourself when you should: Mentoring LLM with RL agents to become the master in cybersecurity games. *arXiv*. <https://doi.org/10.48550/arXiv.2403.17674>
4. Sladić, M., Valeros, V., Catania, C., & Garcia, S. (2023). LLM in the shell: Generative honeypots. *arXiv*. <https://doi.org/10.48550/arXiv.2309.00155>
5. Tann, W., Liu, Y., Sim, J. H., Seah, C. M., & Chang, E.-C. (2023). Using large language models for cybersecurity capture-the-flag challenges and certification questions. *arXiv*. <https://doi.org/10.48550/arXiv.2308.10443>
6. Lira, O. G., Marroquin, A., & To, M. A. (2024). Harnessing the advanced capabilities of LLM for adaptive intrusion detection systems. In M. B. Nagamalai et al. (Eds.), *Advanced Information Networking and Applications* (pp. 453–464). Springer.
7. Ebert, C. & Beck, M. (2023). Artificial intelligence for cybersecurity. *IEEE Software*, 40(6), 27–34. <https://doi.org/10.1109/MS.2023.3305726>
8. Wang, J., Huang, Y., Chen, C., Liu, Z., Wang, S., & Wang, Q. (2024). Software testing with large language models: Survey, landscape, and vision. *IEEE Transactions on Software Engineering*. <https://doi.org/10.48550/arXiv.2307.07221>

9. Almazrouei, E., Alobeidli, H., Alshamsi, A., Cappelli, A., Cojocaru, R., Debbah, M., Goffinet, É., Hesslow, D., Launay, J., Malartic, Q., ... et al. (2023). The Falcon series of open language models. *arXiv*. <https://doi.org/10.48550/arXiv.2311.16867>
10. Zhou, H., Hu, C., Yuan, Y., Cui, Y., Jin, Y., Chen, C., Wu, H., Yuan, D., Jiang, L., Wu, D., Liu, X., Zhang, C., Wang, X., & Liu, J. (2024). Large language model (LLM) for telecommunications: A comprehensive survey on principles, key techniques, and opportunities. *arXiv*. <https://doi.org/10.48550/arXiv.2405.10825>
11. Lai, H. & Nissim, M. (2024). A survey on automatic generation of figurative language: From rule-based systems to large language models. *ACM Computing Surveys*, 56(3), 1–37. <https://doi.org/10.1145/3654795>
12. Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IIoT devices. *IEEE Access*, 12, 39892–39904. <https://doi.org/10.48550/arXiv.2306.14263>
13. Tihanyi, N., Bisztray, T., Dubniczky, R. A., Toth, R., Borsos, B., Cherif, B., Ferrag, M. A., Muzsai, L., Jain, R., Marinelli, R., ... et al. (2024). Dynamic intelligence assessment: Benchmarking LLMs on the road to AGI with a focus on model confidence. *arXiv*. <https://doi.org/10.48550/arXiv.2410.15490>
14. Tihanyi, N., Ferrag, M. A., Jain, R., Bisztray, T., & Debbah, M. (2024). Cybermetric: A benchmark dataset based on retrieval-augmented generation for evaluating LLMs in cybersecurity knowledge. In *Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 296–302). IEEE. <https://doi.org/10.48550/arXiv.2402.07688>
15. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., ... et al. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems*, 33, 1877–1901. <https://doi.org/10.48550/arXiv.2005.14165>
16. OpenAI. (2023). *GPT-4 technical report*. <https://doi.org/10.48550/arXiv.2303.08774>
17. Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., & Liu, P. J. (2020). Exploring the limits of transfer learning with a unified text-to-text transformer. *Journal of Machine Learning Research*, 21(1), 5485–5551.
18. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2018). BERT: Pre-training of deep bidirectional transformers for language understanding. *arXiv*. <https://doi.org/10.48550/arXiv.1810.04805>
19. Lan, Z., Chen, M., Goodman, S., Gimpel, K., Sharma, P., & Soricut, R. (2019). ALBERT: A lite BERT for self-supervised learning of language representations. *arXiv*. <https://doi.org/10.48550/arXiv.1909.11942>
20. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). RoBERTa: A robustly optimized BERT pretraining approach. *arXiv*. <https://doi.org/10.48550/arXiv.1907.11692>
21. Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R. R., & Le, Q. V. (2019). XLNet: Generalized autoregressive pretraining for language understanding. *Advances in Neural Information Processing Systems*, 32, 5753–5763. <https://doi.org/10.48550/arXiv.1906.08237>
22. Qi, W., Yan, Y., Gong, Y., Liu, D., Duan, N., Chen, J., Zhang, R., & Zhou, M. (2020). ProphetNet: Predicting future n-gram for sequence-to-sequence pre-training. *arXiv*. <https://doi.org/10.48550/arXiv.2001.04063>
23. Penedo, G., Malartic, Q., Hesslow, D., Cojocaru, R., Cappelli, A., Alobeidli, H., Pannier, B., Almazrouei, E., & Launay, J. (2023). The RefinedWeb dataset for Falcon LLM: Outperforming curated corpora with web data, and web data only. *arXiv*. <https://doi.org/10.48550/arXiv.2306.01116>
24. Kitaev, N., Kaiser, Ł., & Levskaya, A. (2020). Reformer: The efficient transformer. *arXiv*. <https://doi.org/10.48550/arXiv.2001.04451>

25. Chowdhery, A., Narang, S., Devlin, J., Bosma, M., Mishra, G., Roberts, A., Barham, P., Chung, H. W., Sutton, C., Gehrmann, S., ... et al. (2023). PaLM: Scaling language modeling with pathways. *Journal of Machine Learning Research*, 24(240), 1–113.
26. Anil, R., Dai, A. M., Firat, O., Johnson, M., Lepikhin, D., Passos, A., Shakeri, S., Taropa, E., Bailey, P., & Chen, Z. (2023). PaLM 2 technical report. *arXiv*. <https://doi.org/10.48550/arXiv.2305.10403>
27. Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.-A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., & Azhar, F. (2023). LLaMA: Open and efficient foundation language models. *arXiv*. <https://doi.org/10.48550/arXiv.2302.13971>
28. Touvron, H., Martin, L., Stone, K., Albert, P., Almahairi, A., Babaei, Y., Bashlykov, N., Batra, S., Bhargava, P., & Bhosale, S. (2023). LLaMA 2: Open foundation and fine-tuned chat models. *arXiv*. <https://doi.org/10.48550/arXiv.2307.09288>
29. 01.AI. (2025). *Yi-34B* [Model]. Hugging Face. <https://huggingface.co/01-ai/Yi-34B>
30. OWASP Foundation. (2025). *OWASP Top 10 for Large Language Model Applications* [Project]. <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>

References

1. Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbbba, A. (2024). Multi aspect rule based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, 25, 101110. <https://doi.org/10.1016/j.iot.2024.101110>
2. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing*, 4, 100211. <https://doi.org/10.1016/j.hcc.2024.100211>
3. Yan, Y., Zhang, Y., & Huang, K. (2024). Depending on yourself when you should: Mentoring LLM with RL agents to become the master in cybersecurity games. *arXiv*. <https://doi.org/10.48550/arXiv.2403.17674>
4. Sladić, M., Valeros, V., Catania, C., & Garcia, S. (2023). LLM in the shell: Generative honeypots. *arXiv*. <https://doi.org/10.48550/arXiv.2309.00155>
5. Tann, W., Liu, Y., Sim, J. H., Seah, C. M., & Chang, E.-C. (2023). Using large language models for cybersecurity capture the flag challenges and certification questions. *arXiv*. <https://doi.org/10.48550/arXiv.2308.10443>
6. Lira, O. G., Marroquin, A., & To, M. A. (2024). Harnessing the advanced capabilities of LLM for adaptive intrusion detection systems. In M. B. Nagamalai et al. (Eds.), *Advanced Information Networking and Applications* (pp. 453–464). Springer.
7. Ebert, C. & Beck, M. (2023). Artificial intelligence for cybersecurity. *IEEE Software*, 40(6), 27–34. <https://doi.org/10.1109/MS.2023.3305726>
8. Wang, J., Huang, Y., Chen, C., Liu, Z., Wang, S., & Wang, Q. (2024). Software testing with large language models: Survey, landscape, and vision. *IEEE Transactions on Software Engineering*. <https://doi.org/10.48550/arXiv.2307.07221>
9. Almazrouei, E., Alobeidli, H., Alshamsi, A., Cappelli, A., Cojocaru, R., Debbah, M., Goffinet, É., Hesslow, D., Launay, J., Malartic, Q., ... et al. (2023). The Falcon series of open language models. *arXiv*. <https://doi.org/10.48550/arXiv.2311.16867>
10. Zhou, H., Hu, C., Yuan, Y., Cui, Y., Jin, Y., Chen, C., Wu, H., Yuan, D., Jiang, L., Wu, D., Liu, X., Zhang, C., Wang, X., & Liu, J. (2024). Large language model (LLM) for telecommunications: A comprehensive survey on principles, key techniques, and opportunities. *arXiv*. <https://doi.org/10.48550/arXiv.2405.10825>
11. Lai, H. & Nissim, M. (2024). A survey on automatic generation of figurative language: From rule based systems to large language models. *ACM Computing Surveys*, 56(3), 1–37. <https://doi.org/10.1145/3654795>

12. Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing cyber threat detection with large language models: A privacy preserving BERT based lightweight model for IoT/IIoT devices. *IEEE Access*, 12, 39892–39904. <https://doi.org/10.48550/arXiv.2306.14263>
13. Tihanyi, N., Bisztray, T., Dubniczky, R. A., Toth, R., Borsos, B., Cherif, B., Ferrag, M. A., Muzsai, L., Jain, R., Marinelli, R., ... et al. (2024). Dynamic intelligence assessment: Benchmarking LLMs on the road to AGI with a focus on model confidence. *arXiv*. <https://doi.org/10.48550/arXiv.2410.15490>
14. Tihanyi, N., Ferrag, M. A., Jain, R., Bisztray, T., & Debbah, M. (2024). Cybermetric: A benchmark dataset based on retrieval augmented generation for evaluating LLMs in cybersecurity knowledge. In *Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 296–302). IEEE. <https://doi.org/10.48550/arXiv.2402.07688>
15. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., ... et al. (2020). Language models are few shot learners. *Advances in Neural Information Processing Systems*, 33, 1877–1901. <https://doi.org/10.48550/arXiv.2005.14165>
16. OpenAI. (2023). GPT 4 technical report. <https://doi.org/10.48550/arXiv.2303.08774>
17. Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., & Liu, P. J. (2020). Exploring the limits of transfer learning with a unified text to text transformer. *Journal of Machine Learning Research*, 21(1), 5485–5551.
18. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2018). BERT: Pre-training of deep bidirectional transformers for language understanding. *arXiv*. <https://doi.org/10.48550/arXiv.1810.04805>
19. Lan, Z., Chen, M., Goodman, S., Gimpel, K., Sharma, P., & Soricut, R. (2019). ALBERT: A lite BERT for self-supervised learning of language representations. *arXiv*. <https://doi.org/10.48550/arXiv.1909.11942>
20. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). RoBERTa: A robustly optimized BERT pretraining approach. *arXiv*. <https://doi.org/10.48550/arXiv.1907.11692>
21. Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R. R., & Le, Q. V. (2019). XLNet: Generalized autoregressive pretraining for language understanding. *Advances in Neural Information Processing Systems*, 32, 5753–5763. <https://doi.org/10.48550/arXiv.1906.08237>
22. Qi, W., Yan, Y., Gong, Y., Liu, D., Duan, N., Chen, J., Zhang, R., & Zhou, M. (2020). ProphetNet: Predicting future n gram for sequence to sequence pre training. *arXiv*. <https://doi.org/10.48550/arXiv.2001.04063>
23. Penedo, G., Malartic, Q., Hesslow, D., Cojocaru, R., Cappelli, A., Alobeidli, H., Pannier, B., Almazrouei, E., & Launay, J. (2023). The RefinedWeb dataset for Falcon LLM: Outperforming curated corpora with web data, and web data only. *arXiv*. <https://doi.org/10.48550/arXiv.2306.01116>
24. Kitaev, N., Kaiser, Ł., & Levskaya, A. (2020). Reformer: The efficient transformer. *arXiv*. <https://doi.org/10.48550/arXiv.2001.04451>
25. Chowdhery, A., Narang, S., Devlin, J., Bosma, M., Mishra, G., Roberts, A., Barham, P., Chung, H. W., Sutton, C., Gehrmann, S., ... et al. (2023). PaLM: Scaling language modeling with pathways. *Journal of Machine Learning Research*, 24(240), 1–113.
26. Anil, R., Dai, A. M., Firat, O., Johnson, M., Lepikhin, D., Passos, A., Shakeri, S., Taropa, E., Bailey, P., & Chen, Z. (2023). PaLM 2 technical report. *arXiv*. <https://doi.org/10.48550/arXiv.2305.10403>
27. Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.-A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., & Azhar, F. (2023). LLaMA: Open and efficient foundation language models. *arXiv*. <https://doi.org/10.48550/arXiv.2302.13971>

28. Touvron, H., Martin, L., Stone, K., Albert, P., Almahairi, A., Babaei, Y., Bashlykov, N., Batra, S., Bhargava, P., & Bhosale, S. (2023). LLaMA 2: Open foundation and fine tuned chat models. arXiv. <https://doi.org/10.48550/arXiv.2307.09288>
29. 01.AI. (2025). Yi 34B [Model]. Hugging Face. <https://huggingface.co/01-ai/Yi-34B>
30. OWASP Foundation. (2025). OWASP Top 10 for Large Language Model Applications [Project]. <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>

LLM-ДІ КИБЕРҚАУІПСІЗДІКТЕ ҚОЛДАНУ: LLM ҚОСЫМШАЛАРЫ МЕН ОСАЛДЫҚТАРЫНА ШОЛУ

Аңдатпа. Бұл құжат үлкен тілдік модельдер (LLM) арқылы Киберқауіпсіздіктің болашағына жан-жақты шолу жасайды. Біз GPT-4, GPT-3.5, BERT, Falcon2 және LLaMA сияқты модельдердегі жетістіктерге назар аудара отырып, LLM эволюциясы мен оның қазіргі жағдайына шолу жасаймыз. Біздің талдауымыз LLM осалдықтарын қамтиды, мысалы, жылдам іске асыру, қауіпсіз Шығыс өңдеу, деректермен улану, DDoS шабуылдары және қарсыласу нұсқаулары. Біз ықтимал шабуыл сценарийлері мен олардың алдын алу әдістеріне жан-жақты шолу жасай отырып, осы үлгілерді қорғаудың азайту стратегияларын егжей-тегжейлі қарастырамыз. Бұл аналитикалық деректер нақты уақыттағы киберқауіпсіздіктен қорғауды жақсартуға және қауіптерді анықтау және оларға жауап беру үшін LLM қолданбаларының күрделілігін арттыруға бағытталған. Біздің құжат дамып келе жатқан киберқауіпсіздіктерден қорғау үшін LLM-ді болашақ киберқауіпсіздік жүйелеріне біріктірудің негізгі түсінігі мен стратегиялық бағытын ұсынады.

Түйін сөздер: LLM, киберқауіпсіздік, үлкен тілдік модельдер, тілдік модельдеу, Машиналық оқыту, NLP, табиғи тілді өңдеу.

THE USE OF LLM IN CYBERSECURITY: OVERVIEW OF LLM APPLICATIONS AND VULNERABILITIES

Abstract. This document provides a comprehensive overview of the future of cybersecurity through Large Language Models (LLM). We present an overview of the evolution of LLM and its current state, focusing on advances in models such as GPT-4, GPT-3.5, BERT, Falcon2, and LLaMA. Our analysis extends to LLM vulnerabilities such as rapid deployment, insecure output processing, data poisoning, DDoS attacks, and adversarial instructions. We will take a detailed look at mitigation strategies to protect these models, providing a comprehensive overview of potential attack scenarios and methods to prevent them. This analytical data is aimed at improving real-time cybersecurity protection and increasing the complexity of LLM applications for threat detection and response. Our document provides a fundamental understanding and strategic direction for integrating LLM into future cybersecurity systems to protect against evolving cyber threats.

Keywords: LLM, cybersecurity, large language models, language modeling, machine learning, NLP, natural language processing.

Сведение об авторах

Курасбек Аязжан Нурлыбекқызы	Магистрант, Системы информационной безопасности, Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан, E-mail: kurasbek.a.140@mail.ru
Кенжебаева Мерей Омаровна	PhD, и. о. доцента кафедры кибербезопасности и криптологии, Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан, E-mail: merey-mex-2017@mail.ru
Адилжанова Салтанат Адмуханбетовна	PhD, и. о. доцента кафедры кибербезопасности и криптологии, Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан, E-mail: asaltanat81@gmail.com

Авторлар туралы мәлімет

Курасбек Аязжан Нурлыбекқызы	Магистрант, Ақпараттық қауіпсіздік жүйелері, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан, E-mail: kurasbek.a.140@mail.ru
Кенжебаева Мерей Омаровна	PhD, киберқауіпсіздік және криптология кафедрасының доцентінің м. а., әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан, E-mail: merey-mex-2017@mail.ru
Адилжанова Салтанат Адмуханбетовна	PhD, киберқауіпсіздік және криптология кафедрасының доцентінің м. а., әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан E-mail: asaltanat81@gmail.com

Information about the authors

Kurasbek Ayazhan	Master's student, Information Security Systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan, E-mail: kurasbek.a.140@mail.ru
Kenzhebayeva Merey	PhD, Acting Associate Professor of the Department of Cybersecurity and Cryptology, Al-Farabi Kazakh National University, Almaty, Kazakhstan E-mail: merey-mex-2017@mail.ru
Adilzhanova Saltanat	PhD, Acting Associate Professor of the Department of Cybersecurity and Cryptology, Al-Farabi Kazakh National University, Almaty, Kazakhstan, E-mail: asaltanat81@gmail.com



UDC 004.912

IRSTI 16.31.61

https://doi.org/10.53364/24138614_2025_38_3_11

I. Ryabchenko¹, R. Anayatova¹, G. Tulekova¹, A. Koshekov^{1*}, Y. Kuanov¹

¹Civil Aviation Academy, Almaty, Republic of Kazakhstan

*E-mail: a.k.koshekov@gmail.com

MODELING SEMANTIC RELATIONSHIPS OF AVIATION TERMS: VECTOR SPACES AND LANGUAGE MODELS

Abstract. *The proposed article examines methods for modeling semantic relationships of aviation terms using the BERT and RoBERTa language models. The relevance of the study lies in the use of a pre-prepared and annotated corpus of aviation terms that align with international practice and are drawn from documents of international regulatory bodies. The developed language corpus provides the basis necessary for assessing the semantics of aviation terminology in the context of real aircraft operation. The research methodology involves fine-tuning language models trained on an aviation corpus of terms using cosine similarity, rank correlation, and cluster metrics of measurements. The experiments demonstrate the main differences between the two models in tracking synonyms, variability, and shifts in aviation discourse. The results of the study demonstrate that fine-tuning the models enhances their ability to cluster related terms, distinguish closely related but distinct concepts, and align the results with expert judgments. These results provide a methodological basis for the development of aviation terminology resources, enabling the application of lexicography transformer models and ontology construction.*

Keywords: *semantic proximity, aviation terminology, language models, corpus linguistics, transformers, embedding, natural language processing.*

Introduction.

Today, one of the primary tasks of natural language is modeling the semantic similarity of terms, and a substantial number of studies aim to address this problem. The problem of assessing the semantic similarity of terms arises in various practical applications, including automatic text translation, search for relevant information, intelligent search, ontology construction, and text analysis and processing for specific subject areas [1]. In a highly technical field and specialized industry like aviation, the accuracy of terminology is a crucial aspect, as the correctness of language structures directly determines professional international communication and document flow, which is closely related to ensuring flight safety.

Historically, the first approaches to modeling semantic relationships between terms were based on statistical methods, such as TF-IDF, which account for the frequency of a particular term without analyzing its content [2]. The next step in developing these methods is the use of distributed representations, such as Word2Vec and GloVe [3], which provide a representation of words in the form of vector spaces that capture semantic patterns through contextual co-occurrence in texts. However, such models assigned words a fixed vector, which did not allow for effective processing of polysemy and domain-specific meanings.

The next key step in the development of natural language processing is the use of contextualized language models, such as ELMo, BERT, and RoBERTa. These models are trained

on a large language corpus using an attention function that provides context-sensitive embeddings to distinguish the synonymous meanings of terms [4]. These models yield fairly good results in natural language processing; however, their effective application in specialized areas depends on the adaptation of the corpus used, which is specific to each subject area. A feature of applications in the aviation industry is the complex technical terminology, multilingualism, and the use of various semantic changes depending on the content being processed [5]. The relevance of the topic is confirmed by the importance of accurate terminology modeling in ensuring the safe operation of aviation equipment, as well as lexicography and knowledge management. Existing research is primarily focused on the use of universal pre-trained models, which often fail to accurately reflect the semantic structure of aviation terminology [6, 7].

The aim of this study is to address the issue of utilizing language models in the aviation industry by developing and training a model on a new corpus of terminology directly related to aviation. The corpus of terms formed in this study comprises regulatory documents from international aviation authorities, technical manuals for aircraft operation, and training materials [8]. As part of the study, the authors manually annotated the corpus to establish semantic relationships, hierarchies between terms, and synonymous variations [9].

The main problem facing this study was the lack of a comprehensive corpus of terms with multilevel annotations. This complicates the comparison of language models, which negatively affects the development of lexicographic resources. This study aims to address this research gap by creating a specialized corpus of aviation terms from international regulatory documents, detailing the term annotation scheme, determining their quality, and comparing standard models with those trained on the developed language corpus.

As part of the study, the ability to reflect semantic proximity in aviation communication is assessed by fine-tuning the BERT and RoBERTa models on the collected corpus and comparing their performance with that of versions in the general subject area [10].

The objectives of this study are:

To create a corpus of aviation terminology and describe the methodology for its annotation;

To evaluate the effectiveness of the BERT and RoBERTa models for modeling the semantic similarity of aviation terms;

To compare the models using quantitative metrics (cosine similarity, rank correlation, clustering indices);

To visualize the semantic space using dimensionality reduction methods for accurate interpretation of terms.

The scientific novelty of the study lies in the combination of transformer approaches with the use of a subject-oriented annotated language corpus, which enables the utilization of the semantic behavior of terminology in a real professional context. The practical significance lies in the application of the results in the construction of an aviation thesaurus, ontologies, and the development of an intelligent linguistic support system for aviation industry specialists.

Materials and methods.

Formation of the aviation terminology corpus

To conduct the study and enhance the reliability of the experimental results, the authors created a specialized corpus of aviation terms. The material for the corpus was collected from authoritative industry sources, including ICAO Annexes, EASA and FAA regulations and guidelines, IATA operational standards, Airbus and Boeing aircraft operating manuals, aviation textbooks, and scientific articles. The corpus of words comprises 100,000 unique tokens, ensuring comprehensive coverage of all key subdomains within the aviation industry. The tokens include terms from the time period 2000 to 2025. The breakdown of tokens by subdomains is presented in Table 1.

Table 1 – Corpus statistics by aviation subdomains

Subdomain	Documents	Tokens	% of corpus	Unique terms
-----------	-----------	--------	-------------	--------------

Navigations	420	20 000	20	2 600
Flight operations	350	18 000	18	2 200
Safety and emergency	310	16 000	16	2 000
Maintenance and emergency	300	15 000	15	1 900
Airworthiness and regulations	240	12 000	12	1 500
Aircraft structures and parts	210	10 000	10	1 300
Air traffic control and communication	170	9 000	9	1 100
Total	2 000	100 000	100	12 600

The terminology set was selected to be well-balanced across all aviation subdomains. This proportional division reflects the practical importance of each area in aviation communication. The corpus also includes additional terminology, such as maintenance, regulatory language, and phraseology used in air traffic control, which are also important for ensuring flight safety.

The pre-processing process includes tokenization, text cleaning, and normalization, after which the text is annotated at multiple levels. The first level includes morphological markup to ensure the participatory nature of the information and lemmatization. The second level includes terminological markup with the assignment of labels according to aviation subdomains (navigation, safety, etc.). The third level introduces semantic relations such as synonymy, hypernymy, and the part-whole relation, which allows the corpus to reflect the full complexity of professional aviation terminology. The dataset is verified by aviation linguists to ensure terminological accuracy. The process flow diagram for creating and annotating the aviation terminology language corpus is shown in Figure 1.

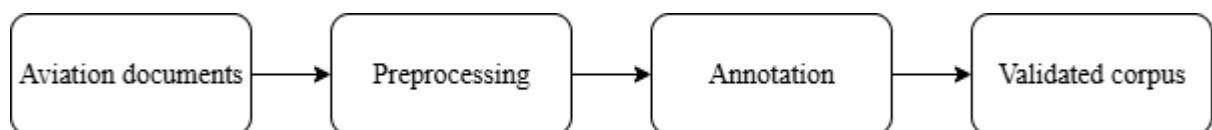


Figure 1 – Scheme of corpus construction and annotation

To demonstrate the term annotation protocol and ensure transparency, Table 2 presents examples of term annotations. Each entry represents the term's canonical form, subdomain, semantic relationship type, representation variants, and example of the term's use in a sentence. This display format demonstrates the multilevel annotation scheme and the encoding of linguistic and semantic information for model training and evaluation.

Table 2 – Examples of annotated aviation terms

Term	Canonical form	Subdomain	Relation	Variants	Example
Briefing	Briefing	Safety	Synonymy	Preflight briefing	The crew conducted a safety briefing prior to engine start
Altitude	Altitude	Navigation	Hypernymy	Flight level	Maintain altitude 3500 feet until

					cleared for approach
Autopilot	Autopilot	Operations	Associative	Flight direction	The autopilot was engaged during climb to reduce pilot workload
Fuselage	Fuselage	Structures	Meronymy	Airframe	The fuselage inspection revealed minor structural damage
GPWS	Ground proximity warning system	Safety	Abbreviation	-	The GPWS alert required an immediate go-around

Table 2 shows that the annotation incorporates both the lexical and semantic aspects of aviation terminology. In the dataset, "briefing" is associated with synonyms in the safety subdomain, while "fuselage," with its part-whole relationship, belongs to the structure subdomain. The abbreviations and multiword variants of terms are explicitly recorded to ensure the model's ability to clearly recognize equivalences. Examples of term usage in sentences provide a contextual basis, and are necessary for expert verification.

Model fine-tuning

Two-stage model fine-tuning and training parameters for universal models were adapted for aviation crops. The first optimization step is domain adaptation using masked language modeling (MLM), which helps models learn the distributional semantics of tokens to predict a randomly masked term from the context:

$$\mathcal{L}_{\text{MLM}} = -\frac{1}{N} \sum_{i=1}^N \log P(w_i | \hat{w}_i, \theta), \quad (1)$$

where w_i – original token, \hat{w}_i – masked version of the token, θ – set of model parameters.

The second step is contrastive learning with triplet loss, which generates a triplet of "anchor-positive-negative" terms based on the annotated complex. This configuration ensures a semantic relationship between the anchor and positive terms while assigning negative terms to a different subdomain. This procedure helps to separate related but conceptually different terms, increasing the robustness of term embedding in professional contexts.

For the MLM, dynamic masking with a probability of 15% was used to ensure a variety of training scenarios. The retraining process was controlled using validation-perplexity-based stopping. Model evaluation was conducted using the MLM and MLM+triplet configurations, allowing for the quantitative evaluation of each stage to be examined. The training settings for the experiment included the following parameters: learning rate MLM (5×10^{-5}), learning rate triplet (2×10^{-5}), batch size – 32, epochs – 20, warmup ratio – 10%, weight decay – 0.01, optimizer – AdamW, validation – 10%, random seed – 42 and hardware – 24 gb vram.

These parameters ensure a balance between the computational efficiency and convergence. The stability of fine-tuning was ensured using warmup learning and parameter weight reduction, while reproducibility was achieved using a fixed initial value. Triplet loss improves the separation of semantically related terms, as reflected in the ablation results.

Semantic similarity estimation

To effectively evaluate the relationships between aviation terms, embeddings were extracted from the proposed models using the SentenceTransformers framework. The embeddings from the models have dimensions of 384 for BERT and 768 for RoBERTa, which provides a detailed

representation of the semantic space. The main similarity measure used in this paper is cosine similarity, which helps estimate the proximity of term vectors in space without relying on absolute values. The similarity between two terms t_1 and t_2 is determined using the formula:

$$\text{sim}(t_1, t_2) = \frac{v_{t_1} \cdot v_{t_2}}{\|v_{t_1}\| \cdot \|v_{t_2}\|}, \quad (2)$$

where the numerator is presented as a scalar product of vectors and the denominator normalizes the values by the Euclidean norm.

The convergence coefficient ranges from -1 to 1, where a higher value indicates stronger semantic similarity. To illustrate this approach, Figure 2 was prepared, which shows an example of calculating similarity using cosine similarity for a pair of aviation terms. The term "vectors" is presented in a two-dimensional coordinate space, where the angle between the vectors corresponds to the strength of semantic similarity.

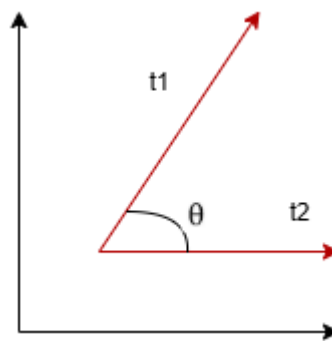


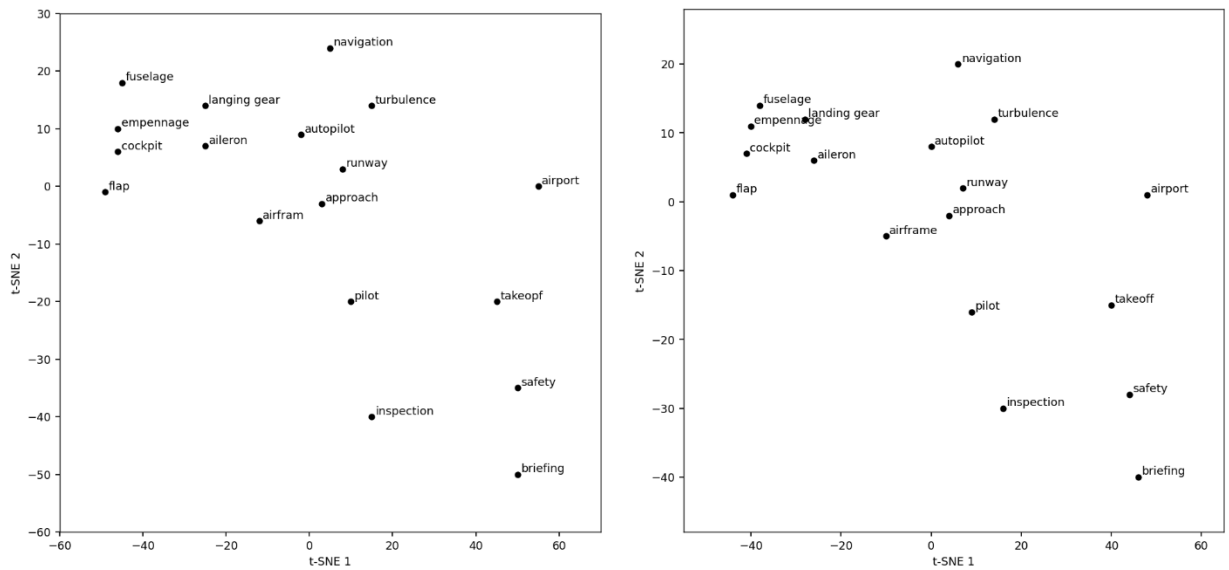
Figure 2 – Example of cosine similarity calculation between aviation term pairs

Semantic evaluations were conducted using internal and external tests to ensure the quantitative reliability and professional validity. For internal evaluation, a dataset of 500 paired terms was created and evenly balanced across four relationship types: synonymy, hypernymy, meronymy (part-whole), and disjoint (contrast) pairs. Each pair of terms was rated by aviation linguists and industry experts and assigned a score from 0 to 4. The annotators' agreement was estimated at 0.82, indicating a high level of agreement. Each model was evaluated using cosine similarity between term vectors, and the correlation between expert assessments was measured using Spearman's rho. Robustness was ensured by resampling 1000 times using the bootstrap method (95% confidence interval). Differences between the models were assessed using Fisher's z-transform. The clustering quality was assessed based on the annotated subdomains. Silhouette and Davies-Bouldin indices were calculated for this assessment. Stochastic effects were accounted for by averaging 10 random initial values. External tests addressed two practical issues. The first was the automatic matching of terms with external thesuri using precision and recall assessments. The second was predicting the correct assignment of meanings for polysemantic terms assessed using expert annotations. In addition to the numerical model indicators, experts manually verified the model's results. This multilevel approach ensured the stochastic and linguistic validity of the results.

Visualization of semantic spaces

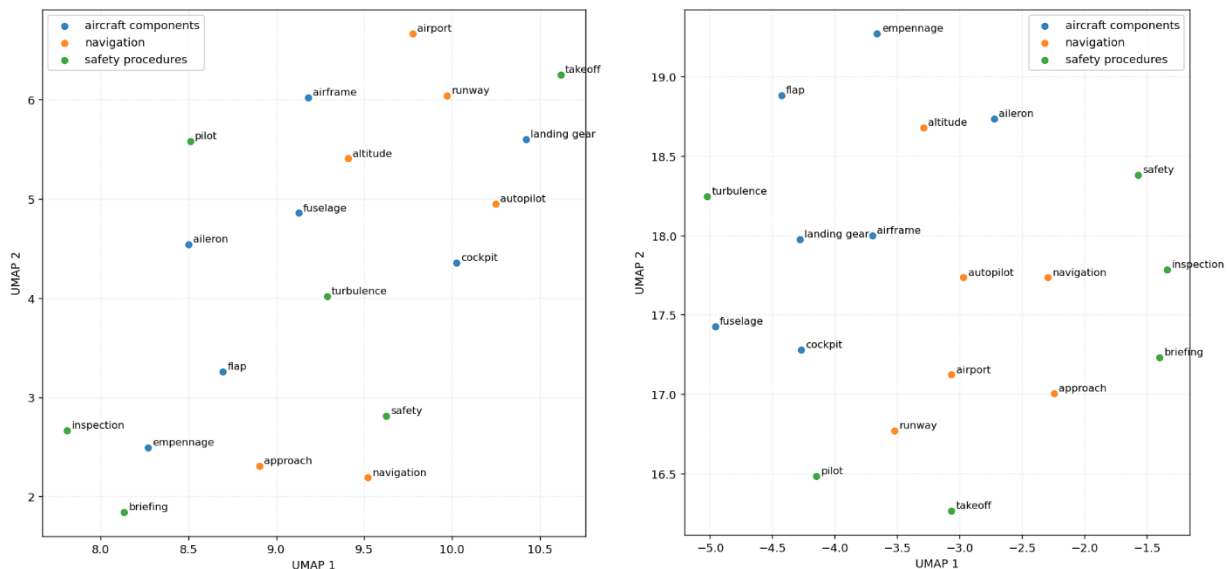
Domain-adapted embeddings structure aviation terminology by projecting multidimensional vectors onto two dimensions using t-SNE and UMAP. T-SNE is used to identify compact groups of terms that are closely related. The stochastic nature of the model is controlled by introducing a fixed seed, the perplexity is tuned to a moderate range to balance local granularity and global readability, and the number of iterations is set high enough to ensure convergence. The resulting t-SNE maps from the study are presented in Figure 3, where semantically consistent clusters (e.g.,

aircraft components, navigation, safety) are highlighted, and subtle differences within the clusters themselves (e.g., control surfaces and structural nodes) are often obscured in quantitative values.



a) BERT
b) RoBERTa
Figure 3 – t-SNE projection of aviation embeddings

In addition, UMAP is used for analysis to examine the local and global structure of diversity, employing a graph approach that ensures the preservation of inter-cluster geometry. Cosine distance is used for the angular nature of similarity in space, which helps to avoid database overflow and preserve intra-class relationships. The projections presented in Figure 4 show a consistent macrostructure for both models, making the inter-cluster separation more obvious compared to t-SNE, which helps capture category leakage (i.e., the shift of exploitable terms towards safety).



a) BERT
b) RoBERTa
Figure 4 – UMAP projection of aviation embeddings

These plots provide complementary evidence across domains. When fine-tuned on a corpus of aviation terms, BERT produces tight, discrete clusters with sharp boundaries, which is useful in tasks that require clear class separation. RoBERTa has smoother transitions between adjacent

subdomains, which is useful in cases where graded similarity is needed. Both models use a fixed seed, hyperparameters, and term set, which is necessary to allow direct comparisons between them. The limitation of 2D projections is that they discard information and introduce layout artifacts, which is addressed in this paper by using quantitative metrics that provide openness and interpretability in the geometry of aviation terminology.

Evaluation protocol

The semantic similarity of terms is assessed using a combination of quantitative metrics and qualitative expert assessment by linguistic teachers. The verification process is designed to assess the mathematical consistency of the results and their compliance with professional linguistic terminology in the aviation industry. The quantitative assessment of the vector proximity measure was determined using cosine similarity. A reference dataset is used to verify the calculated values. This dataset comprises carefully selected pairs of terms that have been independently annotated by linguists and experts from aviation enterprises. The correlation between similarity estimates obtained using the models and expert assessments is calculated using Spearman's rank correlation coefficient to assess the monotonicity of the relationship between similarities.

In addition to pairwise similarity, the quality of clustering is investigated to determine the quality of reflection of the high-level structure of aviation terminology. The silhouette index and Davis-Bouldin are used to evaluate grouping into semantic clusters, which provides a representation of intra-cluster coherence and inter-cluster separation. These metrics complement the overall assessment, which is based on similarity, tracking, subgroup identification consistency, and domain specificity.

Linguistic experts assessed the representativeness of a subset of the model results. This expert assessment is crucial for confirming the practical significance of the results, as some semantic relationships may not be fully reflected when evaluating statistical indicators. The assessment of the model's ability to accurately represent aviation terminology is achieved by integrating clustering indicators, expert assessment, and a protocol to ensure the multidimensionality and reproducibility of the assessment. Such an integrated approach ensures methodological sustainability and practical significance of the results of lexicographic and terminological applications in the aviation industry.

Results and discussion.

Pairwise semantic similarity

The key method for assessing the effectiveness of semantic models is the comparison of pairwise similarity scores between aviation terms. The cosine convergence coefficient is used to assess the degree of correspondence of the selected term pairs in the semantic space. The term pairs are selected taking into account typical relationships adopted in the aviation industry: near-synonyms (aircraft-plane), functional relatedness (autopilot-flight director), contextual similarity (safety-inspection), and semantic similarities (cockpit-fuselage). Table 3 presents the similarity scores for the term pairs described above. The results are presented for the universal versions of BERT and RoBERTa, as well as optimized versions of these models trained on the aviation terminology corpus.

Table 3 – Cosine similarity scores for selected aviation term pairs under general and fine-tuned models

Term pair	General BERT	Fine-tuned BERT	General RoBERTa	Fine-tuned RoBERTa
Aircraft-plane	0.62	0.89	0.65	0.91
Runway-airstrip	0.58	0.87	0.60	0.85
Autopilot-flight director	0.49	0.76	0.55	0.82
Turbulence-disturbance	0.44	0.72	0.47	0.75
Cokpit-fuselage	0.33	0.64	0.35	0.61
Safety-inspection	0.39	0.70	0.42	0.73

The obtained results demonstrate that fine-tuning improves the consistency of vectors and expert judgment in the aviation industry. For example, for the pair of terms “airstrip” and “runway”, the similarity score after fine-tuning the BERT model increased from 0.58 to 0.87, and for the RoBERTa model from 0.60 to 0.85, which means that they are used synonymously. Additionally, terms with functional or procedural overlap also increased the convergence rate after fine-tuning the models, a finding confirmed by expert judgment.

An interesting difference is demonstrated between the two models on pairs containing functional differences. For example, the RoBERTa model shows high stability for similar pairs, indicating high sensitivity to graded similarity. In contrast, the BERT model shows a sharp increase in convergence on synonymous words, indicating a strength in forming discrete equivalence classes. Overall, when analyzing pairwise convergence, we can conclude that both models improve their performance after fine-tuning, with complementary strengths.

Table 4 presents the performance differences between the methods (TF-IDF, Word2Vec, GloVe, and FastText) and the transformer-based models (BERT and RoBERTa) in the baseline settings and with fine-tuning for aviation terminology. The results were presented as Spearman correlations and clustering metrics.

Table 4 – Comparison of baseline and transformer models

Model	Spearman	Silhouette	Davies-Bouldin
TF-IDF	0.41	0.28	1.92
Word2Vec	0.53	0.36	1.65
GloVe	0.55	0.38	1.59
FastText	0.59	0.42	1.48
BERT	0.62	0.44	1.37
BERT (aviation)	0.83	0.61	1.01
RoBERTa	0.65	0.46	1.35
RoBERTa (aviation)	0.81	0.58	1.08

The results demonstrated three key findings. First, both transformer models outperformed the classical baseline models, confirming the superiority of the contextual models. Fine-tuning enables the capture of subtle semantic relationships. Second, the models are domain-adaptable; fine-tuned models demonstrate a 0.2-point increase in Spearman coefficient compared to their generic counterparts, and two other metrics demonstrate effectiveness, demonstrating the formation of coherent clusters. Third, both transformer architectures have mutually exclusive advantages: fine-tuned BERT produces clear and discrete clusters, enabling effective ontologies and dictionary development, whereas RoBERTa produces smooth semantic gradients between terms, which facilitates term similarity search.

Visualization of semantic spaces

To provide a qualitative check of the structuring of aviation terminology, the authors examined Figure 3 by dividing it into subdomains using a color scheme to better demonstrate the differences. Adaptation to the domains yields clusters that align with the experts’ expectations. In Figure 5(a), the clusters have a denser and more discrete grouping structure. This geometry is consistent with the BERT model’s tendency to have clear decision boundaries, often related to tasks such as terminological labeling and dictionary meaning assignment.

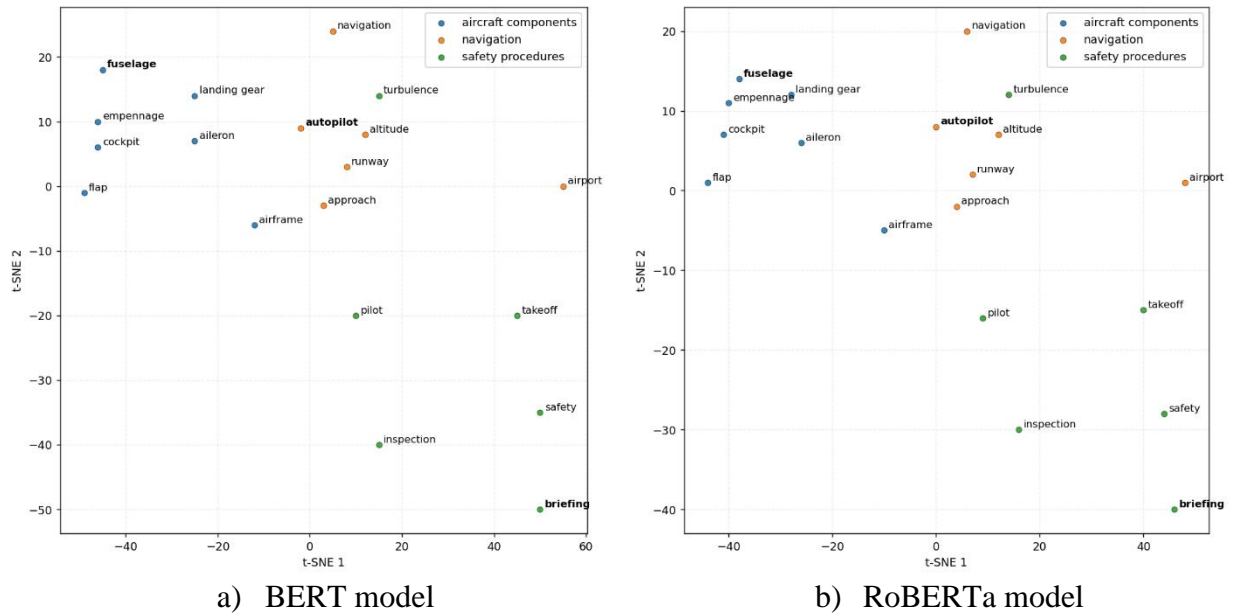


Figure 5 – Scatter plot for both models with consistent color subdomains coding

In Figure 5(b), the clusters remain stable and show smooth gradients along their boundaries, for example the term "autopilot" in this model is closer to the operational sample, while maintaining its distance from the structural lexicon subdomain, while "briefing" still belongs to the safety cluster, but shows a move towards operational, due to its use in pre-flight procedures. Such smooth transitions make the RoBERTa model a valuable tool for synonym search and expansion of the aviation lexicon, where nuances of proximity are more effective than rigid partitioning.

Using a uniform color scheme and term lists allows for a visual comparison of true differences in term embeddings. Random seeds and identical dimensionality reduction settings are fixed for both models to ensure reproducibility. Two-dimensional projections compress information and may distort long-term relationships, but the observed patterns confirm the results obtained in the previous two subsections. Based on the analysis, we can conclude that fine-tuning enhances intra-cluster connectivity and improves inter-cluster separation. The BERT model ensures separability, while RoBERTa captures semantic gradients.

Expert validation

The previously proposed quantitative metrics provide mechanisms for assessing semantic models, but for specific domains such as aviation, it is necessary to rely on expert understanding of terminology. To achieve this, a group of linguists and representatives of aviation enterprises was involved in the study, who examined subsets of the model results and compared them with semantic expectations. The experts confirmed that the fine-tuned model better matched professional interpretations of aviation terms. The generic model often associates terms with every day or general language, which often differs from the specialized use of these terms in aviation. In contrast, the fine-tuned proposed models effectively reinforced context-dependent and aviation-specific relationships. A brief example of the comparison between expert assessments and the base model's judgments is presented in Table 5.

Table 4 – Case-study examples of expert validation

Term	Closet term in general model	Closet term in fine-tuned model	Expert judgement	Expert comment (general model/fine-tuned model)
Briefing	communication	inspection	Safety context	General talk/Safety

Altitude	height	approach	Navigation	Everyday synonym/Aviation specific role
Autopilot	robotics	Flight director	Operations	Robotics/Cockpit system
Airframe	Construction	Fuselage	Aircraft components	Construction/Structural vocabulary
Takeoff	Departure	Runway	Flight operation	Travel synonym/Operational aviation context
Turbulence	chaos	safety	Safety procedures	Abstract notion/Procedural and safety term

These examples demonstrate the importance of creating domain-specific term corpora. Basic models often linked technical aviation terms to a broad everyday context. Fine-tuned models align terms with professional usage, ensuring that clusters and convergence rates match authentic linguistic practice. Conformity to expert assessment demonstrates the methodological soundness and practical value of this approach, especially in cases of lexicographic databases, training materials, and safety documentation.

Implications and limitations

The results obtained in this study demonstrate the strengths and weaknesses of applying the transformer-based models to the aviation terminology domain. Fine-tuning the models shows improvements in semantic similarity, clustering quality, and expert judgment. These achievements demonstrate the practical importance of adapting models to a specific domain, which helps avoid distorting the meaning of technical terms when comparing them with everyday synonyms or unrelated concepts. The creation of a specialized aviation corpus helps to create a reliable terminology resource for curriculum improvement and intelligent search in the aviation context.

In addition to the advantages, this study has several limitations in its results. First, the corpus used for fine-tuning the models remains small in size, which limits the representativeness of the training material and increases the risk of overfitting the model on specific subsets of aviation subdomains. Second, the annotation process is limited by the resources of the academic institution and does not reach the level of coverage typical of large-scale corpus linguistics projects. Another methodological limitation is the use of two-dimensional projection as an interpretation tool, which compress multivariate relationships and may obscure the boundaries of some clusters. Therefore, the insights gained from scatterplots should always be considered in conjunction with quantitative metrics. Although fine-tuning resulted in measurable improvements, the results exhibit model-specific biases: BERT favors crisp and discrete clusters, leading to the simplification of semantic continua, while the RoBERTa model exhibits smooth gradients that may blur distinctions critical for aviation safety terminology. These limitations underscore the importance of careful model selection and the ability to combine models based on the task they are intended to perform.

Based on the limitations described, it can be concluded that this study, while developing a specific subject area and offering a replicable assessment system, represents only the first step in creating a comprehensive dictionary of aviation terms. Future work involves expanding the corpus of terms to include multilingual data reflecting the identity of each state, as well as participants in international organizations. Additionally, it involves introducing advanced assessment methods that take into account pragmatic and discursive phenomena beyond pairwise similarity or clustering.

Conclusion.

The main objective of this study was to evaluate the transformer-based language models for aviation terminology by creating a specialized corpus and fine-tuning the BERT and RoBERTa

models. The obtained results demonstrate that domain-specific adaptation increases the semantic accuracy of vector representations, improves the quality of the clustering process, and ensures accurate compliance with expert assessments. These results demonstrate the need for a specialized corpus in the aviation industry and indicate the potential application in databases, training materials, and decision support systems. At the same time, the study reveals critical limitations: to date, the corpus does not have a high level of scale and depth of annotation, the methods of visualization of results are useful for analytics, but certain structural properties of the embedding space cannot be taken from it, and specific distortions characteristic of these models indicate the need for a hybrid solution for processing aviation linguistics.

This study represents the first step in creating a comprehensive dictionary of aviation terms. The primary contribution of this study is to confirm the hypothesis that we need to build our own language corpus and fine-tune it to the specific needs of the aviation industry. For aviation linguistics and applied natural language processing, the results underscore the need for further research on developing a large, multilingual, and systematically annotated language corpus, as well as hybrid methods for evaluating model performance. With continued efforts, it is possible to provide reliable, reproducible, and practically applicable tools for terminology, lexicography, and security of communication.

Funding.

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23490578) «Development of linguistic support and mobile application for a Kazakh-English-Russian thesaurus-type dictionary of modern aviation terms regulated by ICAO, EASA, IATA standards».

References

1. Jiang, J., & Wang, H. H. (2020). Application intelligent search and recommendation system based on speech recognition technology. *International Journal of Speech Technology*, 24(1), 23–30. <https://doi.org/10.1007/s10772-020-09703-0>.
2. Zhuohao, W., Dong, W., & Qing, L. (2021). Keyword Extraction from Scientific Research Projects Based on SRP-TF-IDF. *Chinese Journal of Electronics*, 30(4), 652–657. <https://doi.org/10.1049/cje.2021.05.007>
3. Al-Aidaros, A. S., & Bamzahem, S. M. (2023). The Impact of GloVe and Word2Vec Word-Embedding Technologies on Bug Localization with Convolutional Neural Network. *International Journal of Science and Engineering Applications*, 108–111. <https://doi.org/10.7753/ijsea1201.1035>
4. Wada, S., Takeda, T., Okada, K., Manabe, S., Konishi, S., Kamohara, J., & Matsumura, Y. (2024). Oversampling effect in pretraining for bidirectional encoder representations from transformers (BERT) to localize medical BERT and enhance biomedical BERT. *Artificial Intelligence In Medicine*, 153, 102889. <https://doi.org/10.1016/j.artmed.2024.102889>
5. Tang, H., Kamei, S., & Morimoto, Y. (2023). Data Augmentation Methods for Enhancing Robustness in Text Classification Tasks. *Algorithms*, 16(1), 59. <https://doi.org/10.3390/a16010059>
6. Gandour, J. (2002). *Interdisciplinary Approaches to Language Processing* (review). *Language*, 78(2), 359. <https://doi.org/10.1353/lan.2002.0081>
7. Muraki, E. J., Feddema, C. Y., Pexman, P. M., & Reggin, L. D. (2023). The Development of Abstract Word Meanings. *Journal of Child Language*, 52(1), 195–207. <https://doi.org/10.1017/s0305000923000569>
8. Zhao, L., Fang, J., & Gao, W. (2024). Optimizing Large Language Models on Multi-Core CPUs: A Case Study of the BERT Model. *Applied Sciences*, 14(6), 2364. <https://doi.org/10.3390/app14062364>
9. Moe, R. (2010). Compiling dictionaries using semantic domains. *Lexikos*, 13(1). <https://doi.org/10.4314/lex.v13i1.51389>

10. Shu, X. (2024). BERT and RoBERTa for Sarcasm Detection: Optimizing Performance through Advanced Fine-tuning. Applied and Computational Engineering, 97(1), 1–11. <https://doi.org/10.54254/2755-2721/97/20241354>

ТЕРМИНДЕРДІҢ СЕМАНТИКАЛЫҚ БАЙЛАНЫСТАРЫН МОДЕЛЬДЕУ: ВЕКТОРЛЫҚ КЕҢІСТІКТЕР ЖӘНЕ ТІЛДІК МОДЕЛЬДЕР

***Аңдатпа.** Ұсынылған мақалада авиациялық терминдердің семантикалық қатынастарын модельдеудің әдістері BERT және RoBERTa тілдік модельдерін қолдану арқылы қарастырылады. Зерттеудің өзектілігі алдын ала дайындалған және аннотацияланған авиациялық терминдер корпустарын пайдаланумен айқындалады, олар халықаралық тәжірибеге сәйкес келеді және халықаралық реттеуші органдардың құжаттарынан алынған. Құрастырылған тілдік корпус ұшақтарды нақты пайдалану жағдайында авиациялық терминология семантикасын бағалау үшін қажетті негізді қамтамасыз етеді. Зерттеу әдіснамасы авиациялық терминдер корпусында алдын ала үйретілген тілдік модельдерді қайта баптауды (fine-tuning) қамтиды және ол косинустық ұқсастық, рангілік корреляция мен кластерлік метрикаларды өлшеуге негізделген. Эксперимент нәтижелері екі модельдің синонимдерді қадағалау, вариативтілік пен авиациялық дискурстағы мағыналық ығысудағы негізгі айырмашылықтарын көрсетті. Зерттеу нәтижелері модельдерді қайта баптау олардың байланысты терминдерді топтастыру қабілетін арттыратынын, өзара ұқсас, бірақ әртүрлі ұғымдарды ажырата алатынын және нәтижелерді сарапшылардың бағаларымен сәйкестендіретінін дәлелдейді. Бұл нәтижелер авиациялық терминологиялық ресурстарды дамытуға әдістемелік негіз ұсынады, трансформер модельдерін лексикографияда және онтология құруда қолдануға мүмкіндік береді.*

***Түйін сөздер:** семантикалық жақындық, авиациялық терминология, тілдік модельдер, корпус лингвистикасы, трансформерлер, эмбединг, табиғи тілдерді өңдеу.*

МОДЕЛИРОВАНИЕ СЕМАНТИЧЕСКИХ ОТНОШЕНИЙ ТЕРМИНОВ: ВЕКТОРНЫЕ ПРОСТРАНСТВА И МОДЕЛИ ЯЗЫКА

***Аннотация.** Предлагаемая статья рассматривает методы моделирования семантических отношений авиационных терминов с использованием языковых моделей BERT и RoBERTa. Актуальность исследования заключается в применении заранее подготовленного и аннотированного корпуса авиационных терминов, который соответствует международной практике и сформирован на основе документов международных регулирующих организаций. Разработанный языковой корпус обеспечивает необходимую основу для оценки семантики авиационной терминологии в контексте реальной эксплуатации воздушных судов. Методология исследования включает дообучение (fine-tuning) языковых моделей на корпусе авиационных терминов с использованием косинусного сходства, ранговой корреляции и кластерных метрик. Эксперименты продемонстрировали основные различия между двумя моделями в отслеживании синонимов, вариативности и семантических сдвигов в авиационном дискурсе. Результаты исследования показали, что дообучение моделей повышает их способность кластеризовать связанные термины, различать близкие, но отличающиеся понятия, а также согласовывать результаты с экспертными оценками. Полученные данные обеспечивают методологическую основу для разработки ресурсов авиационной терминологии, что позволяет применять трансформерные модели в лексикографии и построении онтологий.*

Ключевые слова: семантическая близость, авиационная терминология, языковые модели, корпусная лингвистика, трансформеры, эмбединг, обработка естественного языка.

Information about the authors

Ryabchenko Inna	Research Fellow, Civil Aviation Academy, Almaty, Kazakhstan E-mail: i.ryabchenko@agakaz.kz
Anayatova Raziyam	PhD, Head of the Department of Aviation English, Civil Aviation Academy, Almaty, Kazakhstan, E-mail: r.anayatova@agakaz.kz
Tulekova Gulnaz	PhD, Professor, Department of Aviation English, Civil Aviation Academy, Almaty, Kazakhstan, g.tulekova@agakaz.kz
Koshekov Abay	PhD, Associate Professor, Department of Aviation Engineering and Technology, Civil Aviation Academy, Almaty, Kazakhstan, E-mail: a.k.koshekov@gmail.com
Kuanov Yerkanat	Research Fellow, Civil Aviation Academy, Almaty, Kazakhstan E-mail: e.kuanov@agakaz.kz

Авторлар туралы мәлімет

Рябченко Инна	Азаматтық авиация академиясының ғылыми қызметкері, Алматы, Қазақстан, E-mail: i.ryabchenko@agakaz.kz
Анаятова Разиям	PhD, Азаматтық авиация академиясының авиациялық ағылшын тілі кафедрасының меңгерушісі, Алматы, Қазақстан, E-mail: r.anayatova@agakaz.kz
Тулекова Гульназ	PhD, профессор, авиациялық ағылшын тілі кафедрасы, Азаматтық авиация академиясы, Алматы, Қазақстан, g.tulekova@agakaz.kz
Кошеков Абай	PhD, азаматтық авиация академиясының авиациялық техника және технологиялар кафедрасының доценті, Алматы, Қазақстан E-mail: a.k.koshekov@gmail.com
Куанов Еркнат	Азаматтық авиация академиясының ғылыми қызметкері, Алматы, Қазақстан, E-mail: e.kuanov@agakaz.kz

Сведение об авторах

Рябченко Инна	Научный сотрудник Академии гражданской авиации, Алматы, Казахстан, E-mail: i.ryabchenko@agakaz.kz
Анаятова Разиям	PhD, заведующий кафедры «Авиационный английский язык» Академии гражданской авиации, Алматы, Казахстан, E-mail: r.anayatova@agakaz.kz
Тулекова Гульназ	К.ф.н., профессор кафедры «Авиационный английский язык» Академии гражданской авиации, Алматы, Казахстан, g.tulekova@agakaz.kz
Кошеков Абай	PhD, ассоциированный профессор кафедры «Авиационная техника и технологии» Академии гражданской авиации, Алматы, Казахстан E-mail: a.k.koshekov@gmail.com
Куанов Еркнат	Научный сотрудник Академии гражданской авиации, Алматы, Казахстан E-mail: e.kuanov@agakaz.kz



UDC 004.048

IRSTI 20.15.13

https://doi.org/10.53364/24138614_2025_38_3_12

A. Mukashova^{1,2*}, J. Tussupov², A. Mukhanova², V. Makhatova³, L. Kurmangaziyeva³

¹Astana IT University, Kazakhstan

²L.N. Gumilyov Eurasian National University, Kazakhstan

³Kh. Dosmukhamedov University Atyrau University, Kazakhstan

*E-mail: A.Mukashova@astanait.edu.kz

INTELLIGENT COMPETENCE AND LEARNING OUTCOMES MANAGEMENT SYSTEM: ADAPTING EDUCATIONAL PROGRAMS TO THE LABOR MARKET

Abstract. *The article presents an intelligent information system (IIS) developed to automate the formation of competencies and learning outcomes based on professional standards. A distinctive feature of the IIS is the integration of professional standards with the Atlas of New Professions, which allows adapting educational programs to the dynamically changing requirements of the labor market and technological transformations. The key functional capabilities of the system are described, including user authentication, generation of competencies and learning outcomes for the design of educational programs. The implementation of the system includes an interactive JavaScript interface with support for asynchronous sending of requests to the server using AJAX technologies. OpenAI generative models are used to automatically generate competencies and learning outcomes. The presented system has a wide range of potential applications: from designing curricula based on competencies to creating career guidance systems, analyzing and forecasting changes in the labor market, as well as adapting educational programs to the requirements of high-tech industries. Thus, the developed model contributes to the digitalization of education, improving its quality and ensuring that educational standards meet the modern challenges of the knowledge economy.*

Keywords: *Competency management, Learning outcomes, Curriculum development, Intelligent information system, Professional standards, Atlas of New Professions.*

Introduction.

Modern educational systems face the need to adapt to new challenges associated with digitalization, globalization and changing labor market requirements. In the conditions of rapid technological progress, the key task is to develop educational programs that ensure the formation of relevant competencies and adaptation of graduates to complex and dynamic professional environments [1,2,3]. In the face of rapid technological progress, modern educational systems face the imperative to evolve and align their programs with the emerging demands of the digital age [1]. The key task is to develop educational curricula that cultivate the relevant competencies and enable graduates to thrive in complex, dynamic professional environments [2]. The need for educational reform is driven by the profound transformations occurring in the labor market, fueled by the accelerating pace of digitalization. As stated in the 'Formation of Requirements to the Competency Model for a University Graduate in the Digital Economy' study, digital technologies can increase company productivity by up to 40% [4]. Accordingly, the key competencies required by modern employers include systems thinking, adaptability, proficiency in IT systems, creative problem-solving, cultural awareness, and teamwork [2]. Alongside this framework, an important

tool for formalizing digital skills and competencies is the Skills Framework for the Information Age (SFIA), a model that classifies digital skills and competencies into seven levels. SFIA is used by international organizations to define the requirements for IT professionals, which makes it an important reference point when designing digital education programs [5].

However, traditional methods of educational programs development and competence formation have a number of limitations:

- Time-consuming processes due to the need for expert analysis of normative documents,
- Subjectivity of competence formulations depending on different interpretations,

Difficulties in scaling and adaptation to changing market requirements [6,7,8].

Overcoming these challenges requires the adoption of innovative approaches to curriculum design and competence development.

As the authors note [9] the key areas for improving educational systems in the digital age, as identified in this research, include:

- Developing adaptive, personalized curricula aligned with evolving labor market demands
- Leveraging data analytics and generative AI to accelerate the design and iteration of educational programs
- Strengthening the connection between educational institutions and industry to ensure graduates' readiness for complex, dynamic professional environments [3,10,11].
- Promoting lifelong learning and continuous upskilling to empower individuals to thrive in the face of technological change [2,11,12,13,14,2,1].

Modern educational systems must undergo a profound transformation to equip graduates with the competencies required by the digital economy and global labor market. Innovative approaches to curriculum design, digital tools for program development, and strengthening academia-industry collaboration are crucial to enabling this evolution [3,2,15].

By addressing these critical challenges, educational systems can fulfill their vital role in equipping the next generation with the competencies required to succeed in the 21st century world of work. The emergence of generative AI provides new opportunities to address these limitations. Generative AI systems are able to automate the creation of competencies and learning outcomes, significantly accelerating the process of designing educational programs and adapting them to the current requirements of the professional environment [16,17,18,19]. Additionally, AI-powered analytics can be leveraged to analyze large datasets of job postings and educational program information, empowering educators to identify emerging skill gaps and inform the development of relevant curricular changes that better prepare students for the evolving labor market demands [20,21,22]. By harnessing the power of technology, educational institutions can become more agile and responsive to the rapidly transforming landscape of work, equipping the next generation with the competencies necessary to thrive in the digital age [2,1,23]. The paper [24] proposes an AI-powered learning recommendation system that utilizes educational data mining to enhance educational outcomes. It employs machine learning algorithms to predict student success and offers personalized, data-driven learning strategies to improve academic interventions. The research [25] proposes a hybrid intelligent system for assessing educational outcomes, utilizing expert systems and fuzzy simulation to structure databases of learning elements, thereby facilitating the formation of competencies and learning outcomes through interactive communication between the system and experts. The results [26] of this research underscore the tremendous potential of leveraging advanced technologies, such as generative AI and educational data analytics, to transform educational systems and better prepare graduates for the dynamic professional environments of the future.

The aim of this study is to create intelligent information systems capable of autonomously generating competencies and learning outcomes based on professional standards, as well as adapting educational programs in real time using a competency map. Thus, this work will open up new prospects for the complete digitalization and intellectualization of the competency modeling

process, which will lead to the creation of more effective, personalized and adaptive educational systems.

Materials and methods.

The proposed system utilizes a combination of data sources and generative AI systems to automate the process of generating competencies and learning outcomes.

The system integrates professional standards, Atlases of new professions, and industry requirements, enabling the automatic formation of competencies that align with user requests and current trends in the professional field.

Additionally, the system aligns the generated competencies and learning outcomes with Bloom's taxonomy verbs, adapting them for integration into educational programs. The generated data is stored in a database, ensuring the possibility of further editing, refinement, and use in the development of educational courses.

Mathematical representation

To build an intelligent information system for comparing professional standards and educational programs, we formalize the relationships between key components: labor functions (LF), knowledge, skills and abilities (KSA), and learning outcomes (LO).

Let $PS = \{PS_1, PS_2, PS_3, \dots, PS_n\}$ be a set of professional standards, $LF = \{LF_1, LF_2, LF_3, \dots, LF_m\}$ be a set of labor functions, and $KSA = \{KSA_1, KSA_2, KSA_3, \dots, KSA_p\}$ be a set of knowledge, skills, and abilities. The set \mathcal{M} is a three-dimensional matrix in which each $LF_{i,l}$ element is associated with the corresponding knowledge, skills and abilities $KSA_{i,j}$ and learning outcomes $LO_{i,j}$. This structure allows modeling interdependencies between labor functions and educational outcomes.

$$\mathcal{M} = \begin{bmatrix} LF_{1,1} & KSA_{1,1} & LO_{1,1} \\ LF_{1,2} & KSA_{1,2} & LO_{1,2} \\ \vdots & \vdots & \vdots \\ LF_{m,n} & KSA_{m,n} & LO_{m,n} \end{bmatrix}$$

To simplify the representation, we construct a matrix \mathcal{N} , where each professional standard PS_k groups the corresponding labor functions LF and relates them to competencies C_k . Thus, the matrix \mathcal{N} allows us to formalize the correspondence between professional standards and educational programs.

$$\mathcal{N} = \begin{bmatrix} PS_1 & LF_{1,1} & LF_{1,2} & \dots & LF_{1,2} & C_1 \\ PS_2 & LF_{2,1} & LF_{2,2} & \dots & LF_{2,2} & C_2 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ PS_k & LF_{k,1} & LF_{k,2} & \dots & LF_{k,2} & C_k \end{bmatrix}$$

We define a correspondence operator φ that maps the set of labor functions, knowledge, skills and abilities to the set of learning outcomes:

$$\varphi = (LF_{i,j}, KSA_{i,j}) \rightarrow LO_{i,j}$$

The matching function $f(y)$ can be represented as:

$$f(y) = \sum_{i=1}^{n_k} \omega_i \cdot LO_{i,j}$$

where ω_i - are the significance coefficients for each learning outcome.

Thus, the proposed model allows to automate the process of building educational trajectories aligned with the requirements of professional standards, as well as to formalize the rules for an intelligent system engaged in the generation of competencies and learning outcomes.

System Architecture

The intelligent information system is built according to the modular principle and includes several interrelated components to ensure smooth management of competencies and learning outcomes. The system consists of three main levels: user interface (Frontend), server part (Backend) and data storage level (Database).

The user interface (Frontend) is designed using JavaScript and AJAX to provide dynamic interaction without reloading pages. This allows users to enter queries (knowledge, skills, abilities) and instantly retrieve the generated competencies. The interface also includes tools for visualization and customization of specialization focus selection, which makes the process of working with the system convenient and intuitive.

The server part (Backend) processes input requests, passes them to the generative model (GPT/OpenAI) and receives the generated results. It also interacts with the database to store and update competency information.

The Database is based on MySQL and is designed to store structured information about new occupations, professional standards and competencies. It provides high performance when executing complex SQL queries, and also contains tables for storing the history of user queries, training results and dynamic changes of competencies. The system architecture is presented in Figure 1.

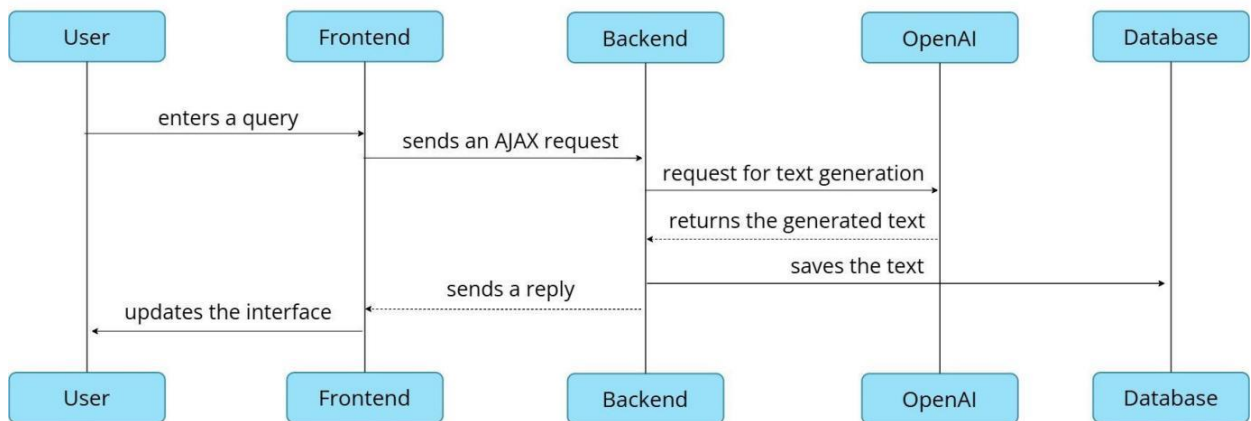


Figure 1 – Intelligent Information System Architecture

User Authentication and Authorization

The system employs a robust user authentication and authorization module to ensure secure access to the platform. Users are required to provide valid credentials, and their roles and permissions are strictly enforced to maintain the integrity of the system. For example, academic administrators can access tools for curriculum development and program evaluation, while instructors can utilize the system to design course materials and assessments aligned with the generated learning outcomes. Figure 2 shows the user access control mechanisms in the system.

ВОЙТИ

Адрес электронный почта:

Пароль:

 [Показать пароль](#)

User Type:

Change user type ▾

- Change user type
- Для администратор
- Для чтение
- As expert

Figure 2 – Authentication and authorization system for user roles and permissions

Automated learning outcomes generation

The main functionality of the IIS is the automated generation of competencies and learning outcomes for educational programs based on professional standards and the Atlas of New Professions. The system analyzes the knowledge, skills, abilities, and job functions outlined in professional standards and uses this data to generate relevant competencies and expected learning outcomes. This ensures the adaptation of educational program content to the current labor market demands.

The practical application of the generation of learning outcomes is shown in Figure 3. The process of generating learning outcomes includes several stages:

1. The system loads knowledge, skills and abilities according to the selected standards.
2. Then the generation method is selected (NLP/Transformer/OpenAI)
3. Then, based on the selected method, the training result is generated.
4. Finally, the obtained learning outcomes are biased towards verbs from Bloom's taxonomy and presented to the user for the development of educational programs.

The screenshot shows a web interface for 'Индикаторы для достижения ключевых компетенций'. At the top, there are filters for 'Проф стандарт' and 'Трудовая функция'. Below, a dropdown menu is set to 'Информационно-коммуника' and 'Администрирование баз данных'. The main content area displays a table with columns for 'Требуемой компетенции', 'расширенной требуемой компетенции', and 'Глубокое расширенной требуемой компетенции'. The table contains detailed text for each stage, with blue circles 1, 2, 3, and 4 marking the steps. A 'Добавить' button is visible at the bottom right of the table.

Figure 3 – Learning outcome generation process

Learning outcomes are generated by analyzing the knowledge, skills, and abilities defined in professional standards, and then translating them into measurable and observable statements. This

ensures that the content of educational programs is closely aligned with the evolving requirements of the labor market. This functionality is supported by various data analysis and verification tools, which minimize human errors and enhance the accuracy of educational material development.

Automated competency generation

The practical application of competence generation is shown in Figure 4. The competence generation process includes several stages:

1. The system loads all labor functions in accordance with the selected standards.
2. Then, the OpenAI methods generate competence in the selected direction
3. Finally, the obtained competencies are shifted towards verbs from Bloom's taxonomy and added to the database to form a competence map.

Ключевые компетенции

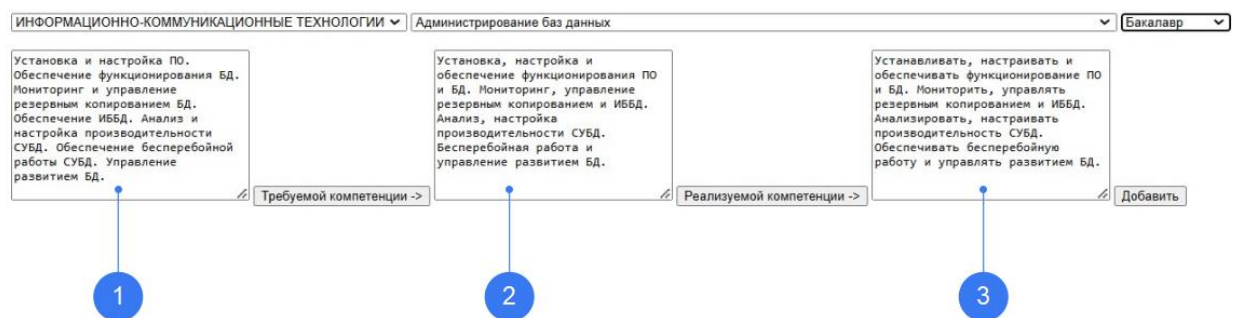


Figure 4 – Competencies generation process

Results and Discussion.

This paper presents an Intelligent Information System (IIS) designed to automate the formulation of competencies and learning outcomes for educational programs. The system integrates professional standards with data from the Atlas of New Professions, ensuring the alignment of educational content with the dynamically evolving labor market requirements and technological advancements.

Key functional capabilities of the system include user authentication, automated competency selection, learning outcome generation, and support for curriculum development. The system's data analysis and verification tools play a crucial role in minimizing human errors and improving the accuracy of educational material development. Additionally, the modular architecture and robust user access controls ensure secure and efficient management of competency-based education.

By streamlining the competency formulation process and integrating multiple data sources, the IIS addresses key challenges associated with educational program development. The automation of competency mapping not only enhances efficiency but also contributes to the adaptability of curricula in response to emerging professional standards and industry demands. The findings demonstrate that the proposed system significantly reduces manual workload, improves consistency in competency formulation, and provides a scalable solution for higher education institutions seeking to modernize their curriculum development processes.

Conclusion.

The developed Intelligent Information System (IIS) represents a significant advancement in educational technology. By leveraging automation and data analysis, the system ensures the effective adaptation of educational programs to the rapidly changing demands of the labor market. The integration of professional standards and labor market data minimizes the gap between the education system and real employer needs.

The key functionalities of the IIS include automated competency selection, learning outcome generation, and support for curriculum development. These tools not only streamline the course planning process but also enhance its relevance through a data-driven approach. Additionally,

built-in data verification and analysis mechanisms ensure the accuracy and reliability of generated educational elements, reducing the risk of errors and improving the overall quality of learning materials.

Despite the achieved results, further development of the IIS involves improving the interpretation of professional standards, enhancing the system's adaptability to diverse educational contexts, and integrating it with modern digital learning platforms. Future research may also focus on developing intelligent recommendations for personalized learning pathways, further enhancing adaptability and individualization in education.

Thus, the proposed system contributes to the digitalization and intellectualization of education, laying the foundation for the development of flexible and efficient educational programs that meet the challenges of the modern technological landscape.

ҚҰЗЫРЕТТЕРДІ ЖӘНЕ ОҚЫТУ НӘТИЖЕЛЕРІН БАСҚАРУДЫҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕСІ: БІЛІМ БЕРУ БАҒДАРЛАМАЛАРЫН ЕҢБЕК НАРЫҒЫНА БЕЙІМДЕУ

Аңдатпа: Мақалада кәсіби стандарттар негізінде құзыреттіліктер мен оқыту нәтижелерін қалыптастыруды автоматтандыруға арналған Интеллектуалды ақпараттық жүйе (ИАЖ) ұсынылған. ИАЖ-ның айрықша ерекшелігі-білім беру бағдарламаларын еңбек нарығының серпінді өзгеріп отыратын талаптарына және технологиялық өзгерістерге бейімдеуге мүмкіндік беретін жаңа кәсіптер Атласымен кәсіби стандарттарды интеграциялау болып табылады. Жүйенің негізгі функционалдығы, соның ішінде пайдаланушының аутентификациясы, білім беру бағдарламаларын жобалау үшін құзыреттілік пен оқу нәтижелерін қалыптастыру сипатталған. Жүйені енгізу AJAX технологияларын қолдана отырып, серверге асинхронды сұраныстарды жіберуді қолдайтын JavaScript-те интерактивті интерфейсін қамтиды. Құзыреттілік пен оқу нәтижелерін автоматты түрде қалыптастыру үшін OpenAI генеративті модельдері қолданылады. Ұсынылған жүйе құзыреттілікке негізделген оқу жоспарларын жобалаудан бастап кәсіптік бағдар жүйелерін құруға, еңбек нарығындағы өзгерістерді талдауға және болжауға, сондай-ақ білім беру бағдарламаларын жоғары технологиялық салалардың талаптарына бейімдеуге дейінгі әлеуетті қолданудың кең спектріне ие. Осылайша, әзірленген модель білім беруді цифрландыруға, оның сапасын арттыруға және білім беру стандарттарының білім экономикасының заманауи талаптарына сай болуын қамтамасыз етуге ықпал етеді.

Түйін сөздер: Құзыреттілікті басқару, Оқыту нәтижелері, Оқу бағдарламаларын әзірлеу, Интеллектуалды ақпараттық жүйе, Кәсіби стандарттар, Жаңа кәсіптер Атласы.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ КОМПЕТЕНЦИЯМИ И РЕЗУЛЬТАТАМИ ОБУЧЕНИЯ: АДАПТАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ К РЫНКУ ТРУДА

Аннотация: В статье представлена интеллектуальная информационная система (ИИС), разработанная для автоматизации формирования компетенций и результатов обучения на основе профессиональных стандартов. Отличительной особенностью ИИС является интеграция профессиональных стандартов с Атласом новых профессий, что позволяет адаптировать образовательные программы к динамично изменяющимся требованиям рынка труда и технологическим трансформациям. Описаны ключевые функциональные возможности системы, включая аутентификацию пользователей, генерацию компетенций и результатов обучения для проектирования образовательных программ. Реализация системы включает интерактивный интерфейс на JavaScript с

поддержкой асинхронной отправки запросов на сервер с использованием технологий AJAX. Для автоматической генерации компетенций и результатов обучения применяются генеративные модели OpenAI. Представленная система имеет широкий спектр потенциальных применений: от проектирования учебных планов, основанных на компетенциях, до создания систем карьерного ориентирования, анализа и прогнозирования изменений на рынке труда, а также адаптации образовательных программ к требованиям высокотехнологичных отраслей. Таким образом, разработанная модель способствует цифровизации образования, повышению его качества и обеспечению соответствия образовательных стандартов современным вызовам экономики знаний.

Ключевые слова: *Управление компетенциями, Результаты обучения, Разработка учебных программ, Интеллектуальная информационная система, Профессиональные стандарты, Атлас новых профессий.*

References

1. Maj-Waśniowska, K., Stanienda, J., & Wyrobek, J. (2022). Challenges for the education system in the era of the Fourth Industrial Revolution. Routledge eBooks, Informa. <https://doi.org/10.4324/9781003274681-7>
2. Theoretical analysis on the effect of digitalization on the labor market. (2019, September 5). <https://doi.org/10.34190/km.19.110>
3. Digitalization of education in modern scientific discourse: New trends and risks analysis. (2020, June 12). Academic Publisher House Researcher. <https://doi.org/10.13187/ejced.2020.2.313>
4. Formation of requirements to the competency model for a university graduate in the digital economy. (2019). <https://doi.org/10.2991/icdtli-19.2019.58>
5. Brown, J. (2019, December 27). An examination of the skills framework for the information age (SFIA) version 7. International Journal of Information Management. Elsevier BV. <https://doi.org/10.1016/j.ijinfomgt.2019.102058>
6. Sitopu, J. W., Khairani, M., Roza, M., Judijanto, L., & Aslan. (2024). The importance of integrating mathematical literacy in the primary education curriculum: A literature review.
7. Soledad, M., Andrade-Vargas, L., Rivera, D., & Castro, M. P. (2021, June 29). Trends for the future of education programs for professional development. Sustainability, 13(13), 7244. Multidisciplinary Digital Publishing Institute. <https://doi.org/10.3390/su13137244>
8. Padovano, A., & Cardamone, M. (2024, June 15). Towards human-AI collaboration in the competency-based curriculum development process: The case of industrial engineering and management education. Computer Applications in Engineering Education. Elsevier BV. <https://doi.org/10.1016/j.caeai.2024.100256>
9. Alshantqiti, A., Alam, T., Benaida, M., Namoun, A., & Taleb, A. (2020). A rule-based approach toward automating the assessments of academic curriculum mapping. International Journal of Advanced Computer Science and Applications, 11(11), 285. Science and Information Organization. <https://doi.org/10.14569/ijacsa.2020.0111285>
10. Personalized education in the artificial intelligence era: What to expect next. (2021). <https://doi.org/10.1109/msp.2021.3055032>
11. International experience of artificial intelligence implementation in the field of science and higher education. (2021). <https://doi.org/10.2991/aebmr.k.211118.115>
12. Zhai, X., et al. (2021). A review of artificial intelligence (AI) in education from 2010 to 2020. Complexity, 2021(1). Hindawi Publishing Corporation. <https://doi.org/10.1155/2021/8812542>
13. Academic policy regarding sustainability and artificial intelligence (AI). (2020). <https://doi.org/10.3390/su12229435>

14. Rambousek, V., Fuglík, V., & Štípek, J. (2015, June 30). Selected outcomes of research of digital competency development on elementary schools. *Educational Research and Innovation*, 8(2). Czech University of Life Sciences Prague. <https://doi.org/10.7160/eriesj.2015.080201>
15. Leybert, T. B., & Khalikov, E. (2019, January 1). Digital and organizational transformation of the educational process. <https://doi.org/10.2991/icdtli-19.2019.20>
16. Łodzikowski, K., Foltz, P. W., & Behrens, J. T. (2024). Generative AI and its educational implications. *Postdigital Science and Education*. Springer International Publishing. https://doi.org/10.1007/978-3-031-64487-0_2
17. Yan, L., Greiff, S., Teuber, Z., & Gašević, D. (2024, October). Promises and challenges of generative artificial intelligence for human learning. *Nature Human Behaviour*. Retrieved February 2, 2025, from <https://www.nature.com/articles/s41562-024-02004-5>
18. Gonzalez-Rodriguez, M. (2023, July). Empowering education with generative artificial intelligence tools: Approach with an instructional design matrix. *Sustainability*, 15(15), 11524. Retrieved February 2, 2025, from <https://www.mdpi.com/2071-1050/15/15/11524>
19. Bastani, H., Bastani, O., Sungu, A., Ge, H., Kabakçı, Ö., & Mariman, R. (2024, January 1). Generative AI can harm learning. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4895486>
20. Börner, K., Scrivner, O., Gallant, M., Ma, S., Liu, X., Chewning, K., Wu, L., & Evans, J. A. (2018, December). Skill discrepancies between research, education, and jobs reveal the critical need to supply soft skills for the data economy. *Proceedings of the National Academy of Sciences*. Retrieved February 2, 2025, from <https://www.pnas.org/doi/full/10.1073/pnas.1804247115>
21. Acemoglu, D. (2021, August). The demand for AI skills in the labor market. *Labour Economics*. Retrieved February 2, 2025, from <https://www.sciencedirect.com/science/article/abs/pii/S0927537121000373>
22. Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Ogundipe, D. O. (2024, April 10). Revolutionizing education through AI: A comprehensive review of enhancing learning experiences. *International Journal of Applied Research in Social Sciences*, 6(4), 589. Fair East Publishers. <https://doi.org/10.51594/ijarss.v6i4.1011>
23. What students can learn about artificial intelligence – Recommendations for K-12 computing education. (2024). https://doi.org/10.1007/978-3-031-43393-1_19
24. Herath, D., Dinuwan, C., Ihalagedara, C., & Ambegoda, T. D. (2024, January 1). Enhancing educational outcomes through AI powered learning strategy recommendation system. *International Journal of Advanced Computer Science and Applications*, 15(10), 75. Science and Information Organization. <https://doi.org/10.14569/ijacsa.2024.0151075>
25. Smirnov, E., Dvoryatkina, S. N., & Shcherbatykh, S. V. (2022, April 5). Parameters and structure of neural network databases for assessment of learning outcomes. <https://doi.org/10.6000/1929-4409.2020.09.188>
26. Sari, H., Tumanggor, B., & Efron, D. (2024, November 6). Improving educational outcomes through adaptive learning systems using AI. *Italic*, 3(1). <https://doi.org/10.33050/italic.v3i1.647>

Авторлар туралы мәлімет

Айнур Мукашова	сенъор лектор, Есептеу және деректер туралы ғылым департаменті, Astana IT University, Қазақстан. E-mail: A.Mukashova@astanait.edu.kz , ORCID: https://orcid.org/0009-0007-2794-4748
Джамалбек Тусупов	ф.-м.ғ. докторы, профессор, Гумилев атындағы Еуразиялық ұлттық университеті, Астана, Қазақстан, email: tussupov@mail.ru; https://orcid.org/0000-0002-9179-0428
Аягоз Муханова	PhD, Ақпараттық технологиялар факультеті, Л. Н. Гумилев атындағы Еуразия Университеті, Астана, Қазақстан. E-mail: ayagoz198302@mail.ru , ORCID: https://orcid.org/0000-0003-3987-0938
Махатова Валентина	Профессор, т. ғ.к., Х. Досмұхамедов атындағы Атырау университеті, Атырау. Қазақстан. E-mail: mahve@mail.ru , ORCID: https://orcid.org/0000-0002-4082-9193
Курмангазиева Ляйля Таскалиевна	Профессор, т. ғ.к., Х. Досмұхамедов атындағы Атырау университеті, Атырау. Қазақстан. E-mail: Kurmangazieval@mail.ru ORCID ID: https://orcid.org/0000-0003-0640-7306

Сведение об авторах

Айнур Мукашова	сенъор лектор, Департамент Вычислений и науки о данных, Astana IT University, Казакстан. E-mail: A.Mukashova@astanait.edu.kz , ORCID: https://orcid.org/0009-0007-2794-4748
Джамалбек Тусупов	д. ф.-м. н., профессор, заведующий кафедрой «Информационные системы» факультета информационных технологий Евразийского национального университета им. Л. Н. Гумилева, E-mail: tussupov@mail.ru, https://orcid.org/0000-0002-9179-0428 ;
Аягоз Муханова	PhD, Факультет информационных технологий, Евразийский университет имени Л.Н. Гумилева, Астана, Казакстан. E-mail: ayagoz198302@mail.ru , ORCID: https://orcid.org/0000-0003-3987-0938
Махатова Валентина	Профессор, к.т.н., кафедры программной инженерии, Атырауский университет имени Х. Досмұхамедова, Атырау, Казакстан. E-mail: mahve@mail.ru , ORCID: https://orcid.org/0000-0002-4082-9193
Курмангазиева Ляйля Таскалиевна	Профессор, к.т.н., Атырауский университет имени Х. Досмұхамедова, Атырау. Казакстан. E-mail: Kurmangazieval@mail.ru ORCID ID: https://orcid.org/0000-0003-0640-7306

Information about the authors

Ainur Mukashova	Senior Lecturer, Department of Computation and Data Science, Astana IT University, Astana, Kazakhstan. E-mail: A.Mukashova@astanait.edu.kz , ORCID: https://orcid.org/0009-0007-2794-4748
Jamalbek Tussupov	Doctor of Physical and Mathematical Sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: tussupov@mail.ru, https://orcid.org/0000-0002-9179-0428
Ayagoz Mukhanova	PhD, Department of Information technology, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan. E-mail: ayagoz198302@mail.ru , orcid.org/0000-0003-3987-0938
Makhatova Valentina	Candidate of technical science, professor of the Department of software engineering, Kh.Dosmukhamedov University Atyrau University, Kazakhstan. E-mail: mahve@mail.ru , ORCID: https://orcid.org/0000-0002-4082-9193
Kurmangaziyeva Lyailya	Professor, Candidate of technicalscience, Atyrau University named after H. Dosmukhamedov, Atyrau, Kazakhstan. e-mail: Kurmangazieval@mail.ru ORCID ID: https://orcid.org/0000-0003-0640-7306



ӘОЖ 004.056.53

ҒТАХА 28.23.15

https://doi.org/10.53364/24138614_2025_38_3_13

С.А. Адилжанова¹, Б. Қ. Ыбрайымбай^{1*}, Л. Ш.Черикбаева¹

¹ Өл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан

*E-mail: baxa.nusipov01@mail.ru

ЭНЕРГЕТИКАЛЫҚ НЫСАНДАР ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ АРҚЫЛЫ DDoS ШАБУЫЛДАРЫНАН ҚОРҒАУ ЖҮЙЕСІН ӘЗІРЛЕУ

Аңдатпа. Энергетикалық нысандарды цифрландыру олардың жұмыс істеуінің ажырамас бөлігіне айнала отырып, киберқауіптердің, соның ішінде қызмет көрсетуден бас тартуға бағытталған шабуылдардың (DDoS) артуына алып келуде. Мұндай шабуылдар SCADA жүйелері, IoT құрылғылары және интеллектуалды энергетикалық желілердің тұрақты жұмысын бұзып, сыни инфрақұрылымға елеулі қатер төндіреді. Мақалада энергетикалық сектордағы DDoS шабуылдарын анықтау мен болдырмаудың заманауи әдістері қарастырылады. Бұл мақсатта машиналық оқыту әдістері (Random Forest, Decision Tree, Gradient Boosting, SVM) және терең оқыту модельдері (CNN, LSTM), сондай-ақ олардың гибриді нұсқалары (LSTM-CNN) талданады. Модельдердің тиімділігі CICDDoS2019 және KDD-CUP деректер жиынтықтары, сондай-ақ SCADA жүйесінің модельденген тестілік ортасында бағаланды. Негізгі назар энергетикалық нысандардағы желілік трафиктегі аномалияларды нақты уақыт режимінде анықтай алатын, жаңа қауіптерге бейімделетін интеллектуалды қорғаныс жүйесін құруға бағытталады. Зерттеу нәтижелері гибриді модельдердің шабуылды анықтау дәлдігінің кейбір сценарийлерде 99%-ға жететінін көрсетті. Сонымен қатар, блокчейн және бұлттық технологияларды интеграциялау арқылы киберқауіпсіздікті арттыру мүмкіндіктері қарастырылды. Алынған қорытындылар энергетикалық инфрақұрылымды қорғауға арналған кешенді шешімдерді әзірлеуде практикалық тұрғыда қолдануға жарамды.

Түйін сөздер: Киберқауіпсіздік, DDoS-шабуылдар, энергетикалық нысандар, SCADA, IoT, машиналық оқыту, терең оқыту, гибриді модельдер, блокчейн, интеллектуалды желілер.

Кіріспе.

Қазіргі таңда энергетика саласы интеллектуалды жүйелерге, бұлттық технологияларға және Интернет заттары (IoT) инфрақұрылымына негізделген цифрландыру бағытымен қарқынды дамуда. Бұл технологиялар өндірістік және басқару процестерінің тиімділігін арттырғанымен, желілік инфрақұрылымның қауіпсіздігіне қатысты жаңа сын-тегеуріндер туындатуда. Әсіресе, қызмет көрсетуден бас тартуға бағытталған шабуылдар (Distributed Denial of Service – DDoS) SCADA жүйелері, IoT құрылғылары мен интеллектуалды энергетикалық желілердің қалыпты жұмысын бұзып, маңызды жүйелердің істен шығуына, өндіріс циклінің үзілуіне және әлеуетті техногендік апаттарға алып келуі мүмкін. DDoS-шабуылдар көбіне желіні шамадан тыс жүктеу арқылы жүзеге асырылады, бұл ретте шабуылдаушы құрылғылардың ботнет желісі арқылы SCADA-серверге зиянды трафик

жіберіп, жүйенің жауап беру мүмкіндігін тежейді. Электр станциялары, қосалқы станциялар, таратушы желілер мен тұтыну мониторингі жүйелері сияқты сыни энергетикалық нысандар мұндай шабуылдарға ерекше осал келеді. Олардың салдары тек экономикалық шығынмен шектеліп қалмай, қоғам өміріне де тікелей қауіп төндіруі мүмкін[1].

Дәстүрлі қорғау механизмдері – статикалық ережелерге немесе сигнатураларға негізделген тәсілдер – қазіргі заманғы күрделі шабуылдарды ерте кезеңде анықтап, тиімді түрде алдын алуға қауқарсыз болып отыр. Осыған байланысты шабуыл үлгілерін автоматты түрде үйреніп, бейімделе алатын интеллектуалды киберқауіпсіздік жүйелерін әзірлеу қажеттілігі туындайды. Бұл зерттеудің негізгі мақсаты – энергетикалық нысандарға бағытталған DDoS-шабуылдарды жоғары дәлдікпен анықтай алатын, нақты уақыт режимінде әрекет ететін интеллектуалды анықтау жүйесін әзірлеу. Осы мақсатта машиналық оқыту (Random Forest, Decision Tree, SVM, Gradient Boosting) және терең оқыту (LSTM, CNN) әдістері қолданылды. Сонымен қатар, олардың гибридті комбинациялары (мысалы, LSTM-CNN) салыстырылып, тиімділік көрсеткіштері (Accuracy, Precision, Recall, F1-score) негізінде бағаланды. Зерттеу дереккөздері ретінде CICDDoS2019, KDD-CUP сияқты танымал жиынтықтармен қатар, SCADA жүйесінің модельденген сынақтық ортасында алынған шынайы желілік трафик пайдаланылды. Зерттеу нәтижелері энергетикалық жүйелер үшін бейімделетін интеллектуалды қорғаныс архитектураларын құруда гибридті тәсілдердің қолдану тиімділігін дәлелдейді және бұлттық технологиялар мен блокчейн әдістерін интеграциялау арқылы жүйенің сенімділігін арттыруға бағыт берді[2].

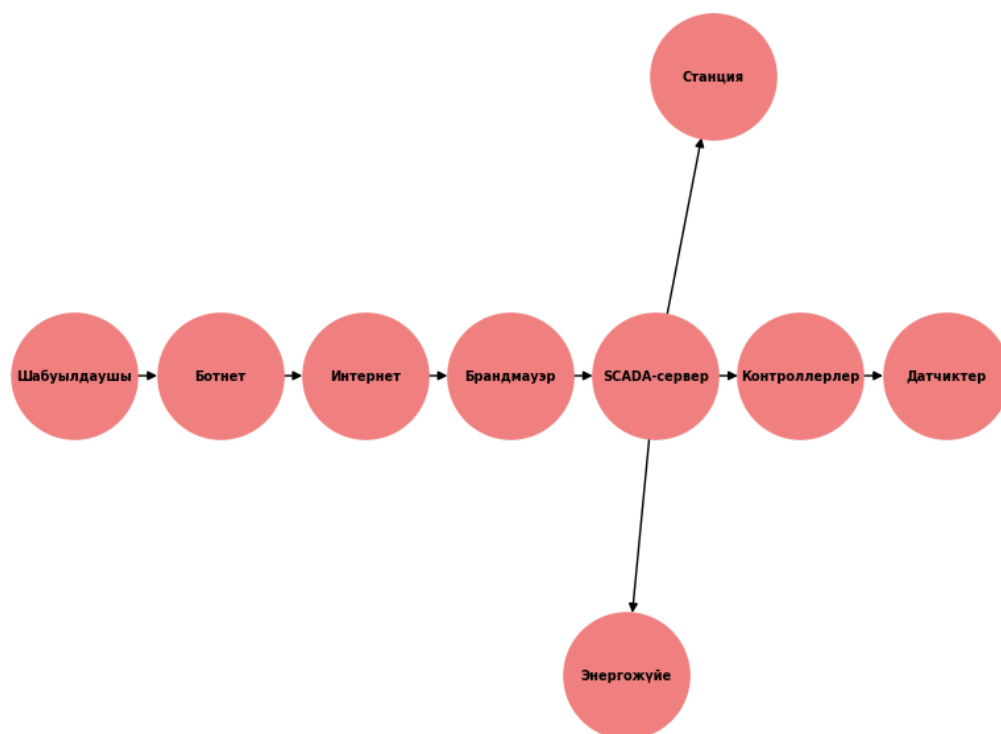
Зерттеу материалдары мен әдістері.

Зерттеу жұмысы энергетикалық инфрақұрылымдағы SCADA жүйелеріне жасалатын DDoS-шабуылдарды машиналық оқыту және терең оқыту әдістері арқылы тиімді анықтау және олардан қорғау жүйесін құруға бағытталды. Энергетикалық нысандардағы DDoS-шабуылдарды модельдеу үшін нақты деректер жиынтықтары (CICDDoS2019, KDD-CUP) және SCADA жүйесінің жұмысын имитациялайтын тестілік ортадағы желілік трафик пайдаланылды. Деректерді жинау үшін Wireshark және Zeek мониторинг құралдары, ал шабуылдарды эмуляциялау үшін hping3, LOIC, HOIC құралдары қолданылды. Жиналған мәліметтер құрамына IP-адресстер, жіберілген пакеттер көлемі, қолданылған протоколдар, уақыт белгілері және басқа желілік сипаттамалар енгізілді.

Зерттеу барысында бес негізгі DDoS-шабуыл түрі (TCP Flood, UDP Flood, SYN Flood, ICMP Flood, IP Spoofing) жеке-жеке модельденді. Қалыпты трафик эталон ретінде алынды. Бұл тәсіл әрбір модельдің түрлі шабуыл сценарийіндегі нәтижелілігін объективті бағалауға мүмкіндік берді.

DDoS-шабуылдарды анықтау үшін классикалық және терең оқыту модельдері таңдалды. Decision Tree және Random Forest: құрылымдалған желілік деректермен тұрақты және интерпретациясы оңай болғандықтан таңдалды. LSTM-CNN гибриді: уақыттық заңдылықтарды тиімді үйрену, күрделі шабуылдарды динамикалық талдау үшін енгізілді. Салыстыру үшін Gradient Boosting, SVM, KNN сияқты басқа әдістер де пайдаланылды.

Сурет 1-де көрсетілген шабуыл механизмі ең алдымен шабуылдаушы ботнетке шабуылды бастау командасын жібергеннен басталады. Ботнет үлкен көлемдегі зиянды трафикті қалыптастырады. Трафик интернет арқылы өтіп, SCADA серверіне жетеді. Желі аралық экран пакеттерді сүзгіден өткізуге тырысады, бірақ қарқынды шабуыл кезінде шамадан тыс жүктелуі мүмкін. SCADA сервері жүктемеге төтеп бере алмай, істен шығып, энергетикалық инфрақұрылым басқаруында ақаулар туындайды [3].



Сурет 1 – SCADA жүйесіне DDoS-шабуыл схемасы

Нәтижелер және оны талқылау.

Модельдерді таңдау кезінде олардың энергетикалық инфрақұрылымға бейімділігі, нәтижелердің ғылыми негізделуі және заманауи әдебиеттегі тиімділігі ескерілді. Барлық модельдерді оқыту және тестілеу үшін Scikit-Learn және TensorFlow кітапханалары қолданылды. Модельдердің гиперпараметрлері Grid Search және кросс-валидация (cross-validation) арқылы анықталды. Деректер жиынтығының өкілдігін арттыру үшін SMOTE әдісімен класстар теңестірілді. Модельдер тиімділігі дәлдік (Accuracy), шабуылды болжау дәлдігі (Precision), толықтық (Recall) және F1-score секілді негізгі метрикалар арқылы бағаланды. Зерттеу нәтижелері бойынша, гибриді модельдер мен терең оқыту әдістері SCADA жүйелерінде DDoS-шабуылдарды анықтауда жоғары тиімділік көрсетті. Кейбір сценарийлерде дәлдік 99%-ға дейін жетті[4].

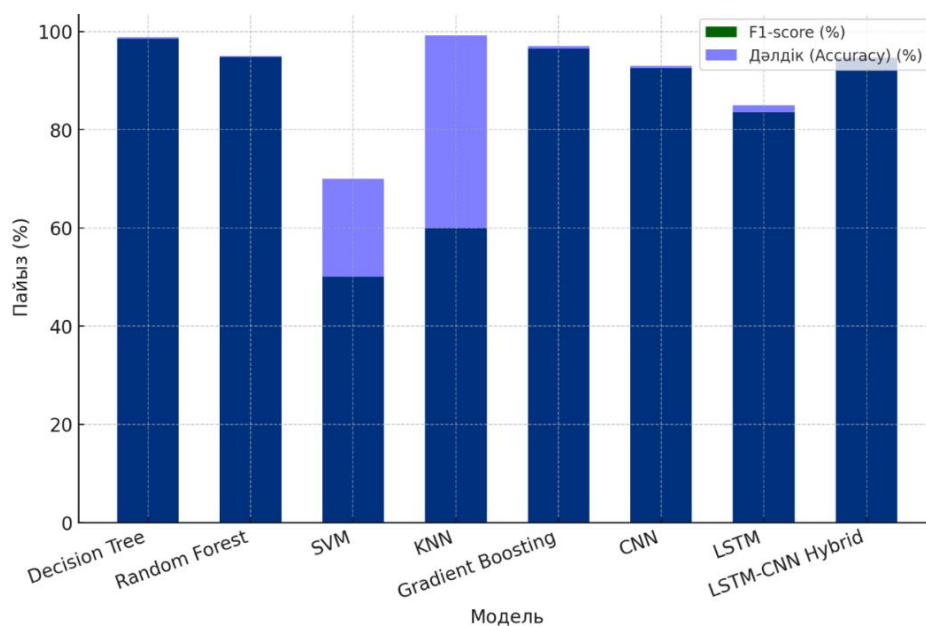
Кесте 1 - Жүргізілген зерттеулер негізінде алынған нәтижелер

	Мақала	Анықтама	Датасет	Әдіс	Нәтиже
1	Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain	Мақалада энергетикалық жүйелердегі DoS/DDoS шабуылдарын классификациялау және идентификациялау үшін Deep Learning мен LSTM біріктіретін гибриді машиналық оқыту	IoT құрылғылары мен блокчейн инфрақұрылымынан (DERs) жиналған жеке деректер жиынтығы.	Deep Learning, LSTM	HML моделі шабуылдарды 95%-ға дейінгі дәлдікпен классификациялай алды.

	(IoBC)-based energy networks. <i>Data in Brief</i> , 54, 110461.	моделі (HML) ұсынылған.			
2	Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. <i>International Journal of Science and Research Archive</i> , 13(01), 3417-3435.	SCADA жүйелерін жаңғырту үшін IoT, машиналық оқыту және бұлттық технологияларды біріктіру зерттеледі. Алдын ала техникалық қызмет көрсету, аномалияларды анықтау және киберқауіпсіздік мәселелері сипатталған.	SCADA IoT құрылғылары мен бұлттық жүйелердің деректерін қамтитын әртүрлі өндірістік деректер жиынтықтары.	Random Forest, LSTM, k-means	Random Forest алдын ала техникалық қызмет көрсету үшін 90–93% дәлдік көрсетті, ал LSTM уақыттық деректермен жұмыс істегенде 95%-ға дейін дәлдікке жетті.
3	Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. <i>Egyptian Informatics Journal</i> , 28, 100540.	Мақалада мультиэнергетикалық жүйелердегі IoT құрылғыларына жасалған DDoS-шабуылдарды анықтау үшін машиналық оқыту әдістері (Gradient Boosting, Random Forest және басқалары) қарастырылады.	CICDDOS2019, KDD-CUP	Gradient Boosting, Random Forest	Gradient Boosting шабуылдарды талдау үшін ең жоғары 99.16% дәлдік көрсетті, бұл оны IoT ортасындағы шабуылдарды анықтауда ең тиімді әдіс етеді.
4	Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for	SCADA жүйелеріне жасалған шабуылдарды классификациялау және анықтау үшін	Жеке деректер жиынтығы (SCADA тестілік ортасы),	LSTM, CNN, LSTM-CNN Hybrid,	LSTM-CNN гибриді моделі 94.73% дәлдік көрсетті, ал Decision Tree

Classification and Detection of DDoS Attacks on SCADA Systems. <i>Applied Sciences</i> , 13(5993).	LSTM-CNN гибриді тәсілі мен машиналық оқыту әдістері зерттеледі. Шабуылдарды модельдеу үшін тестілік орта іске асырылды.	Mississippi State University SCADA зертханасы.	Decision Tree, Random Forest	98.77%-ға жетіп, оны SCADA жүйелері үшін ең тиімді әдіс етті.
--	--	--	------------------------------	---

Сурет 2-де көрсетілген зерттеу нәтижелері, Decision Tree моделі 98.77% дәлдік және жоғары F1-score көрсетіп, SCADA жүйелеріндегі DDoS-шабуылдарды анықтаудың ең тиімді әдісі ретінде танылды, ал LSTM-CNN гибриді моделі 94.73% дәлдікке қол жеткізіп, шабуылдарды классификациялауда жақсы теңгерім көрсетті. Сонымен қатар, SVM және KNN әдістері төмен тиімділік көрсетіп, шабуылдарды классификациялау үшін тиімсіз екендігі анықталды. Гибриді тәсілдердің артықшылығы да дәлелденді: LSTM-CNN моделі жеке CNN немесе LSTM-ге қарағанда жоғары нәтиже көрсетіп, трафиктегі уақыттық және кеңістіктік заңдылықтарды тиімдірек талдауға мүмкіндік берді. SCADA жүйесінің нақты трафиінде тестілеу көрсеткендей, Decision Tree және LSTM-CNN модельдері шабуылдарды 1 секундтан аз уақыт ішінде анықтап, оларды нақты уақыт режимінде қолдануға болатындығын дәлелдеді. Сонымен қатар, зерттеу барысында блокчейн технологиясын шабуыл үлгілері мен аномалияларды сақтау үшін пайдалану мүмкіндігі қарастырылды, бұл жүйенің деректердің бұрмалануына төзімділігін арттыруға мүмкіндік береді. Зерттеу нәтижелерін ескере отырып, LSTM-CNN гибриді моделі мен Decision Tree энергетикалық нысандардағы DDoS-шабуылдарды анықтау үшін ең перспективті әдістер екені анықталды. Терең оқыту әдістерін қолдану шабуылдарды анықтау дәлдігін арттырғанымен, олардың үлкен есептеу ресурстарын қажет ететіндігі белгілі болды. Осыған байланысты, SCADA жүйелерін қорғау үшін машиналық оқыту модельдерін блокчейн және бұлттық технологиялармен біріктіру қажет. Алдағы зерттеулер модельдерді жаңа шабуыл түрлеріне бейімдеуге, сондай-ақ олардың жоғары жүктемелі желілерде тиімділігін арттыруға бағытталуы тиіс[5].



Сурет 2 – Әртүрлі модельдердің дәлдігі (Accuracy) мен F1-score көрсеткіштерін салыстыратын график

Заманауи зерттеулер SCADA жүйелеріне жасалатын DDoS-шабуылдарды анықтау және классификациялау, машиналық оқыту әдістерін қолдану, сондай-ақ IoT және блокчейн технологияларын сыни инфрақұрылымның киберқауіпсіздігіне біріктіру мәселелерін қарастырады. Дегенмен, олардың ғылыми және практикалық құндылығын арттыру үшін бірнеше аспектілерді жетілдіру қажет. Біріншіден, эксперименттер мен тестілеуді кеңейту маңызды, өйткені қазіргі зерттеулерде көбінесе CICDDoS2019, KDD-CUP сияқты шектеулі деректер жиынтықтары қолданылады. Нақты энергетикалық нысандардан алынған мәліметтерді енгізу қорытындылардың сенімділігін арттырады. Сонымен қатар, AWS, Azure немесе Google Cloud секілді бұлттық платформаларда модельдерді сынау, олардың нақты ортада қаншалықты тиімді екенін бағалауға мүмкіндік береді[6].

Зерттеулерде белгілі бір алгоритмдердің (мысалы, Decision Tree немесе LSTM-CNN) тиімділігі көрсетілгенімен, қателіктердің егжей-тегжейлі талдауы жиі назардан тыс қалады. ROC, PR және AUC-ROC метрикаларын енгізу модельдердің өнімділігін жан-жақты бағалауға көмектеседі. Екіншіден, гибриді әдістер мен жаңа модельдерді қарастыру қажет. Decision Tree және нейрондық желілерден тұратын ансамбльдік әдістер шабуылдарды дәлірек анықтауға мүмкіндік береді, ал Self-Supervised Learning (SSL) және Federated Learning (FL) әдістерін енгізу үлкен деректерді алдын ала белгілеу қажеттілігін азайтып, модельдерді орталықтандырылмаған ортада оқытуға мүмкіндік береді. Үшіншіден, киберқауіпсіздікті басқа технологиялармен біріктіру де өзекті болып отыр. Блокчейнді тек деректерді сақтау үшін ғана емес, сонымен қатар таратылған аутентификацияны жүзеге асыру үшін қолдану мүмкіндігі бар, бұл MITM шабуылдарынан қорғануды күшейтеді. Сондай-ақ Zero Trust Security (ZTS) қағидасын енгізу арқылы SCADA жүйелерінде пайдаланушылар мен құрылғыларға әдепкі сенім білдірмеуді қамтамасыз ету, ал SIEM жүйелерін машиналық оқыту модельдерімен біріктіру оқиғаларды автоматты түрде корреляциялауға мүмкіндік береді. Төртіншіден, модельдердің практикалық енгізілуі мен валидациясы маңызды, өйткені көптеген зерттеулер зертханалық жағдайда немесе тестілік ортада жүргізіледі, ал модельдерді нақты SCADA жүйелерінде қолдану олардың тиімділігін дәлелдеуге көмектеседі. Сонымен қатар, киберқауіпсіздік шешімдерін енгізу құнын талдау, машиналық оқыту модельдерін оқытуға кететін шығындарды бағалау, сондай-ақ DDoS-шабуылдардың энергетикалық инфрақұрылымға тигізетін қаржылық әсерін зерттеу маңызды. Соңында, зерттеу аясын кеңейту болашақ киберқауіпсіздік жүйелерін жетілдіруге мүмкіндік береді. Автономды шабуылға қарсы жүйелерді дамыту, Reinforcement Learning (RL) негізінде SCADA жүйелерін қорғау, сондай-ақ SCADA жүйелерінде AI қолдану барысында құқықтық шектеулер мен этикалық аспектілерді қарастыру зерттеудің болашақ бағыттары ретінде ұсынылады. Бұл ұсыныстар SCADA жүйелерінің қауіпсіздігін жаңа деңгейге көтеруге, сондай-ақ DDoS-шабуылдардан қорғанудың тиімділігін арттыруға мүмкіндік береді[7].

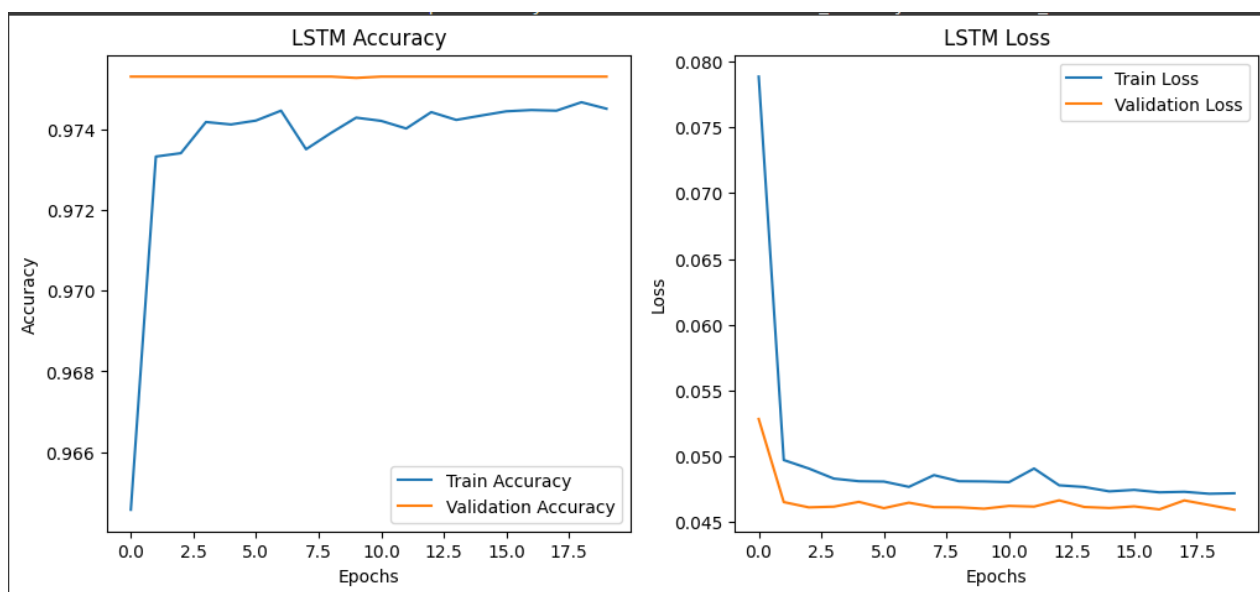
Қазіргі таңда машиналық оқыту әдістері DDoS-шабуылдардан қорғанудың негізгі құралдарының біріне айналууда. Алайда қолданыстағы тәсілдер әрдайым шабуылдарды анықтаудың жеткілікті дәлдігі мен толықтығын қамтамасыз ете алмайды. Әсіресе, желілік трафиктің уақыт өте өзгеруіне байланысты дәстүрлі әдістер шабуылдардың жаңа үлгілерін тиімді анықтауда қиындықтарға тап болады. Сондықтан бұл зерттеуде терең оқыту (LSTM) және классикалық машиналық оқыту әдістерін (Random Forest, Decision Tree) біріктіруге негізделген жетілдірілген шешім ұсынылады. Бұл тәсіл шабуылдардың уақыттық заңдылықтарын тереңірек талдауға мүмкіндік береді, жүйенің динамикалық өзгерістерге бейімділігін арттырады. Сонымен қатар, Random Forest және Decision Tree алгоритмдерінің гиперпараметрлерін оңтайландыру арқылы желілік трафикті дәлірек классификациялау мүмкіндігі қарастырылды [8].

Зерттеудің басты мақсаты – желілік трафиктегі аномалияларды және DDoS-шабуылдарды дәл әрі автоматты түрде анықтайтын жүйе құру және оны кең көлемді нақты

деректерде тексеру болды. Осы мақсатта бірінші кезекте Random Forest пен Decision Tree әдістері желідегі құрылымдық заңдылықтарды және аномалияларды тануға, ал LSTM архитектурасы трафиктің уақыттық динамикасын талдауға бағытталды. Нәтижелерді толық бағалау үшін әрбір модельдің оқыту үдерісі, қателік матрицасы, ROC сияқты визуализациялар мен метрикалар қолданылды. Бұл процестердің барлығы автоматтандырылған Python коды арқылы жүзеге асырылды [9].

Зерттеу деректер жиынтығы 311 028 желілік қосылымнан тұрды, оның бір бөлігі қалыпты трафик, қалғаны DDoS-шабуылдарға тиесілі. Бұл үлкен көлемді әрі әртараптандырылған жиынтық модельдердің әртүрлі шабуыл сценарийлеріндегі жұмысын жан-жақты бағалауға жағдай жасады. Шабуылдарды сенімді анықтау үшін бірнеше машиналық оқыту әдісі қолданылды. Random Forest – құрылымдалған деректермен тұрақты жұмыс істейтін, Decision Tree – түсіндіруге оңай және желілік заңдылықтарды тиімді анықтайтын классикалық модельдер ретінде таңдалды. Сонымен қатар, LSTM рекурренттік нейрондық желісі уақыттық паттерндерді талдау арқылы шабуылдарды дәл анықтауда жоғары нәтижеге қол жеткізді. Бұл тәсіл модельдердің шабуылдарды нақты анықтау қабілетін бағалауға, сондай-ақ олардың SCADA жүйесінде нақты уақыт режимінде қолданылу мүмкіндігін анықтауға мүмкіндік берді [10].

Сурет 3-те көрсетілген LSTM моделінің оқыту нәтижелері екі негізгі көрсеткіш арқылы бағаланды: оқыту және тексеру жиынындағы дәлдік (Accuracy), шығын функциясының (Loss) динамикасы. Сол жақ график LSTM моделінің дәлдігінің 97,5% деңгейіне дейін тұрақтанатынын көрсетеді, бұл модельдің тұрақты оқыту қабілетін айғақтайды. Оң жақ графикте шығынның (Loss) айтарлықтай төмендеуі көрсетілген, яғни модельдің сәтті оқытылғанын білдіреді.

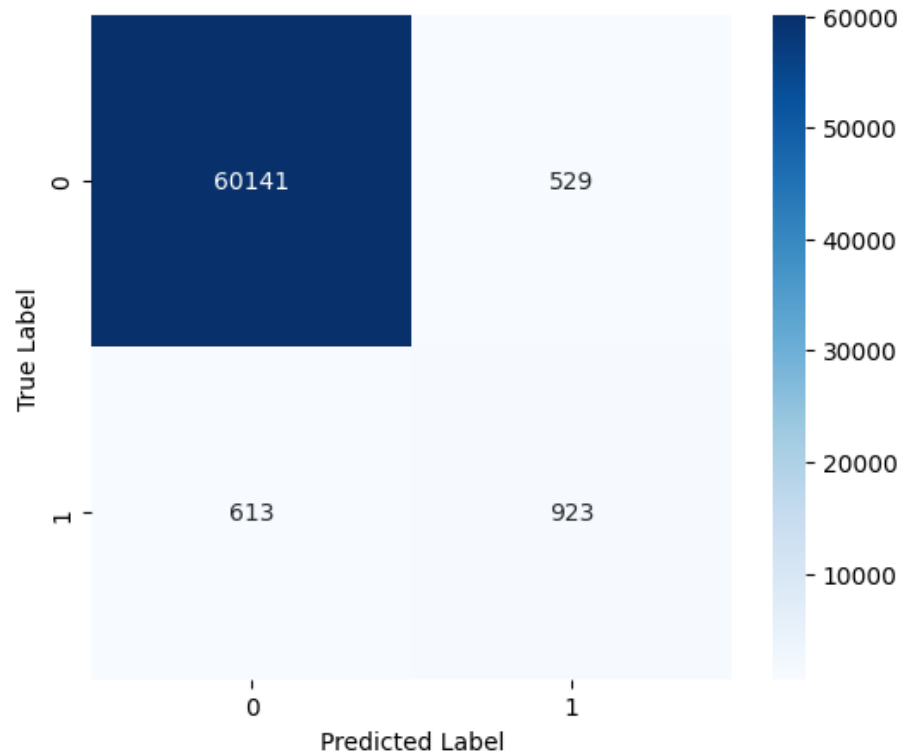


Сурет 3 – LSTM моделінің оқыту графиктері

Сурет 4 және Сурет 5-те Random Forest пен Decision Tree модельдерінің қателік матрицалары нақты сандармен бірге көрсетілген. Random Forest моделінің дәлдігі 98,16%-ды құрап, 613 шабуылды (False Negatives) қалыпты трафик деп, 529 қалыпты трафикті (False Positives) шабуыл ретінде қате анықтаған. Decision Tree моделі 98,18% дәлдікпен 526 шабуылды өткізіп жіберген және 601 жағдайда жалған іске қосылу тіркелген. Бұл нәтижелер Decision Tree-дің шабуылды анықтау қабілеті жоғары екенін көрсетсе де, жалған іске қосылу санының көптігі жүйе тұрақтылығына әсер етуі мүмкін екенін аңғартады.

Жалпы, Random Forest моделі шабуылдарды анықтауда жақсы нәтиже бергенімен, оның дәлдігін әрі қарай жақсарту маңызды. Қате классификацияларды азайту үшін

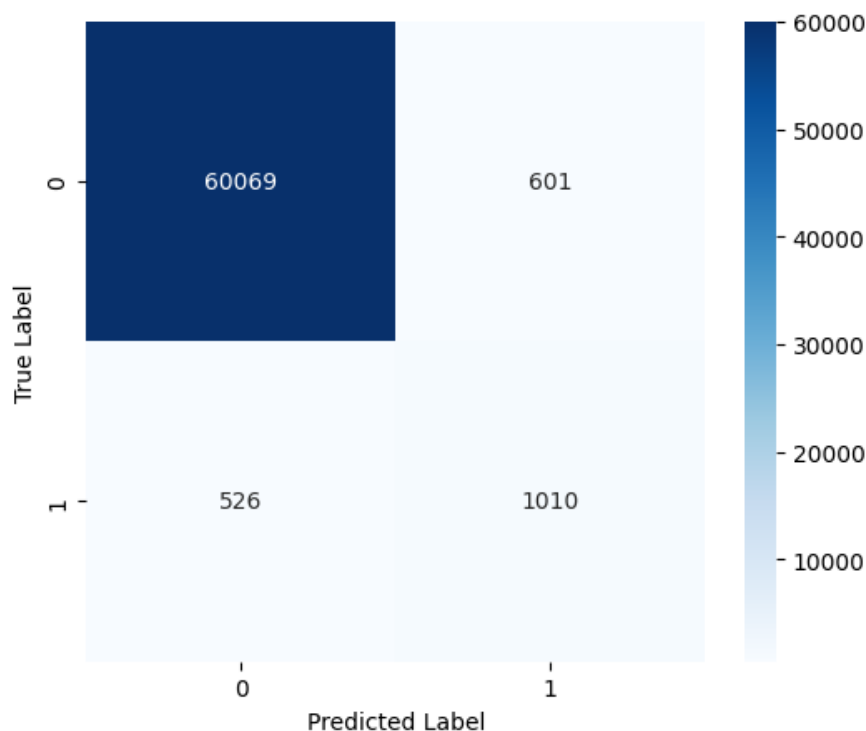
гиперпараметрлерді қосымша оңтайландыру, деректерді теңестіру немесе модельдерді ансамбльдік тәсілмен біріктіру секілді әдістерді қолдану ұсынылады. Сонымен қатар, жаңа ерекшеліктерді енгізу (feature engineering) мен басқа озық алгоритмдерді қосу модельдің сенімділігін арттыруға септігін тигізеді.



Сурет 4 – Random Forest моделінің қателік матрицасы

Әрбір матрицада нақты категориялар анық көрінеді (True Positive, True Negative, False Positive, False Negative), және бұл визуализациялар модельдердің шабуылдарды анықтаудағы нақты өнімділігін толық ашады. Гиперпараметрлерді таңдау кезінде Random Forest үшін ағаш саны – 100, максималды тереңдік – 8, ал Decision Tree үшін – максималды тереңдік пен бөліну критерийлері Grid Search арқылы таңдалды. LSTM моделінде қабат саны – 2, нейрондар саны – 64, epochs – 10, batch size – 64 етіп белгіленді.

Үлгінің репрезентативтілігін қамтамасыз ету үшін барлық негізгі шабуыл түрлері (TCP Flood, UDP Flood, SYN Flood, ICMP Flood, IP Spoofing) және қалыпты трафик тең үлесте таңдалды. Сонымен қатар, деректердегі класстар арасындағы теңгерімсіздікті жою мақсатында SMOTE әдісі қолданылды.



Сурет 5 – Decision Tree моделінің қателік матрицасы

Кесте 2-де – Random Forest және Decision Tree модельдерінің тиімділігінің салыстырмалы көрсеткіштері дәлдік (Accuracy), нақты анықтау көрсеткіші (Precision), шақыру (Recall), және F1-score бойынша толық берілген. Бұл кесте арқылы әр модельдің артықшылықтары мен әлсіз тұстары объективті салыстырылады.

Кесте 2 – Модельдер тиімділігінің салыстырмалы көрсеткіштері

Модель	Accuracy	Precision	Recall (Шабуылдарды анықтау)	F1-score
Random Forest	98.16%	63.56%	60.09%	61.78%
Decision Tree	98.18%	62.69%	65.75%	64.18%

Жүргізілген эксперименттер нәтижесінде Random Forest моделі жалпы дәлдік (accuracy) бойынша 98,16% нәтижеге жетті, Decision Tree — 98,18%. Бұл көрсеткіштер екі модельдің де шабуылды жалпы дұрыс анықтауда өте сенімді екенін көрсетеді. Random Forest үшін precision – 63,56% және recall – 60,09% деңгейінде болды. Бұл оның анықтаған шабуылдардың 63,56%-ы ғана шынайы шабуыл екенін, ал барлық шынайы шабуылдардың 60,09%-ын анықтай алғанын білдіреді. F1-score – 61,78%. Decision Tree алгоритмі бойынша precision – 62,69%, recall – 65,75% және F1-score – 64,18%. Бұл Decision Tree үлгісі жалпы шабуылды толық табуда (recall) біршама басым болғанымен, нақты анықтауда (precision) сәл артта қалады. Жалпы алғанда, барлық модельдер SCADA және өнеркәсіптік инфрақұрылымдарда DDoS-шабуылдарды автоматты және нақты анықтауға жақсы мүмкіндік береді. Бірақ қолдану саласына қарай модель таңдау кезінде дәлдік, толық табу және жалған іске қосылу көрсеткіштерін жан-жақты бағалау қажет.

Қорытынды.

Бұл зерттеуде энергетика саласындағы инфрақұрылымды кибершабуылдардан қорғау үшін заманауи машиналық оқыту және терең оқыту тәсілдерінің мүмкіндіктері жүйелі зерттелді. Зерттеу нәтижесінде жаңа гибридті модельдердің энергетикалық желілердің

қауіпсіздігін арттырудағы әлеуеті дәлелденді. Әдістемелік бөлімде ерекше көңіл модель параметрлерін дұрыс таңдауға, деректерді теңестіру мен аномалияларды анықтау алгоритмдерін жетілдіруге бөлінді. Осының нәтижесінде жүйе желілік шабуылдарды ерте кезеңде сенімді айыра алатыны анықталды.

Практикалық сынақтар барысында ұсынылған модельдер SCADA және IoT жүйелерінің киберқауіпсіздігін қамтамасыз етуде тиімді шешім ұсынатыны көрінді. Инфрақұрылымға енгізілгенде, бұл әдістер кибершабуылдардан туындайтын шығындарды азайтып, энергия жүйелерінің үздіксіз жұмысын қолдай алады. Зерттеу барысында алынған барлық модельдер нақты уақыт тәртібінде жылдамдық пен дәлдік көрсеткіштері бойынша оң нәтиже берді.

Ғылыми тұрғыдан бұл жұмыс энергетикалық инфрақұрылымды қорғау үшін тек бір ғана алгоритмге сүйену жеткіліксіз екенін, керісінше әртүрлі әдістерді үйлестіре қолдану тиімділікті арттыратынын көрсетті. Сонымен бірге, киберқауіптер үнемі эволюцияланып отырғандықтан, қорғаныс жүйелерін тұрақты түрде жетілдіріп отырудың маңызы ерекше екені айқындалды. Алдағы уақытта зерттеу бағыты энергетика саласындағы нақты өнеркәсіптік желілерде сынақ жүргізу, модельдердің икемділігін арттыру және жасанды интеллект негізінде толық автоматтандырылған шабуылға қарсы жүйелер құруға бағытталмақ. Сондай-ақ, кибершабуылдарға қарсы қорғанысты кешенді басқару үшін блокчейн, бұлттық технологиялар және Zero Trust концепциясын интеграциялау ұсынылады.

Жалпы, бұл зерттеудің нәтижелері энергетикалық жүйелердің сенімділігін қамтамасыз етуге, өндірістік желілердің қауіпсіздігін нығайтуға және саладағы болашақ инновацияларға жол ашады.

Пайдаланылған әдебиеттер тізімі

1. С.А.Адилжанова, Л. Ш. Черикбаева, М.Ж.Сақыпбекова, Г.А.Тюлепбердинова, Б.Д.Шарипова, В.А.Лахно. Концептуальное проектирование системы поддержки принятия решений для задачи распределения ресурсов стороны защиты информации на объектах информатизации// Вестник Национальной инженерной академии Республики Казахстан. 2024. № 1 (91)

2. Ismail, M. I., Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443-21456, 2022. DOI: 10.1109/ACCESS.2022.3152577

3. Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences*, 13(5993). MDPI. <https://doi.org/10.3390/app13105993>.

4. Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal*, 28, 100540. Elsevier. <https://doi.org/10.1016/j.eij.2024.100540>.

5. Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. *Data in Brief*, 54, 110461. Elsevier. <https://doi.org/10.1016/j.dib.2024.110461>.

6. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. Information and analytical system for assessing the health status of students. *KazNU Bulletin. Mathematics, Mechanics, Computer Science Series*, 2023, 118(2), p. 83–94

7. Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. *International Journal of Science and Research Archive*, 13(01), 3417-3435. <https://doi.org/10.30574/ijsra.2024.13.1.1975>.

8. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810-146822, 2021. DOI: 10.1109/ACCESS.2021.3123791.

9. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskiy, V., Desiatko, A. Adaptive Monitoring of Companies' Information Security. *International Journal of Electronics and Telecommunications*, 2023, 69(1), p. 75–82

10. Aljuhani, A. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236-42252, 2021. DOI: 10.1109/ACCESS.2021.3062909.

References

1. S.A. Adilzhanova, L.Sh. Cherikeyeva, M.Zh. Sakypbekova, G.A. Tulepberdinova, B.D. Sharipova, V.A. Lakhno. Conceptual Design of a Decision Support System for the Task of Allocating Defense Resources in Information Security Objects // *Bulletin of the National Engineering Academy of the Republic of Kazakhstan*. 2024. No. 1 (91).

2. Ismail, M. I., Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443-21456, 2022. DOI: 10.1109/ACCESS.2022.3152577

3. Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences*, 13(5993). MDPI. <https://doi.org/10.3390/app13105993>.

4. Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal*, 28, 100540. Elsevier. <https://doi.org/10.1016/j.eij.2024.100540>.

5. Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. *Data in Brief*, 54, 110461. Elsevier. <https://doi.org/10.1016/j.dib.2024.110461>.

6. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. Information and analytical system for assessing the health status of students. *KazNU Bulletin. Mathematics, Mechanics, Computer Science Series*, 2023, 118(2), p. 83–94

7. Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. *International Journal of Science and Research Archive*, 13(01), 3417-3435. <https://doi.org/10.30574/ijrsra.2024.13.1.1975>.

8. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810-146822, 2021. DOI: 10.1109/ACCESS.2021.3123791.

9. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskiy, V., Desiatko, A. Adaptive Monitoring of Companies' Information Security. *International Journal of Electronics and Telecommunications*, 2023, 69(1), p. 75–82

10. Aljuhani, A. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236-42252, 2021. DOI: 10.1109/ACCESS.2021.3062909.

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ DDOS-АТАК С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Аннотация. Цифровизация энергетической инфраструктуры становится неотъемлемой частью ее функционирования, одновременно повышая уязвимость перед киберугрозами, в частности распределёнными атаками отказа в обслуживании (DDoS).

Эти атаки нарушают стабильную работу SCADA-систем, устройств Интернета вещей (IoT) и интеллектуальных энергетических сетей, создавая серьёзные риски для критически важной инфраструктуры. В статье рассматриваются современные методы выявления и предотвращения DDoS-атак на энергетические объекты с применением алгоритмов машинного обучения. Анализируются классические модели (Random Forest, Decision Tree, Gradient Boosting, SVM), архитектуры глубинного обучения (CNN, LSTM), а также их гибридные комбинации (LSTM-CNN). Эффективность моделей оценивалась с использованием эталонных наборов данных (CICDDoS2019, KDD-CUP) и тестировалась в модельной среде SCADA. Основное внимание уделяется разработке адаптивной интеллектуальной системы защиты, способной в режиме реального времени выявлять аномалии в сетевом трафике энергетических объектов. Результаты показали, что гибридные модели достигают точности распознавания до 99% в ряде сценариев. Дополнительно рассматриваются перспективы интеграции технологий блокчейна и облачных вычислений для повышения устойчивости и масштабируемости систем кибербезопасности. Полученные выводы имеют прикладное значение при проектировании комплексных решений по защите цифровой энергетической инфраструктуры.

Ключевые слова: Кибербезопасность, DDoS-атаки, энергетические объекты, SCADA, IoT, машинное обучение, глубокое обучение, гибридные модели, блокчейн, интеллектуальные сети.

DEVELOPMENT OF A DDOS ATTACK PROTECTION SYSTEM FOR ENERGY FACILITIES USING MACHINE LEARNING METHODS

Abstract. The digitalization of energy infrastructure has become an integral component of modern operation, concurrently increasing exposure to cyber threats—particularly distributed denial-of-service (DDoS) attacks. These attacks disrupt the normal functioning of SCADA systems, IoT devices, and intelligent power grids, thereby posing significant risks to critical infrastructure. This study investigates contemporary approaches to detecting and mitigating DDoS attacks targeting energy systems through the application of machine learning techniques. A range of models is examined, including classical algorithms (Random Forest, Decision Tree, Gradient Boosting, SVM), deep learning architectures (CNN, LSTM), and hybrid models (LSTM-CNN). Model performance was evaluated using benchmark datasets (CICDDoS2019, KDD-CUP) and validated in a simulated SCADA environment. Emphasis is placed on developing an adaptive and intelligent protection framework capable of real-time anomaly detection within energy network traffic. The findings indicate that hybrid models can achieve detection accuracies of up to 99% under certain scenarios. Furthermore, the study explores the potential of integrating blockchain and cloud-based technologies to enhance the robustness and scalability of cybersecurity solutions. These outcomes provide practical guidance for designing comprehensive defense mechanisms in digitalized energy systems.

Keywords: Cybersecurity, DDoS attacks, energy facilities, SCADA, IoT, machine learning, deep learning, hybrid models, blockchain, intelligent networks.

Авторлар туралы мәлімет

Адилжанова Салтанат Альмуханбетовна	PhD, доцент м.а., әл-Фараби атындағы Қазақ ұлттық университеті, Киберқауіпсіздік және криптология кафедрасы, Скопус ID: 57194443737, orcid : https://orcid.org/0000-0003-1768-064X , Алматы қ., Қазақстан E-mail: asaltanat81@gmail.com
Ыбрайымбай Бағжан Қанатұлы	Магистрант, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан E-mail: baxa.nusipov01@mail.ru
Черикбаева Ляйля Шариповна	PhD, доцент, әл-Фараби атындағы Қазақ ұлттық университеті, Компьютерлік ғылымдар кафедрасы, Скопус ID: 57200073690, orcid : https://orcid.org/0000-0001-8948-4205 , Алматы қ., Қазақстан E-mail: cherikbayeva.lyailya@gmail.com

Сведения об авторах

Адилжанова Салтанат Альмуханбетовна	PhD, доцент (и.о.), Казахский национальный университет имени аль-Фараби, кафедра кибербезопасности и криптологии, Scopus ID: 57194443737, ORCID: 0000-0003-1768-064X, г. Алматы, Казахстан
Ыбрайымбай Бағжан Қанатұлы	Магистрант, Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан, E-mail: baxa.nusipov01@mail.ru
Черикбаева Ляйля Шариповна	PhD, доцент, Казахский национальный университет имени аль-Фараби, кафедра компьютерных наук, Scopus ID: 57200073690, ORCID: 0000-0001-8948-4205 , г. Алматы, Казахстан, E-mail: cherikbayeva.lyailya@gmail.com

Information about the authors

Adilzhanova Saltanat	PhD, Associate Professor (Acting), Al-Farabi Kazakh National University, Department of Cybersecurity and Cryptology, Scopus ID: 57194443737, ORCID: 0000-0003-1768-064X , Almaty, Kazakhstan, E-mail: asaltanat81@gmail.com
Ybraiymbay Bagzhan	Master's student, Al-Farabi Kazakh National University, Almaty, Kazakhstan E-mail: baxa.nusipov01@mail.ru
Cherikbayeva lyailya	PhD, Associate Professor, Al-Farabi Kazakh National University, Department of Computer Science, Scopus ID: 57200073690, ORCID: 0000-0001-8948-4205 , Almaty, Kazakhstan, E-mail: cherikbayeva.lyailya@gmail.com



UDC 004.738.5

IRSTI 28.23.29

https://doi.org/10.53364/24138614_2025_38_3_14

Zh. B. Lamasheva¹, U.T. Makhazhanova¹, A.B. Kassekeyeva¹, Y.K. Iskakov^{1*}

¹L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

*E-mail: thisyera@gmail.com

MULTINOMIAL NAIVE BAYES FOR KAZAKH LANGUAGE SPAM DETECTION: A CASE STUDY WITH MORPHOLOGICAL ANALYSIS

Abstract. *The growing number of spam messages in digital communication highlights the urgent need for effective spam detection systems, particularly for languages that lack sufficient digital resources, such as Kazakh. This research aims to develop a machine learning-based approach tailored for spam detection in Kazakh messages, utilizing various text preprocessing techniques and methods to enhance model performance.*

The primary objective of this study is to evaluate the effectiveness of the Multinomial Naive Bayes algorithm in classifying spam and non-spam messages within a dataset composed of 200 manually labeled samples. The methodology involves several essential steps, including data collection, preprocessing to clean and normalize the text, and feature extraction to transform the messages into a suitable format for analysis.

The findings reveal that the proposed model achieves an impressive accuracy rate of 95%, demonstrating its potential for effective spam detection in the Kazakh language. This work significantly contributes to addressing the existing gap in spam detection resources specifically designed for the Kazakh-speaking community. The practical implications of the results are considerable, as they can inform the development of more sophisticated spam filtering systems, thereby enhancing user experience and security in digital communications. Moreover, theoretical significance lies in its contribution to the fields of natural language processing and machine learning, encouraging further research and development of algorithms and techniques applicable to underrepresented languages. The study outlines text processing steps to enhance spam detection accuracy in Kazakh messages improving machine learning models' ability to identify patterns.

Keywords: *spam detection, TF-IDF, Multinomial Naive Bayes, kazakh language, spam prediction, machine learning.*

Introduction.

In the digital century the spread of spam messages across communication and on social platforms has become a major challenge. Hackers, intruders and advertisers use these platforms to profit, by many tools and schemes. Spam is defined as an unwanted message or SMS sent on mobile phones, and platforms, often containing malicious, irrelevant content [1]. Spam messages come in different types, each with various characteristics and purposes. One common type is phishing spam, which attempts to trick users into sharing personal information, to steal personal data. Promotional spam includes over-the-top marketing messages that overwhelm recipients with advertisements. Another type is fraudulent spam, where scammers promise financial gain to trick recipients into providing money or bank details. Additionally, malware spam contains malicious links or attachments that infect devices with viruses or spyware. [2]. As usage and continuing to

gain traction in online services, the need for filtering unwanted Internet resource is an urgent problem [3], in our case spam detection system adapted for Kazakh text is becoming increasingly evident.

Kazakh language speakers are estimated to be over 13 million, and they are growing annually [4]. Also, demand for internet resources is fueled by the growing number of Kazakh speakers engaging in digital interactions, especially on social media and messaging applications. Despite the importance of spam detection, existing models are primarily focused on most popular languages such as English, German Russian etc. [5]. This creates a notable gap in resources available for the Kazakh language.

Numerous studies have demonstrated the effectiveness of various algorithms, especially in languages rich in linguistic resources. Although machine learning techniques surpass manual review in spam detection, distinguishing fake from real reviews remains challenging due to limited distinguishing features, as noted by [6]. For example, algorithms such as Naive Bayes, Support Vector Machines (SVM), and Deep Learning models have been widely used for spam classification tasks, consistently yielding promising results in terms of accuracy and precision, as highlighted in several research papers [7]. The increasing prevalence of spam emails poses significant challenges that require the development of effective spam detection systems. Researchers have explored various machine learning techniques, showing that methods such as Logistic Regression and Naive Bayes can achieve impressive accuracy levels of up to 99% [7-8].

Additionally, the integration of natural language processing techniques has proven useful in improving the effectiveness of spam detection [9]. These advances suggest that combining different algorithms or filtering methods can lead to more intelligent spam detection classifiers, ultimately improving user experience and security in email communication.

There are a lot of related works across the that apply machine learning methods in spam and fishing detection. Spam detection is a classification problem in which machine learning models are trained to distinguish between legitimate messages, called not-spam and unwanted messages, known as spam [10]. This involves using various features from the text to help the models recognize patterns that define each category.

The theoretical basis for spam detection is rooted in natural language processing (NLP) and machine learning algorithms. These methodologies analyze various text features, such as word frequency, syntax, and semantics, to identify patterns that can effectively distinguish spam from unwanted messages [11]. A common approach in this area is supervised learning, in which models are trained using labeled data sets that contain both spam and non-spam examples, allowing meaningful insights to be extracted from the data.

In particular, the work mentioned in [12] highlights the KazNLP initiative, which focuses on developing tools specifically for processing the Kazakh language. This project includes critical features such as text normalization and tokenization, which are important steps in building a robust spam detection system. Despite these advances, the tools developed in KazNLP still require further improvement to improve their performance in spam detection tasks.

Various machine learning algorithms have demonstrated effectiveness in spam detection in multiple languages. In [6], the authors evaluated several email spam detection algorithms and found that both Naive Bayes and Logistic Regression achieved accuracy levels of up to 99%. This finding highlights the robustness and stability of traditional classifiers in solving spam detection tasks. Similarly, a study cited in [10] investigated spam detection using different classifiers, showing that the multinomial naive Bayes method was the most effective, although it faced limitations arising from its class independence assumptions.

Further study cited in [9] evaluated several machine learning methods for spam detection and found that random forest and support vector machine achieved 96.67% and 97.33% accuracy, respectively, when using Count Vectorizer and TF-IDF methods for feature extraction. In studies focusing on other languages, works cited in [7] and [13] examined the performance of naive Bayes networks, convolutional neural networks, SVMs, and long short-term memory (LSTM) networks

for spam detection. In particular, LSTM demonstrated the highest accuracy among the models tested, illustrating the applicability of deep learning approaches to spam classification problems.

Moreover, the authors of [8] proposed improvements to naive Bayes classifiers aimed at improving the accuracy of high-precision spam detection, in particular to address the persistent problem of false positives that continues to challenge spam filtering systems. The results of the study mentioned in [14] concluded that the Multinomial Naive Bayes algorithm outperformed the Bernoulli Naive Bayes algorithm, albeit with a small difference in accuracy of 73% on a small dataset of 312 records. However, both algorithms showed limited performance due to the limitations imposed by the dataset size, highlighting the importance of using larger and more comprehensive datasets for training spam detection models.

The aim of this article is to address this gap by developing a machine learning-based spam detection model that is tailored for Kazakh text messages. Using text preprocessing techniques, we will examine how effective Multinomial Naive Bayes machine algorithm is at classifying messages as spam or non-spam based on our dataset. We labeled messages in dataset into spam and not-spam, which indicates our email message if relevant 0, if not then 1.

Materials and methods.

We identified several key challenges addressed in previous studies: reducing false positives to improve accuracy, developing and improving model accuracy using larger and diverse datasets. These goals highlight the need for complex machine learning methods and algorithms and the importance of language resources to achieve high accuracy in spam detection tasks.

So, Naive Bayes was selected for this study a high accuracy in spam filtering tasks, second only to more complex deep learning-based models, but requires fewer computational resources and is easier to interpret.

Its effectiveness in processing Kazakh text is further justified by the fact that this algorithm works well even with a limited amount of training data, which is a pressing issue for resource-constrained languages such as Kazakh.

The methodological framework outlines the steps required to apply a machine learning approach to identify spam messages in the Kazakh language. The process begins with data collection, where spam and legitimate messages in the Kazakh language are gathered from sources. Following this, preprocessing is carried out to clean and format the data, addressing issues such as noise removal and text normalization to enhance the quality of the input [12]. The next step involves TF-IDF vectorization, feature extraction technique that converts the textual data into numerical representations, making it compatible with machine learning algorithms [15]. Once the features are extracted, model training occurs, where machine learning algorithm, including Naive Bayes, is trained on the dataset to learn the characteristics of spam messages. This process is followed by model evaluation, where the trained models are assessed for their accuracy and performance using metrics like precision, recall, and F1-score. Finally, the results will be presented, illustrating the effectiveness of the proposed approach in accurately detecting spam messages in Kazakh (see Fig. 1). This systematic methodology provides a thorough spam detection in specific languages. We would like to engage in more in-depth regarding the methodology and findings related to steps.

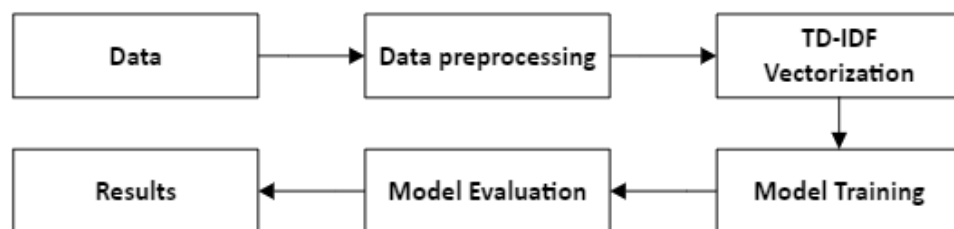


Figure 1 – Flow Chart of methodology

Note – compiled by the authors based on work [13]

The effectiveness of any machine learning model heavily relies on the quality and representativeness of the dataset used for training and testing [16]. For this research, we meticulously collected a dataset consisting of user-generated content in the Kazakh language from SMS, social media and emails. This dataset comprised a total of 200 instances, which were manually labeled into two categories: spam and non-spam (ham).

The data was sourced from various platforms, including social media, messaging applications where language speakers interact. We also ensured that the dataset captured a diverse array of spam types, including phishing attempts, advertisement spam, and irrelevant content, alongside legitimate messages (see Fig. 2).

label	message
0	Біздің жаңа жобамызды қараңыз.
0	Кітап жазу бойынша жиналысқа қатысыңыз.
0	Сәлем, досым, қалайсың!
0	Сенбі күні футбол ойыны болады.
0	Бүгін ауа райы өте керемет.
...	...
0	Сіздің сараптамалық нәтижелеріңіз шықты алып к...
1	Өзіңді таппай дал болсан, біздің тестті өт
0	Ертең іс-шарада белгілі шетелдік меймандар болады
0	Кешікпей кел, мен саған сенемін
0	Сағат 17 00 де кездесу болатынын ұмытпаңыз!

Figure 2 – Dataset representation

We can see the distribution of spam and non-spam messages across the dataset in figure 3, where categories are distributed almost equally.

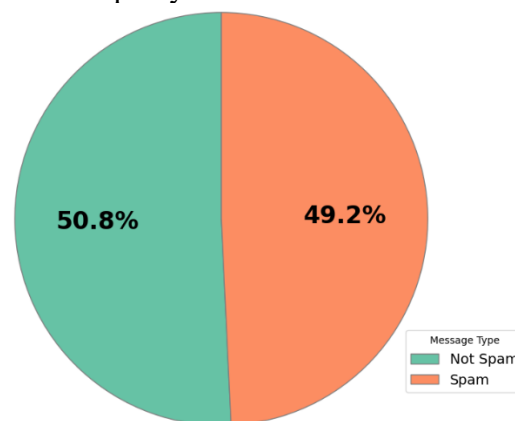


Figure 3 – Distribution of spam and non-spam messages

Data preprocessing is the process of modifying a dataset to improve its utility during model development by minimizing the impact of less important features [15]. The main goal of text preprocessing is to standardize each message into a uniform format using various transformation techniques, thereby ensuring that the data is clean, relevant, and ready for effective analysis in machine learning models.

Data preprocessing includes tokenization, stopwords removal, stemming, ensuring the text is clean and transformed for effective analysis [7] (see Fig. 4).

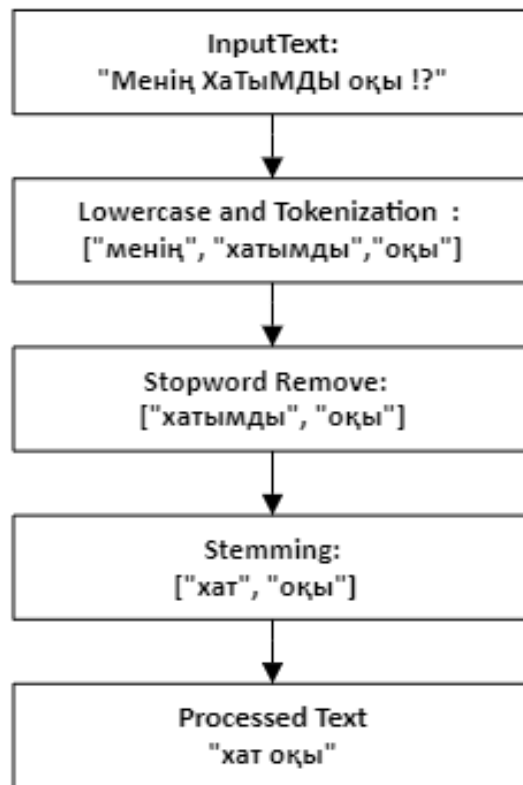


Figure 4 – Data preprocessing steps

Note – compiled by the authors based on work [3]

For each message, the first step is to convert each word in the message to lowercase. This transformation can be formally defined as a mapping where each word is transformed into its lowercase version.

Next, the lowercased string is split into a sequence of words or tokens. This process converts the string into a list of alphanumeric tokens.

Stopwords are commonly used words in a language, such as conjunctions, prepositions, and pronouns, that are often filtered out in natural language processing tasks because they carry minimal meaning and do not significantly contribute to the content of the text.

Connectives and Conjunctions: (және (and), бірақ (but), сонымен (also) etc.)

Pronouns: (мен (I), сен (you), біз (we) etc.)

Articles: (бұл (this), сол (that), әр (each), барлық (all), кейбір (some) etc.)

Prepositions: (үшін (for), арқылы (through), дейін (until) etc.)

Adverbs: (жиі (often), әрқашан (always), тез (quickly), баяу (slowly) etc.)

Miscellaneous: (жоқ (not), әр (every), тағы (again), осы (this), онда (then) etc.)

After tokenization, we remove stopwords from the token set, se identified these words above.

Before starting steaming step let's consider structure of the words in the Kazakh language by its features. Morphology is a branch of linguistics that studies the structure of words, including affixes and parts of speech [17]. Words can be categorized into two main types based on their structure: simple and compound words.

Simple words are made up of a single root.

Compound words consist of at least two roots and convey a single meaning.

According to morphology, each word consists of parts: root, suffix, and ending.

Root: The most basic, indivisible part of a word («хат»).

Suffix: An affix that creates new words or modifies the form of a word («хатшы»).

Ending: A grammatical form that connects the word it is attached to with another word, establishing a relationship between them («хатшыларға»).

In the Kazakh language, there are types of endings:

Plural endings: (-лар/лер, -дар/дер, -тар/тер, etc.), which indicate a plural meaning for the words they are attached to.

Possessive endings: Grammatical categories that express ownership by one of three persons (-ым/ім, -ның/дің, -ікі/дікі/тікі, etc.).

Case endings: Affixes that link words to one another, facilitating their relationship and interaction. They include: (-ның/нің, -дың/дің, -тың/тің, -ға/ге, -қа/ке, -на/не, -а/е, -ны/ні, -ды/ді, -ты/ті, -н, -да/де, -та/те, -нда/нде, -нан/нен, -дан/ден, -тан/тен, -мен, -бен, -пен, -менен, -пенен, -бенен).

Stemming is the process of reducing words to their root form (or stem) to normalize inflected words. The stemming function maps a word to its stemmed version, representing the preprocessed message.

At the end, the preprocessing pipeline for any message $x_i \in X$ can be expressed as the composition of above steps. The final transformation $x_i' = \text{stemming}(\text{tokenization}(\text{lowercase}(x_i)) - \text{stopwords})$, representing the preprocessed version of x_i , is given by: x_i'

After preprocessing the text, we extracted features using the Term Frequency-Inverse Document Frequency vectorizer. It is a statistical measure used to evaluate the importance of a word in a document relative to a collection of documents. This technique assigns greater weight to terms that are frequent in a document but rare across other documents, effectively reducing the influence of common words that do not add meaningful information for classification. The formula for calculating TF-IDF for each word t in document d is shown as in formula 1.

$$TD - IDF(t, d) = TF(t, d) \times \log\left(\frac{N}{DF(t)}\right) \quad (1)$$

where:

$TF(t, d)$ – is the term of word t in document d ;

N – is the total number of documents in the corpus;

$DF(t)$ – is the document frequency, which represents the number of documents in which term t appears.

By using TF-IDF, each document in the corpus is converted into a numerical vector that highlights the significance of each word. This vector representation enhances the model's ability to differentiate between spam and non-spam messages effectively [15].

The Multinomial Naive Bayes (MNB) method was chosen for this analysis due to its effectiveness in handling categorical data and its strong theoretical foundation in probabilistic classification. In applications such as spam detection, this algorithm is effective when processing discrete features, which represent word frequencies in messages. By assuming feature independence (i.e., each word or feature contributes independently to the classification result), MNB simplifies the calculations, making it computationally efficient while maintaining its effectiveness in classification problems [18]. Additionally, previous studies have highlighted its strong performance in spam detection tasks across various languages, reinforcing its applicability to Kazakh text messages.

To detect spam, MNB calculates the probability that a given message belongs to a certain class “spam” or “not spam” based on the occurrence and frequency of words in the text. The model

calculates the posterior probability $P(C | X)$ of a class C (spam or not-spam) given a feature set X (words). The equation is shown in formula 2.

$$P(C | X) = \frac{P(c) \prod_{i=1}^n P(x_i | C)}{P(X)} \quad (2)$$

where:

$P(C)$ – is the prior probability of the class;

$P(x_i | C)$ – is the likelihood of word x_i occurring in class C ;

$P(X)$ – is the evidence.

In spam detection tasks, Multinomial Naive Bayes algorithm works effectively because spam messages tend to use distinctive words or phrases. The algorithm learns these patterns from the training data, making it adept at identifying new messages like spam such as “free”, “offer”, “click here” or non-spam based on word frequencies and the calculated probabilities for each class [19].

The dataset was divided into an 80/20 ratio for training and testing, respectively, to evaluate the performance of the spam detection model. Subsequently, the model was evaluated on the unseen test set to gauge its performance. Several metrics were employed for this evaluation, including accuracy, precision, recall, and F1-score.

Results and Discussion.

The spam detection was evaluated using a dataset consisting of 200 messages, where 20% of data is tested, 21 of which were labeled as not spam and 19 of which were labeled as spam. The performance of the system is shown in Table 1, which presents the precision, recall, F1 score, and support (see Table 1).

For the non-spam, the model achieved a precision of 0.9524, meaning that 95% of the messages predicted as not spam were indeed non-spam. The recall for non-spam was 0.9524, indicating that the model correctly identified 95% of all actual non-spam messages. The F1 score, which combines precision and recall, was 0.9524 for non-spam. For spam, the model performed with a precision of 0.9474, meaning that messages predicted as spam were closely correctly classified. The recall for spam was 0.9474, showing that most of all actual spam messages were correctly identified. The F1 score for spam was 0.9474.

The overall accuracy of the system, which reflects the percentage of correctly classified messages, was 95%.

Table 1 - Classification Report of the program

	precision	recall	F1-score	support
non-spam	0.9524	0.9524	0.9524	21
spam	0.9474	0.9474	0.9474	19
accuracy			0.9500	40

Overall, the model demonstrated an accuracy of 95%, reflecting the percentage of correctly classified messages. These results highlight the efficacy of the spam detection model for Kazakh language texts based on the Multinomial Naive Bayes algorithm, showcasing high precision and recall in both spam and non-spam categories.

The TF-IDF analysis highlight the most influential words in the dataset, with "сіз" (you) having the highest importance. Other top-ranked words such as "туралы" (about) and "тегін" (free) indicate a focus on informational and promotional content, which is relevant for spam classification (see fig. 5).

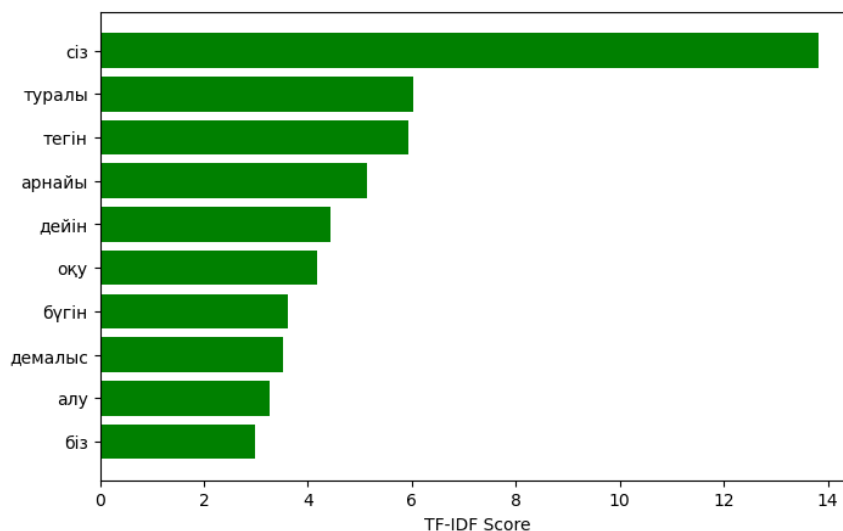


Figure 5 – Significant terms ranked by their TF-IDF scores

In comparison to existing literature, our results align closely with findings from [6] and [10], which also reported high accuracy rates using similar algorithms. However, our model's performance is particularly significant given the limited resources and datasets available for the Kazakh language.

In contrast to [7] findings, which reported varying results across algorithms, our model consistently performed with high precision and recall metrics. The comparative studies by [14], [19] work also emphasized the efficiency of Multinomial Naive Bayes, which aligns with our results, reinforcing the model's applicability for Kazakh language spam detection.

Despite the outstanding performance of the model, some challenges and limitations emerged during its implementation. The complexity of preprocessing the language, given its rich morphology and syntax, presented obstacles. Although the main preprocessing methods used for this purpose yielded good performance, they did not fully capture the subtleties of grammatical structures. In addition, the relatively small dataset limited the model's ability to generalize across contexts. This suggests the need for more comprehensive linguistic preprocessing, with lemmatization or word embedding steps, to better capture semantic nuances. An alternative approach could involve more advanced machine learning techniques, such as deep learning models or transformer-based models which could enhance contextual understanding.

Furthermore, the relatively small dataset limited the model's ability to generalize across varied contexts. This suggests the need for more comprehensive linguistic preprocessing, such as lemmatization or word embeddings, to better capture the semantic nuances. Future research should focus on advanced machine learning techniques. Additionally, expanding the dataset with more diverse text sources would strengthen the model's robustness and improve its classification accuracy in detecting spam within the Kazakh language.

Although the data preprocessing steps are well-detailed, the explanation of model selection can be further improved by discussing its limitations and alternative approaches. One notable limitation of MNB is its assumption of feature independence, which may not always hold in real-world data. This assumption can sometimes lead to suboptimal performance when features are strongly correlated. Additionally, MNB relies on sufficient training data to estimate reliable probabilities, and it can struggle when dealing with rare features or unseen words, which can be mitigated using Laplace or other forms of smoothing.

Alternative classification methods, such as logistic regression or support vector machines, could also be considered. While these models do not rely on the naive independence assumption, they may require more computational resources and hyperparameter tuning. Furthermore, deep learning approaches, such as recurrent neural networks (RNNs) or transformers, could improve

performance in complex text classification tasks but at the cost of increased training time and model interpretability.

Conclusion.

Effective spam filtering is critical not only for user experience but also to protect against potential security risks associated with malicious content. This research contributes to addressing the existing gap in spam detection resources specifically designed for the Kazakh language, which has been largely ignored in the field of natural language processing.

In this study, text preprocessing methods, combined with a Multinomial Naive Bayes algorithm, provided a reliable framework for distinguishing between spam and non-spam messages in a dataset of manually labeled texts. The model's performance yielded an impressive 95% accuracy, demonstrating the potential for automated spam detection in Kazakh. The accuracy rate indicates the efficacy of this method for distinguishing unwanted content in this language context.

Despite promising results, challenges remain due to the syntax, morphology and complex grammatical structures of the Kazakh language. Basic preprocessing methods did not fully capture the intricacies of Kazakh syntax and semantics.

The theoretical novelty of this research lies in the application of MNB in the given context and its adaptation to the specific characteristics of the dataset. The study explores how prior distributions influence classification performance and evaluates the impact of different feature engineering techniques on the model's accuracy. By refining preprocessing methods and optimizing model parameters, this research contributes to improving the applicability of Bayesian classification in high-dimensional data scenarios. Additionally, the practical significance of this study lies in its potential to enhance text classification methodologies, offering an efficient and interpretable approach for categorizing textual information with probabilistic reasoning.

Future work in this domain should prioritize the integration of advanced preprocessing techniques and sophisticated machine learning models that can better accommodate these linguistic complexities. Potential solutions could include the use of deep learning methods, which excel at capturing nuanced language patterns and other promising models that covered in review.

References

1. Dharani, V., Hegde, D., & Mohana. (2023). Spam SMS (or) email detection and classification using machine learning. 5th International Conference on Smart Systems and Inventive Technology, 1104-1108. <https://doi.org/10.1109/ICSSIT55814.2023.10060908>
2. Sulthana, R., Verma, A., & Jaithunbi, A. K. (2023). A detailed analysis on spam emails and detection using machine learning algorithms. *Inventive Systems and Control, Lecture Notes in Networks and Systems*, 672, 65–76. https://doi.org/10.1007/978-981-99-1624-5_5
3. Mussiraliyeva, S., Omarov, B., Bolatbek, M., Bagitova, K., & Alimzhanova, Z. (2021). Bigram-based deep neural network for extremism detection in online user-generated contents in the Kazakh language. *Advances in Computational Collective Intelligence, Communications in Computer and Information Science*, 1463, 559-570. https://doi.org/10.1007/978-3-030-88113-9_45
4. Kuderinova, K. (2024). Kazakh public speech: Language norm, ethics of speech, and speech structure. *Vestnik KazNU. Series: Philological*, 193(1), 65-76. <https://doi.org/10.26577/EJPh.2024.v193.i1.ph6>
5. Ermakova, L. (2010). Obrabotka teksta i kognitivnye tekhnologii: Kognitivnoe modelirovanie v lingvistike [Text processing and cognitive technologies: Cognitive modeling in linguistics]. XII Mezhdunarodnaya nauchnaya konferenciya, 189-193.
6. Kontsewaya, Y., Antonov, E., & Artamonov, A. (2021). Evaluating the effectiveness of machine learning methods for spam detection. *Procedia Computer Science*, 190, 479–486. <https://doi.org/10.1016/j.procs.2021.06.056>

7. Cota, R. P., & Zinca, D. (2022). Comparative results of spam email detection using machine learning algorithms. 14th International Conference on Communications (COMM), 1-5. <https://doi.org/10.1109/COMM54429.2022.9817305>
8. Song, Y., Kołcz, A., & Giles, C. L. (2009). Better naive Bayes classification for high-precision spam detection. *Software Practice and Experience*, 39(11), 1003–1024. <https://doi.org/10.1002/spe.925>
9. Negi, H. S., Bhatt, A., & Rawat, V. (2024). Spam mail detection: Various machine learning methods and their comparisons. In *Algorithms: Big Data, Optimization Techniques, Cyber Security* (pp. 119-136). De Gruyter. <https://doi.org/10.1515/978311229157-007>
10. Kumar, N., Sonowal, S., & Nishant. (2020). Email spam detection using machine learning algorithms. 2020 Second International Conference on Inventive Research in Computing Applications, 108-113. <https://doi.org/10.1109/ICIRCA48905.2020.9183098>
11. Kadam, S., Gala, A., Gehlot, P., Kurup, A., & Ghag, K. (2018). Word embedding-based multinomial naive Bayes algorithm for spam filtering. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 1-5. <https://doi.org/10.1109/iccubea.2018.8697601>
12. Yessenbayev, Z., Kozhirbayev, Z., & Makazhanov, A. (2020). KazNLP: A pipeline for automated processing of texts written in Kazakh language. In *Speech and Computer. SPECOM 2020. Lecture Notes in Computer Science* (Vol. 12335, pp. 657-666). https://doi.org/10.1007/978-3-030-60276-5_63
13. Siddique, Z. B., Khan, M. A., Din, I. U., Almogren, A., Mohiuddin, I., & Nazir, S. (2021). Machine learning-based detection of spam emails. *Scientific Programming*, 1–11. <https://doi.org/10.1155/2021/6508784>
14. Singh, G., Kumar, B., Gaur, L., & Tyagi, A. (2019). Comparison between multinomial and Bernoulli naïve Bayes for text classification. 2019 International Conference on Automation, Computational and Technology Management (ICACTM), 593-596. <https://doi.org/10.1109/ICACTM.2019.8776800>
15. Shahzad, Q., & Ali, R. (2018). Text mining: Use of TF-IDF to examine the relevance of words to documents. *International Journal of Computer Applications*, 181(1), 25-29. <https://doi.org/10.5120/ijca2018917395>
16. Vijay, V., & Verma, P. (2023). Variants of naïve Bayes algorithm for hate speech detection in text documents. *International Conference on Artificial Intelligence and Smart Communication (AISC)*, 18-21. <https://doi.org/10.1109/AISC56616.2023.10085511>
17. Kessikbayeva, G., & Cicekli, I. (2016). A rule-based morphological analyzer and a morphological disambiguator for Kazakh language. *Linguistics and Literature Studies*, 4(1), 96–104. <https://doi.org/10.13189/lis.2016.040111>
18. Sabiq, F. F., Rahmatulloh, A., Darmawan, I., Rizal, R., Gunawan, R., & Haeran, E. (2024). Performance comparison of multinomial and Bernoulli naïve Bayes algorithms with Laplace smoothing optimization in fake news classification. *International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD)*, 19-24. <https://doi.org/10.1109/icoabcd63526.2024.10704399>
19. Octaviani, N. L., Rachmawanto, E. H., Sari, C. A., & De Rosal, I. M. S. (2020). Comparison of multinomial naïve Bayes classifier, support vector machine, and recurrent neural network to classify email spams. 2020 International Seminar on Application for Technology of Information and Communication, 17-21. <https://doi.org/10.1109/iSemantic50169.2020.9234296>

ҚАЗАҚ ТІЛІНДЕ СПАМДЫ АНЫҚТАУҒА АРНАЛҒАН МУЛЬТИНОМДЫҚ АҢҒАЛДЫҚ БАЙЕС ТАЛДАУЫ: МОРФОЛОГИЯЛЫҚ ТАЛДАУ МЕН ЗЕРТТЕУ

Аңдатпа. Сандық коммуникациядағы спам хабарлардың көбеюі, әсіресе жеткілікті сандық ресурстары жоқ қазақ тілі сияқты тілдер үшін тиімді спам анықтау жүйелеріне

деген шұғыл қажеттілікті көрсетеді. Бұл зерттеу қазақ тіліндегі спам хабарламаларды анықтауға арналған машиналық оқытуға негізделген әдісті әзірлеуге бағытталған, ол модель өнімділігін арттыру үшін әртүрлі мәтіндерді алдын ала өңдеу әдістерін қолданады.

Зерттеудің негізгі мақсаты – жасанды таңбаланған 200 үлгіден тұратын деректер жиынындағы спам және спам емес хабарламаларды жіктеудегі Мультиномдық Найв Байес алгоритмінің тиімділігін бағалау. Әдіснама деректерді жинау, мәтінді тазарту және қалыпқа келтіру үшін алдын ала өңдеу, сондай-ақ хабарларды талдауға қолайлы форматқа түрлендіру үшін ерекшеліктерді алу қадамдарын қамтиды.

Нәтижелер ұсынылған модельдің 95% дәлдік көрсеткішіне қол жеткізгенін көрсетеді, бұл қазақ тіліндегі спам хабарламаларды анықтаудың тиімділігі зор екендігін дәлелдейді. Бұл жұмыс қазақ тілді қауымдастыққа арнайы әзірленген спам анықтау ресурстарындағы бар олқылықтардың орнын толтыруға елеулі үлес қосады. Нәтижелердің практикалық маңызы зор, себебі олар қолданушылар тәжірибесі мен сандық коммуникациялардағы қауіпсіздікті арттыра отырып, күрделі спам сүзу жүйелерін әзірлеуге негіз бола алады. Теориялық тұрғыдан алғанда, бұл жұмыс табиғи тілді өңдеу және машиналық оқыту салаларына үлес қосып, қолдау таппаған тілдерге қолдануға болатын алгоритмдер мен әдістерді одан әрі зерттеуге және дамытуға ықпал етеді. Зерттеу қазақ тіліндегі спам хабарламаларды анықтау дәлдігін арттыру үшін мәтінді өңдеу қадамдарын ұсынады және машиналық оқыту модельдерінің үлгілерді тану қабілетін жақсартады.

Түйін сөздер: спамды анықтау, TF-IDF, Мультиномдық Найв Байес алгоритмі, қазақ тілі, спамды болжау, машиналық оқыту.

МУЛЬТИНОМИАЛЬНЫЙ НАИВНЫЙ БАЙЕСОВСКИЙ АНАЛИЗ ДЛЯ ОБНАРУЖЕНИЯ СПАМА НА КАЗАХСКОМ ЯЗЫКЕ: ИССЛЕДОВАНИЕ С МОРФОЛОГИЧЕСКИМ АНАЛИЗОМ

Аннотация. *Растущее количество спам-сообщений в цифровой коммуникации подчеркивает острую необходимость в эффективных системах обнаружения спама, особенно для языков, не имеющих достаточных цифровых ресурсов, таких как казахский. Целью данного исследования является разработка подхода на основе машинного обучения, специально предназначенного для обнаружения спама в казахских сообщениях, с использованием различных методов и приемов предварительной обработки текста для повышения производительности модели.*

Основной целью данного исследования является оценка эффективности алгоритма мультиномиального наивного байесовского анализа при классификации спам-сообщений и не спам-сообщений в наборе данных, состоящем из 200 вручную помеченных образцов. Методология включает несколько основных этапов, включая сбор данных, предварительную обработку для очистки и нормализации текста и извлечение признаков для преобразования сообщений в подходящий формат для анализа.

Результаты показывают, что предложенная модель достигает впечатляющего уровня точности в 95%, демонстрируя свой потенциал для эффективного обнаружения спама на казахском языке. Эта работа вносит значительный вклад в устранение существующего пробела в ресурсах обнаружения спама, специально разработанных для казахскоязычного сообщества. Практические последствия результатов значительны, поскольку они могут информировать о разработке более сложных систем фильтрации спама, тем самым улучшая пользовательский опыт и безопасность в цифровых коммуникациях. Более того, теоретическое значение заключается в ее вкладе в области обработки естественного языка и машинного обучения, поощряя дальнейшие исследования и разработку алгоритмов и методов, применимых к недостаточно представленным

языкам. В исследовании излагаются шаги по обработке текста для повышения точности обнаружения спама в казахских сообщениях, улучшая способность моделей машинного обучения определять закономерности.

Ключевые слова: обнаружение спама, TF-IDF, Мультиномиальный Наивный Байесовский алгоритм, казахский язык, прогнозирование спама, машинное обучение.

Авторлар туралы мәлімет

Ламашева Жанар Бейбутовна	PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің аға оқытушы, «Ақпараттық жүйелер» кафедрасы, Астана қ., Қазақстан, E-mail: lamasheva_zhb@enu.kz
Махажанова Улжан Танирбергеновна	PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің аға оқытушы, «Ақпараттық жүйелер» кафедрасы, Астана қ., Қазақстан, E-mail: makhazhan.ut@gmail.com
Касекеева Айслу Бисеновна	PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің аға оқытушы, «Ақпараттық жүйелер» кафедрасы, Астана қ., Қазақстан, E-mail: aibike-7474@yandex.kz
Искаков Ерасыл Кайратович	Л.Н. Гумилев атындағы Еуразия ұлттық университетінің 3 курс студенті, Астана қ., Қазақстан, E-mail: thisyera@gmail.com

Сведения об авторах

Ламашева Жанар Бейбутовна	PhD, ст. преп., кафедра «Информационных систем», Евразийский Национальный Университет имени Л.Н. Гумилева, г. Астана, Казахстан, E-mail: lamasheva_zhb@enu.kz
Махажанова Улжан Танирбергеновна	PhD, ст. преп., кафедра «Информационных систем», Евразийский Национальный Университет имени Л.Н. Гумилева, г. Астана, Казахстан, E-mail: makhazhan.ut@gmail.com
Касекеева Айслу Бисеновна	PhD, ст. преп., кафедра «Информационных систем», Евразийский Национальный Университет имени Л.Н. Гумилева, г. Астана, Казахстан, E-mail: aibike-7474@yandex.kz
Искаков Ерасыл Кайратович	студент 3 курса бакалавр, Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Казахстан, E-mail: thisyera@gmail.com *

Information about the authors

Lamasheva Zhanar Beibutovna	PhD, lecturer, Department of «Information systems», L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: lamasheva_zhb@enu.kz
Makhazhanova Ulzhan Tanirbergenovna	PhD, lecturer, Department of Information systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: makhazhan.ut@gmail.com
Kassekeyeva Aislu Bisenovna	PhD, lecturer, Department of Information systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: aibike-7474@yandex.kz
Iskakov Yerassyl Kairatovich	3 rd year bachelor student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: thisyera@gmail.com



УДК 621.548.5

МРНТИ 50.43

https://doi.org/10.53364/24138614_2025_38_3_15

А. Фазылова¹, К. Алипбаев¹, А. Оразалиева¹, А. Аден^{1*}

¹ Алматинский университет энергетики и связи имени Г. Даукеева, Алматы,
Республика Казахстан

*¹E-mail: a.aden@aes.kz

ТЕОРЕТИЧЕСКОЕ И ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ АЭРОДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК И МЕХАНИЧЕСКОЙ УСТОЙЧИВОСТИ РОТОРА ДАРЬЕ

***Аннотация.** В данной статье представлено теоретическое и численное моделирование ротора Дарье – одного из наиболее популярных роторов для ветровых турбин с вертикальной осью вращения. Проведены расчёты аэродинамических характеристик, включая эффективную площадь ротора, силу сопротивления, подъёмную силу, крутящий момент и мощность. Используются аналитические методы и численное моделирование в среде SolidWorks для оценки работы ротора при различных параметрах воздушного потока. Также выполнен анализ деформации конструкции при критических нагрузках, что позволило оценить её устойчивость и эффективность. Полученные результаты подтверждают способность ротора Дарье к стабильной работе в условиях высоких скоростей ветра и его высокую механическую прочность.*

***Ключевые слова:** ротор Дарье, численное моделирование, аэродинамические характеристики, ветровая турбина, деформационный анализ.*

Введение

Ветровая энергетика является одной из наиболее перспективных отраслей возобновляемых источников энергии. В последние десятилетия активное развитие технологий ветроэнергетики привело к совершенствованию конструкций роторов, повышению их эффективности и снижению эксплуатационных затрат. Особый интерес представляют роторы с вертикальной осью вращения (VAWT – Vertical Axis Wind Turbine), среди которых ротор Дарье является одним из наиболее распространённых решений. Его основные преимущества включают возможность работы при низких скоростях ветра, меньшую чувствительность к изменению направления воздушного потока и простоту конструкции.

За последние годы проведено множество исследований, посвящённых аэродинамическому моделированию ротора Дарье. Так, в работе [1] представлены результаты численного моделирования с использованием метода конечных элементов (CFD-анализ) для изучения влияния геометрии лопастей на коэффициент мощности. В исследовании [2] рассматриваются экспериментальные данные, полученные в аэродинамической трубе, и их сравнение с теоретическими моделями. В работе [3] проведён анализ устойчивости конструкции ротора Дарье при различных скоростях воздушного потока с учётом деформационных характеристик материалов.

Научная новизна данной статьи заключается в объединении теоретических методов и численного моделирования в единую методику комплексной оценки ротора Дарье,

включающей не только аэродинамические характеристики (подъёмную силу, сопротивление, крутящий момент, мощность), но и механическую устойчивость конструкции при высоких скоростях ветра. Особенностью подхода является использование трёхмерной САД-модели ротора с криволинейными лопастями в среде SolidWorks для анализа как аэродинамики, так и деформационных нагрузок.

Гипотеза исследования состоит в том, что ротор Дарье с оптимизированной геометрией лопастей способен эффективно функционировать при значительных скоростях воздушного потока, обеспечивая при этом минимальные деформации конструкции, что повышает его надёжность и устойчивость в эксплуатации. Настоящая работа направлена на проверку данной гипотезы и расширение понимания возможностей применения ротора Дарье в ветроэнергетических установках. Полученные результаты могут быть полезны при проектировании эффективных ветрогенераторов с вертикальной осью вращения, особенно в условиях повышенной ветровой нагрузки.

Материалы и методы.

В данном исследовании использованы численные и аналитические методы для моделирования аэродинамических характеристик ротора Дарье. Для расчёта основных параметров были применены следующие формулы. Эффективный радиус лопасти [4]:

$$R_{\text{эфф}} = k \cdot R \quad (1)$$

Эффективный радиус лопасти определяется с учетом геометрических характеристик ротора. Здесь — эмпирический коэффициент, учитывающий снижение площади взаимодействия с потоком воздуха (для криволинейных лопастей он составляет 0.95), R — радиус ротора. Эффективная ометаемая площадь ротора [5]:

$$A_{\text{эфф}} = 2 \cdot h \cdot R_{\text{эфф}} \quad (2)$$

Данная формула используется для определения площади, ометаемой ротором во время его вращения. Высота ротора и эффективный радиус влияют на взаимодействие с потоком воздуха, что напрямую сказывается на генерируемой мощности. Данная формула используется для определения площади, ометаемой ротором во время его вращения. Высота ротора и эффективный радиус влияют на взаимодействие с потоком воздуха, что напрямую сказывается на генерируемой мощности. Сила сопротивления определяется аэродинамическими характеристиками ротора и зависит от коэффициента сопротивления C , плотности воздуха ρ , скорости воздушного потока $V_{\text{п}}$ и эффективной площади ротора $A_{\text{эфф}}$. Эта сила действует против направления движения лопастей [6]:

$$F_a(\theta) = \frac{1}{2} \cdot C \cdot \rho \cdot A_{\text{эфф}} \cdot V_{\text{п}}^2 \quad (3)$$

Подъёмная сила возникает в результате разницы давлений на верхней и нижней поверхностях лопастей. Она рассчитывается аналогично силе сопротивления, но с использованием коэффициента подъёмной силы [7]:

$$F_n(\theta) = \frac{1}{2} C \cdot \rho \cdot A_{\text{эфф}} \cdot V_{\text{п}}^2 \quad (4)$$

Момент силы можно определить по формуле [7]:

$$T_r = 0,5 \cdot (F_a(\theta) - F_n(\theta)) \cdot R_{\text{эфф}} \quad (5)$$

Этот момент описывает крутящий эффект, создаваемый аэродинамическими силами на роторе. Разность сил сопротивления и подъёма умножается на эффективный радиус, что определяет результирующий крутящий момент. Угловая скорость ротора определяется через коэффициент скорости, который учитывает соотношение линейной скорости края лопасти к скорости воздушного потока по формуле [8]:

$$\omega = \frac{\lambda V_{\text{п}}}{R} \quad (6)$$

Мощность, производимая ротором, определяется произведением крутящего момента на угловую скорость. Это ключевой параметр, отражающий эффективность ротора в преобразовании энергии ветра в механическую [9]:

$$P = T_r \cdot \omega \quad (7)$$

Коэффициент мощности характеризует эффективность преобразования кинетической энергии ветра в механическую энергию ротора. Он рассчитывается как отношение выработанной мощности к максимальной возможной мощности воздушного потока, проходящего через площадь ротора. можно определить по формуле [10]:

$$C = \frac{P}{0.5 \cdot \rho V_n^3 A_{эфф}} \quad (8)$$

Для оценки деформации конструкции под действием нагрузки была использована формула [11]:

$$\Delta L = \frac{FL}{AE} \quad (9)$$

Здесь, F — приложенная сила, L — длина ротора, A — площадь поперечного сечения, E — модуль Юнга материала, который характеризует его жесткость.

Модель, реализованная в рамках данного исследования, была разработана с опорой на типовые конструктивные параметры роторов Дарье, ранее описанные в работах [1,2]. В этих источниках рассматриваются различные геометрии лопастей, условия обтекания, диапазоны скоростей воздушного потока и подходы к численному и экспериментальному моделированию. В процессе разработки численной модели особое внимание было уделено согласованию ключевых параметров (форма, высота, радиус, диапазон скоростей) с теми, что использовались в указанных публикациях. Такой подход позволил сформировать предпосылки для последующего сопоставления результатов, полученных в ходе текущей работы, с данными, имеющимися в литературе. Кроме того, методика моделирования в среде SolidWorks и используемые аналитические зависимости были выбраны таким образом, чтобы обеспечить совместимость с подходами, уже апробированными в научных публикациях, что также способствует корректной интерпретации результатов. В следующем разделе приведены полученные в ходе расчётов значения ключевых аэродинамических и прочностных характеристик, а также выполнен их качественный и количественный анализ в контексте ранее опубликованных исследований. Это позволяет оценить точность расчётной модели, а также обоснованность использованных допущений и методов.

Результаты и обсуждение.

Дарье ротор является одним из наиболее часто используемых типов роторов для ветровых турбин с вертикальной осью вращения, благодаря его способности эффективно преобразовывать энергию ветра в механическую мощность при высоких скоростях ветра. Основная задача данного исследования — рассчитать аэродинамические силы, действующие на ротор Дарье, оценить производимую им мощность, а также изучить поведение ротора при определенных параметрах. В рамках эксперимента используются формулы для расчета эффективной площади ротора, силы сопротивления, подъемной силы, момента силы и мощности, получаемой ротором. Были выбраны следующие параметры ротора: высота ротора $L=2\text{m}$, радиус ротора $R=0.5\text{m}$, скорость ветра $V_n=8\text{ м/с}$, $\rho=1.225\text{кг/м}^3$ [12], Коэффициент скорости для ротора Дарье $\lambda=1.8$, коэффициент подъемной силы $C \approx 0.12$, коэффициент сопротивления $C_c \approx 0.6$ [13]

Эффективный радиус лопасти по формуле 1 равен:

$$R_{эфф} = 0.95 \times 0.5 = 0.475 \text{ м}$$

Для криволинейной лопасти $R_{эфф} \approx 0.95R$, что уменьшает площадь взаимодействия лопасти с потоком воздуха и снижает сопротивление. Следовательно, в соответствии с формулой 2 эффективная ометаемая площадь ротора Дарье равна:

$$A_{эфф} = 2 \times H \times R_{эфф} = 2 \times 2 \times 0.475 = 1.9 \text{ м}^2$$

В соответствии с формулой 3 сила сопротивления равна:

$$F_a(\theta) = \frac{1}{2} \cdot 1.225 \cdot 0.6 \cdot 1.9 \cdot 8^2 = 44,688 \text{ Н}$$

Сила подъема в соответствии с формулой 4 равна:

$$F_n(\theta) = \frac{1}{2} \cdot 1.225 \cdot 0.12 \cdot 1.9 \cdot 64 = 8.938 \text{ Н}$$

Момент силы можно рассчитать, используя разность между силами сопротивления и подъема по формуле 5:

$$T_T = 0.5 \times (44.688 - 8.938) \times 0.475 = 8.491 \text{ Нм}$$

В соответствии с формулой 7 была рассчитана угловая скорость:

$$\omega = \frac{1.8 \cdot 8}{0.5} = 28.8 \text{ рад/с}$$

Используя угловую скорость ω , была рассчитана мощность по формуле 7:

$$P = 8.491 \times 28.8 = 244.53 \text{ Вт}$$

Коэффициент мощности для ротора Дарье для выбранных условий составляет:

$$C = \frac{244.53}{\frac{1}{2} \cdot 1.225 \cdot 1.9 \cdot V_n^3} \quad (10)$$

На рисунке 1 представлена трехмерная модель ротора Дарье, созданная в программной среде SolidWorks. Лопасти выполнены в криволинейной форме, что способствует снижению аэродинамического сопротивления и повышению эффективности работы. Конструкция включает центральный вал и три лопасти, обеспечивающие оптимальное преобразование энергии воздушного потока в механическую мощность. Данная модель применялась для численного анализа, позволяющего исследовать поведение ротора при высоких скоростях ветра.

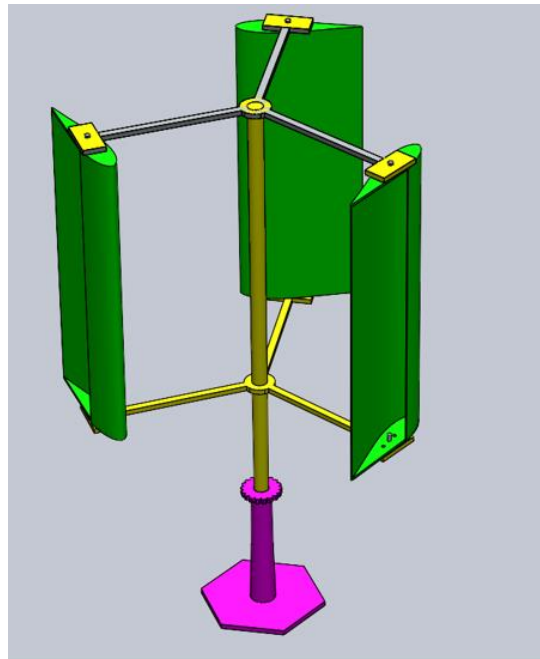


Рисунок 1 – 3Д модель ротора

На рисунке 2 приведён график нормализованных характеристик работы ротора Дарье, полученных в ходе численного моделирования, где одна итерация эквивалентна одной секунде. Процесс нормализации позволяет отследить динамику изменения параметров во времени в диапазоне от 0 до 1, что облегчает визуализацию момента стабилизации системы после определённого количества итераций. Синяя кривая отражает динамическое давление, которое возрастает на протяжении первых 30 итераций, достигает максимального значения, а затем выходит на стабильный уровень, равный 1, что свидетельствует о переходе ротора

в устойчивый режим работы. Фиолетовая линия отображает суммарное давление (статическое и динамическое), также демонстрирующее стабилизацию после 30 секунд. Этот параметр является ключевым для оценки аэродинамической нагрузки на конструкцию. Жёлтая линия характеризует уровень турбулентности, который возрастает в течение первых 30 секунд и достигает значения около 6%, что указывает на умеренную степень турбулентности в системе, положительно влияющую на эффективность работы ротора. Зелёные кривые показывают изменения вертикальной и общей скорости воздушного потока, которые, аналогично другим параметрам, выходят на стабильный уровень после первых 30 итераций, подтверждая установившийся режим работы. В целом, график демонстрирует, что основные рабочие характеристики ротора стабилизируются после 30 итераций, что свидетельствует о достижении устойчивого состояния системы.

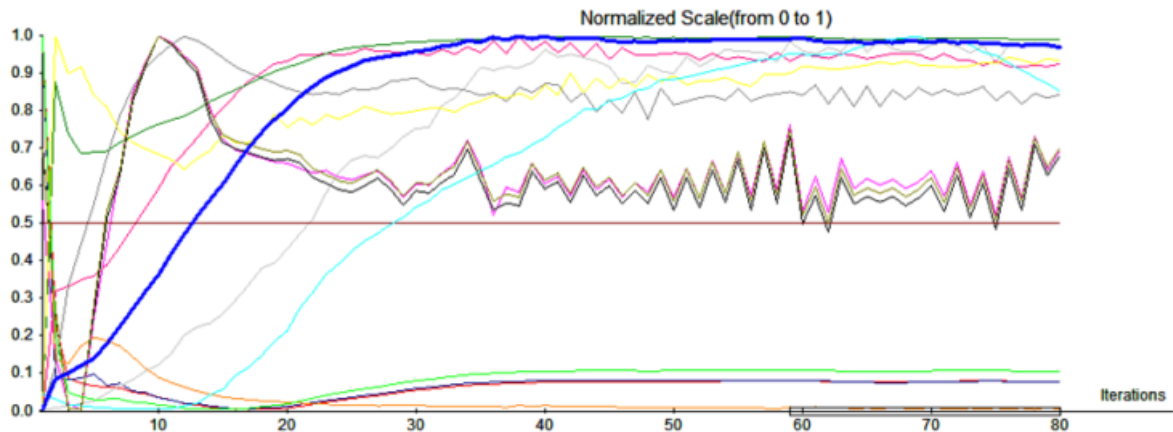


Рисунок 2 – Диаграмма нормализованных характеристик функционирования ротора Дарье

На рисунке 3 представлена таблица с основными параметрами работы ротора Дарье, полученными в результате численного моделирования. В неё включены как средние показатели, так и максимальные значения, зафиксированные в ходе расчётов. Основные параметры:

Среднее динамическое давление (GG Av Dynamic Pressure 1): составило 268.243 Па, отражая воздействие воздушного потока на лопасти ротора;

Среднее статическое давление (GG Av Static Pressure 1): стабильно на уровне 101370 Па, что соответствует атмосферному давлению и важно для оценки равномерности работы ротора;

Средняя вертикальная скорость (GG Av Velocity (Y) 1): достигла 20.165 м/с, демонстрируя характер движения воздушного потока относительно лопастей;

Максимальное динамическое давление (GG Max Dynamic Pressure 1): достигло 592.489 Па, что указывает на наибольшую нагрузку, испытываемую ротором;

Максимальная скорость воздушного потока (GG Max Velocity 1): составила 31.1 м/с, что является предельной скоростью, при которой ротор эффективно генерирует энергию.

Эти данные свидетельствуют о том, что ротор Дарье способен стабильно функционировать в условиях высоких скоростей ветра. Достижение устойчивых значений давления и скорости указывает на стабильное рабочее состояние системы и подтверждает способность конструкции выдерживать значительные аэродинамические нагрузки.

Name	Current Value	Progress	Criterion	Averaged Value
GG Av Dynamic Pressure 1	267.971 Pa	Achieved (IT = 41)	2.97306 Pa	268.243 Pa
GG Av Heat Flux 1	0 W/m ²	Achieved (IT = 40)	0 W/m ²	0 W/m ²
GG Av Static Pressure 1	101370 Pa	Achieved (IT = 54)	3.83442 Pa	101370 Pa
GG Av Total Pressure 1	101638 Pa	Achieved (IT = 54)	4.51555 Pa	101639 Pa
GG Av Turbulence Intensity 1	7.10725 %	Achieved (IT = 53)	0.571865 %	7.07384 %
GG Av Velocity (Y) 1	20.1664 m/s	Achieved (IT = 80)	0.00255442 m/s	20.1659 m/s
GG Av Velocity (Z) 1	0.234487 m/s	Achieved (IT = 79)	0.0297928 m/s	0.262034 m/s
GG Av Velocity 1	20.3726 m/s	Achieved (IT = 40)	0.0230425 m/s	20.3754 m/s
GG Friction Force (Y) 1	9.3762 N	Achieved (IT = 42)	0.204746 N	9.38799 N
GG Max Dynamic Pressure 1	592.499 Pa	Achieved (IT = 40)	34.3555 Pa	568.328 Pa
GG Max Total Pressure 1	102188 Pa	Achieved (IT = 40)	62.7313 Pa	102194 Pa
GG Max Velocity (Y) 1	31.1091 m/s	Achieved (IT = 40)	1.01021 m/s	30.5578 m/s
GG Max Velocity (Z) 1	19.6333 m/s	Achieved (IT = 40)	1.09542 m/s	19.6183 m/s
GG Max Velocity 1	31.3689 m/s	Achieved (IT = 40)	0.943034 m/s	30.721 m/s
SG Av Total Pressure 1	101373 Pa	Achieved (IT = 53)	5.12907 Pa	101373 Pa

Рисунок 3 – Таблица параметров при работе ротора Дарье

Был проведён эксперимент по численному моделированию деформации ротора Дарье для анализа его поведения при критической скорости ветра 25 м/с, что позволило определить прочностные характеристики конструкции и выявить области наибольших напряжений (рисунок 4). В процессе исследования рассматривался ротор с высотой 2 м и радиусом лопастей 0.5 м, оснащённый криволинейными лопастями. В качестве материала использовался алюминий с модулем Юнга $E = 69 \times 10^9$ Па, что позволило достоверно рассчитать напряжения в конструкции. Значение скорости воздушного потока 25 м/с было выбрано как предельное для данного типа роторов, при этом нагрузка на его поверхность рассчитывалась на основе параметров воздушного потока. Результаты моделирования показали, что максимальное смещение конструкции составило 0.630 мм в верхней части ротора. Этот показатель оказался значительно ниже по сравнению с более гибкими конструкциями, что свидетельствует о высокой устойчивости ротора Дарье к ветровым нагрузкам.

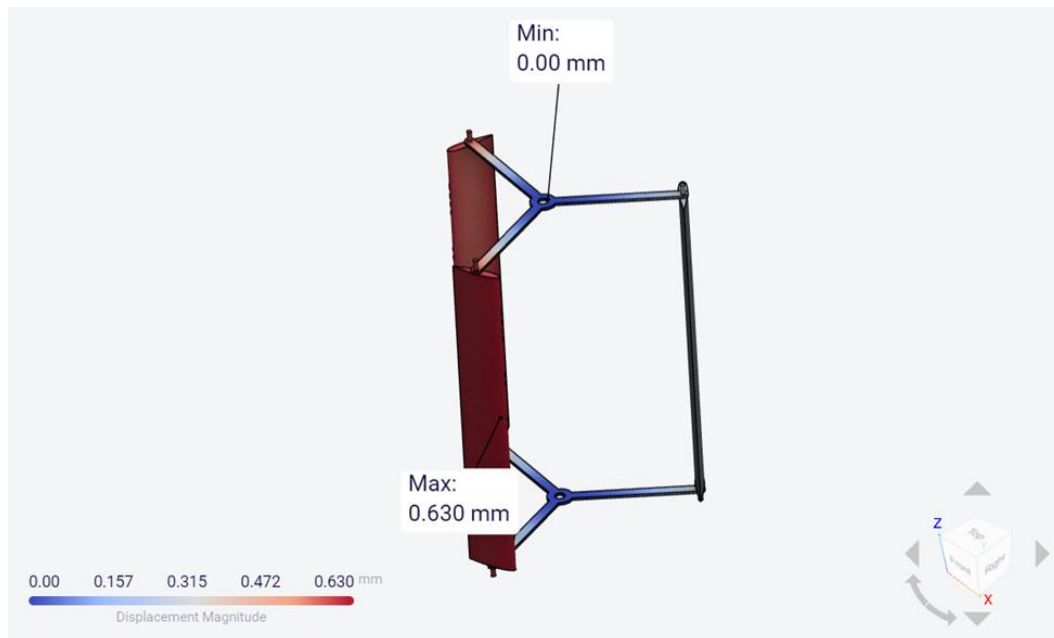


Рисунок 4 – Деформация ротора Дарье

Максимальное смещение, полученное в ходе эксперимента, $\Delta L = 0.630$ мм = 0.00063 м, может быть использовано для расчёта давления, воздействующего на ротор. Оценка давления производится с учётом модуля упругости материала, применяя уравнение деформации согласно формуле 9:

$$0.00063 = \frac{P \cdot 2}{69 \cdot 10^9} \quad (11)$$

Таким образом, давление равно:

$$P = \frac{0.00063 \cdot 69 \cdot 10^9}{2} = 21.735 \cdot 10^6 \text{ Па}$$

Численное моделирование деформации ротора Дарье при критической скорости ветра 25 м/с показало, что максимальное смещение конструкции в верхней части ротора составило 0.630 мм. Применение алюминия с модулем Юнга $E = 69 \times 10^9$ Па позволило провести оценку напряжений, возникающих в роторе. Расчёты продемонстрировали, что при заданных условиях давление на конструкцию достигает 21.735 МПа. Полученные результаты свидетельствуют о высокой прочности ротора Дарье, его устойчивости к ветровым нагрузкам и способности минимизировать деформации, что способствует увеличению срока службы устройства в условиях реальной эксплуатации.

Полученные результаты были сопоставлены с данными, приведёнными в исследовании [14]. Так, расчётный коэффициент мощности, а также значения крутящего момента и аэродинамических нагрузок, полученные в рамках настоящей работы, находятся в пределах, характерных для аналогичных моделей роторов Дарье с криволинейными лопастями, представленных в указанных публикациях. В частности, работы [15] содержат численные и экспериментальные оценки, которые демонстрируют близкую динамику поведения ротора при аналогичных условиях воздушного потока. Это подтверждает адекватность использованной численной модели и применённых допущений.

Кроме того, характер установления устойчивого режима, отражённый на рисунке 2, качественно соответствует временным характеристикам, описанным в работах [16] и [17], что позволяет говорить о воспроизводимости ключевых закономерностей.

Тем не менее, необходимо отметить ряд ограничений, присущих данной модели. Во-первых, численное моделирование проводилось при условии ламинарного обтекания ротора и постоянной скорости воздушного потока, что не в полной мере отражает реальные атмосферные условия, включая турбулентность, порывы ветра и влияние окружающих объектов. Во-вторых, прочностной анализ конструкции базировался на упрощённой геометрии и линейной модели деформаций, что может не учитывать локальные концентрации напряжений и колебательные процессы. В-третьих, расчёты проводились в стационарной постановке, без учёта циклических нагрузок и усталостных характеристик материалов, что ограничивает возможность экстраполяции результатов на длительный период эксплуатации.

Указанные ограничения следует учитывать при интерпретации результатов, а также при планировании дальнейших исследований, направленных на расширение применимости модели и повышение её прогностической точности.

Заключение.

В данной работе проведено теоретическое и численное моделирование ротора Дарье, одного из наиболее эффективных типов роторов для ветровых турбин с вертикальной осью вращения. Исследование включало анализ аэродинамических характеристик ротора, таких как сила сопротивления, подъёмная сила, крутящий момент, угловая скорость и мощность. Используемые аналитические методы и численное моделирование в среде SolidWorks позволили детально оценить поведение ротора при различных параметрах воздушного потока. Результаты численного моделирования подтвердили, что ротор Дарье способен эффективно преобразовывать энергию ветра в механическую мощность, особенно при высоких скоростях воздушного потока. Графики нормализованных параметров показали, что система достигает устойчивого режима работы после 30 итераций, а основные аэродинамические характеристики стабилизируются. Проведённый анализ напряжений и деформаций конструкции ротора при критической скорости ветра 25 м/с продемонстрировал его высокую механическую прочность. Максимальное смещение в верхней части ротора составило 0.630 мм, что подтверждает устойчивость конструкции

даже при значительных аэродинамических нагрузках. Расчёты давления и механической нагрузки показали, что ротор выдерживает воздействие потока воздуха без значительных деформаций, что обеспечивает его долговечность и надёжность в эксплуатации. Таким образом, полученные результаты могут быть полезны для дальнейшего проектирования и оптимизации ветроэнергетических установок с ротором Дарье, позволяя повысить их эффективность и структурную устойчивость.

Проведённое исследование создаёт основу для дальнейшего совершенствования конструкции роторов Дарье. В будущем планируется расширить модель за счёт учёта нестационарных ветровых условий, турбулентности, усталостных характеристик материала и влияния температуры окружающей среды. Также представляется перспективным использование оптимизационных алгоритмов для улучшения аэродинамической формы лопастей и внедрение адаптивных конструктивных элементов, способных изменять геометрию в зависимости от условий эксплуатации.

Информация о финансировании

Результаты исследований проведены при поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан в рамках гранта «AP23489937 Разработка механической саморегулирующейся коробки передач для военно-транспортной техники».

Список источников

1. Mohan M., Saha U. K. «Evolving a Novel Blade Shape of a Savonius Wind Rotor Using an Optimization Technique Coupled With Numerical Simulations and Wind Tunnel Tests», *Journal of Energy Resources Technology*. – 2024. – Т. 146. – № 4. – С. 041301.
2. Banerjee A., Roy S., Mukherjee P., Saha U. K. «Unsteady Flow Analysis Around an Elliptic-Bladed Savonius-Style Wind Turbine», *Proceedings of the ASME Gas Turbine India Conference*. – 2019. – С. V001T06A003.
3. Sharma S., Sharma R. K. «Performance Improvement of Savonius Rotor Using Multiple Quarter Blades – A CFD Investigation», *Energy Conversion and Management*. – 2018. – Т. 127. – С. 43–54.
4. Roy S., Mukherjee P., Saha U. K. «Aerodynamic Performance Evaluation of a Novel Savonius-Style Wind Turbine under an Oriented Jet», *Proceedings of the ASME Gas Turbine India Conference*. – 2023. – С. V001T06A004.
5. Acarer S., Uyulan Ç., Karadeniz Z. H. «Optimization of Radial Inflow Wind Turbines for Urban Wind Energy Harvesting», *Energy*. – 2020. – Т. 202. – С. 117772.
6. Grinspan A. S., Saha U. K., Mahanta P. «Experimental Investigation of Twisted Bladed Savonius Wind Turbine Rotor», *Proceedings of the International Conference on Renewable Energy for Developing Countries*. – 2018. – С. 1–6.
7. Pyankov K. S., Toporkov M. N. «Mathematical modeling of flows in wind turbines with a vertical axis», *Fluid Dynamics*. – 2014. – Т. 49. – № 2. – С. 249–258 pp.
8. Zhang S., Lee K. «Dynamic Blade Adjustment Mechanisms for Vertical Axis Wind Turbines», *Energy Conversion and Management*. – 2021. – Т. 54. – С. 89–101 pp.
9. Brown D. S. «The Role of Aerodynamic Resistance in Wind Energy Conversion», *International Journal of Renewable Energy Research*. – 2023. – Т. 31. – № 2. – С. 210–221 pp.
10. Patel G., Novak E. «Advanced Control Strategies for Variable-Speed Wind Turbines», *Wind Engineering Review*. – 2021. – Т. 22. – № 4. – С. 178–192 pp.
11. Schmidt B., Zhao L. «Analysis of P-, I-, and D-Controllers in Wind Energy Applications», *Control Systems Review*. – 2022. – Т. 27. – № 3. – С. 98–115 pp.
12. Yamada S. «Modeling of Wind Force in Energy Systems», *Journal of Theoretical Mechanics*. – 2022. – Т. 45. – № 3. – С. 101–115 pp.
13. Aliyev M., Kadyrov A. «Wind Energy Resource Mapping in Kazakhstan», *Renewable Energy*. – 2022. – Т. 35. – № 4. – С. 451–465 pp.

14. Isataev, M.; Manatbayev, R.; Seydulla, Z.; Kalassov, N.; Yershina, A.; Baizhuma, Z. Experimental and Computational Study of the Aerodynamic Characteristics of a Darrieus Rotor with Asymmetrical Blades to Increase Turbine Efficiency Under Low Wind Velocity Conditions. Appl. Syst. Innov. 2025, 8, 49. <https://doi.org/10.3390/asi8020049>

15. Chen, W.-H.; Lam, T.T.; Chang, M.-H.; Jin, L.; Chueh, C.-C.; Augusto, G.L. Optimizing H-Darrieus Wind Turbine Performance with Double-Deflector Design. Energies 2024, 17, 503. <https://doi.org/10.3390/en17020503>

16. Elbeji, T.; Ben Amira, W.; Souaissa, K.; Ghiss, M.; Bentaher, H.; Ben Fredj, N. Three-Dimensional Aeroelastic Investigation of a Novel Convex Bladed H-Darrieus Wind Turbine Based on a Two-Way Coupled Computational Fluid Dynamics and Finite Element Analysis Approach. Fluids 2025, 10, 17. <https://doi.org/10.3390/fluids10010017>

ДАРЬЕ РОТОРЫНЫҢ АЭРОДИНАМИКАЛЫҚ СИПАТТАМАЛАРЫ МЕН МЕХАНИКАЛЫҚ ТҰРАҚТЫЛЫҒЫН ТЕОРИЯЛЫҚ ЖӘНЕ САНДЫҚ МОДЕЛЬДЕУ

Аңдатпа. Бұл мақалада тік айналу осі бар жел турбиналары үшін ең танымал роторлардың бірі – Дарье роторының теориялық және сандық модельдеуі берілген. Ротордың тиімді ауданын, қарсылық күшін, көтеру күшін, айналу моментін және қуатты қоса алғанда, аэродинамикалық сипаттамалардың есептеулері жүргізілді. Ауа ағынының әртүрлі параметрлерінде ротордың жұмысын бағалау үшін SolidWorks ортасында аналитикалық әдістер мен сандық модельдеу қолданылды. Сондай-ақ, сыни жүктемелер кезінде құрылымның деформациясын талдау жүргізілді, бұл оның тұрақтылығы мен тиімділігін бағалауға мүмкіндік берді. Нәтижелер Дарье роторының желдің жоғары жылдамдығында тұрақты жұмыс істеу қабілетін және оның жоғары механикалық беріктігін растайды.

Түйін сөздер: Дарье роторы, сандық модельдеу, аэродинамикалық өнімділік, жел турбинасы, деформациялық талдау.

THEORETICAL AND NUMERICAL MODELING OF AERODYNAMIC CHARACTERISTICS AND MECHANICAL STABILITY OF THE DARRIER ROTOR

Аннотация. This article presents a theoretical and numerical simulation of the Darrier rotor, one of the most popular rotors for wind turbines with a vertical axis of rotation. Calculations of aerodynamic characteristics, including the effective area of the rotor, drag force, lifting force, torque and power are carried out. Analytical methods and numerical modeling in the SolidWorks environment were used to evaluate the operation of the rotor at various air flow parameters. An analysis of the deformation of the structure under critical loads was also performed, which made it possible to assess its stability and efficiency. The results obtained confirm the Darrier rotor's ability to operate stably at high wind speeds and its high mechanical strength.

Keywords: Darrier rotor, numerical modeling, aerodynamic characteristics, wind turbine, deformation analysis.

Авторлар туралы мәлімет

Фазылова Алина	Электрондық инженерия кафедрасының аға оқытушысы, PhD, Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан Республикасы, e-mail: a.fazylova@aes.kz
Қуаныш Алипбаев	Ғылыми жұмыс жөніндегі проректор, PhD, Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан Республикасы e-mail: k.alipbayev@aes.kz
Арай Оразалиева	Кіші ғылыми қызметкер, PhD докторант, Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан Республикасы e-mail: a.orazaliyeva@aes.kz
Әлішер Әден,	Ғылыми қызметкер, PhD докторант, Алматы энергетика және байланыс университеті. Ғұмарбек Дәукеев, Алматы, Қазақстан Республикасы e-mail: a.aden@aes.kz

Сведение об авторах

Фазылова Алина	Старший преподаватель кафедры «Электронная инженерия», PhD, Алматинский Университет Энергетики и связи имени Гумарбека Даукеева, Алматы, Республика Казахстан, e-mail: a.fazylova@aes.kz
Қуаныш Алипбаев	Проректор по научной работе, PhD, Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы, Казахстан, e-mail: k.alipbayev@aes.kz
Арай Оразалиева	младший научный сотрудник, докторант PhD, Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы, Республика Казахстан e-mail: a.orazaliyeva@aes.kz
Алишер Аден	Научный сотрудник, PhD докторант, Алматинский университет энергетики и связи им. Гумарбека Даукеева, Алматы, Республика Казахстан e-mail: a.aden@aes.kz

Information about the authors

Alina Fazylova,	Senior Lecturer at the Department of Electronic Engineering, PhD, Gumarbek Daukeev Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan, e-mail: a.fazylova@aes.kz
Kuanysh Alipbayev	Vice-Rector of Science, PhD, The Gumarbek Daukeyev Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan e-mail: k.alipbayev@aes.kz
Aray Orazaliyeva	Junior researcher, PhD candidate, The Gumarbek Daukeyev Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan e-mail: a.orazaliyeva@aes.kz
Alisher Aden	Researcher, PhD candidate, The Gumarbek Daukeyev Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan e-mail: a.aden@aes.kz



ӘОЖ 004.9:615.8

ҒТАХА 28.20:61.67

https://doi.org/10.53364/24138614_2025_38_3_16

М.У.Сулейменова^{1*}, К.Б.Абзалиев¹, С.А.Абзалиева¹, Д.М.Мұхаммеджанова¹

¹ Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

*E-mail: madekin940@gmail.com

ЕРТЕ ҚАРТАЮ БЕЛГІЛЕРІН АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНУ

Аңдатпа. Ерте патологиялық қартаю көбіне жүрек-қантамыр ауруларымен байланысты, бұл аурулар әлеуметтік-экономикалық, метаболикалық, мінез-құлық және қоршаған ортаға байланысты тәуекел факторларының жиынтығынан туындайды. Бұл факторлар жыныстық айырмашылықтар, жас, жоғары қан қысымы, семіздік, физикалық белсенділіктің төмендігі, шылым шегу, алкогольді шамадан тыс пайдалану, холестерин мен глюкоза деңгейінің жоғарылығы және қант диабетін қамтиды. Адам ағзасындағы барлық процестер биохимиялық және иммунологиялық талдауларда көрініс табады және олар жүрек-қантамыр жүйесінің ерте қартаюының маркерлері болуы мүмкін.

Авторлар білім, жұмыс, жыныс, отбасылық жағдай, мүгедектік, физикалық белсенділік, шылым шегу және алкоголь тұтыну сияқты әлеуметтік факторлар мен жүректің ишемиялық ауруы (ЖИА), инфаркттан кейінгі кардиосклероз (ИКС), созылмалы жүрек жеткіліксіздігі (СЖЖ), қант диабеті (ҚД), дене массасының индексі (ДМИ), глюкоза деңгейі, жалпы холестерин (ЖХ) және қан қысымы (ҚҚ) сияқты клиникалық көрсеткіштер арасындағы байланыстарды зерттеді. Сонымен қатар, 65-74 жас, 75-89 жас және 90 жастан асқан пациенттердің клиникалық деректері (биомаркерлер) мен әлеуметтік өмірі арасындағы корреляцияны анықтады.

Түйін сөздер: жасанды интеллект, машиналық оқыту, ерте қартаю маркерлері, жүрек-қантамыр аурулары, иммундық қартаю, болжау.

Кіріспе.

Соңғы жылдары халықтың жас құрылымы айтарлықтай өзгерді; соңғы онжылдықтардағы демографиялық жағдай егде жастағы адамдардың санының өсуімен сипатталады. БҰҰ деректеріне сәйкес, қазіргі уақытта 65 жастан асқан қарттар жалпы халықтың шамамен 15%-ын құрайды. Бұл жағдай парадоксты сипатта: өмір сүру ұзақтығы төмен, бірақ егде жастағы, жалғызбасты және жесірлер саны өсуде. Мұндай демографиялық өзгерістер экономикаға әсер етеді, себебі еңбекке қабілетті халықтың үлесі азайып, денсаулық сақтау шығындары артып келеді, оның негізгі бөлігін қарт адамдарға жұмсалады [1,2,4].

Адам өмірінің ұзақтығын арттыру, аурушандықты азайту және ерте қартаюдың алдын алу — қазіргі заманғы алдын алу медицинасындағы ең маңызды міндеттердің бірі. Жасқа байланысты өзгерістер алдымен жүрек-қантамыр жүйесіне әсер етеді. Дәл осы жүйе ұзақ өмір сүру мен ерте қартаюдың арасындағы айырмашылықты анықтайды [1,2,3]. Жүрек-қантамыр аурулары (ЖҚА) ондаған жылдар бойы әлемде өлімнің негізгі себебі болды. 2021 жылы 20,5 миллион адам жүрек-қантамыр ауруларынан қайтыс болды, бұл 1990 жылы

тіркелген 12,1 миллионға қарағанда айтарлықтай жоғары көрсеткіш және жалпы өлім-жітімнің үштен біріне жуығын құрайды. Қазіргі уақытта коронарлық жүрек ауруы (КЖА) 146 елде ерлер арасында және 98 елде әйелдер арасында мерзімінен бұрын қайтыс болудың негізгі себебі болып табылады [5,6,7].

Дүниежүзілік денсаулық сақтау ұйымының (ДДҰ) болжамына сәйкес, демографиялық өзгерістерге (халықтың қартаюуы), инфекциялық емес аурулардың өсуіне және өмір салтының өзгеруіне байланысты дамыған және дамушы елдерде ЖҚА және одан болатын өлім-жітімнің өсуі жалғасады деп күтілуде [8]. Қазақстанда да жүрек-қан тамыр жүйесі патологияларының жиілігінің өсу тенденциясы байқалады, оны бір жағынан, скринингтік тексерулердің сапасын жақсарту және анықтауды жақсарту арқылы, екінші жағынан, медициналық көмектің қолжетімділігі мен сапасының төмендеуімен түсіндіруге болады [9].

Жүрек-қан тамыр аурулары жүрекке немесе қан тамырларына әсер етеді және әлеуметтік-экономикалық, метаболикалық, мінез-құлық және қоршаған орта қауіп факторларының үйлесімінен туындауы мүмкін. Оларға жыныс айырмашылықтары, жас, жоғары қан қысымы, семіздік, физикалық белсенділіктің төмендігі, шылым шегу, алкогольді шамадан тыс тұтыну, холестерин мен глюкоза деңгейінің жоғарылығы және қант диабеті жатады. Әдеби деректерді талдау нәтижелері бойынша қауіп факторларының таралуы негізінен шектеулі популяцияларда зерттеледі [10,11,12].

Ерлер мен әйелдер арасындағы ЖҚА даму қаупі жас ұлғайған сайын теңестірілетіні туралы кейбір ғылыми дәлелдер бар [14]. Соңғы мәліметтер ерлер арасында коронарлық жүрек ауруы (КЖА) жиілігінің төмендегенін, ал әйелдер арасында төмендемегенін көрсетеді. Жыныс пен жас көптеген жүрек-қан тамыр денсаулығы туралы зерттеулерде маңызды өзгермейтін қауіп факторлары ретінде есепке алынады. Жыныс пен жас ЖҚА болжау модельдерінің көпшілігіне кіреді [13,14]. Осылайша, егде жастағы адамдар арасында ЖҚА даму қаупінің факторларын зерттеу алдын алу медицинасында маңызды бағыт болып табылады.

2021 жылы Жаһандық аурудың жүктемесі зерттеуіне сәйкес, әлемдегі өлімнің жетекші өзгермелі қауіп факторы жоғары қан қысымы болып табылады және ол жүрек-қан тамыр ауруларынан 10,8 миллион өлімге жауапты болды [5,13]. ДДҰ семіздікті 21 ғасырдағы жаңа инфекциялық емес "эпидемия" ретінде қарастырады. Бұл аурудың жоғары таралуы урбанизациямен, физикалық белсенділіктің төмендеуімен және жоғары калориялы тағамның қолжетімділігімен байланысты [13,14]. Жүргізілген көптеген ғылыми зерттеулер артық салмақ, семіздік және ЖҚА дамуы арасындағы тығыз байланысты көрсетеді [15]. Семіздіктің себептерінің бірі — физикалық белсенділіктің болмауы, ол ЖҚА негізгі қауіп факторларының бірі болып табылады. Бірнеше зерттеулер гиподинамия мен ЖҚА дамуы арасындағы байланысты растады, сонымен қатар физикалық белсенділіктің төмендігі 2 типті қант диабеті, семіздік, қатерлі ісік, остеопороз сияқты аурулардың даму қаупін арттырады. Бұл аурулар да жасқа байланысты аурулар деп аталады [12,13]. Ғылыми бағалауларға сәйкес, шылым шегу жүрек-қан тамыр ауруларының 10%-ына жауапты және ЖҚА дамуының қан қысымынан кейінгі екінші негізгі себебі болып табылады. Темекі түтініне әсер тек шылым шегушілерге ғана емес, басқаларға да зиянын тигізеді. Жыл сайын темекі шегу немесе темекі түтініне әсер ету салдарынан шамамен 6 миллион адам қайтыс болады, бұл әйелдер арасындағы өлімнің 6%-ын және ерлер арасындағы өлімнің 12%-ын құрайды. Темекіге байланысты өлім-жітім 2030 жылға қарай жылына 8 миллионнан астам өлімге дейін өседі деп болжануда [16,17,18,19]. 2019 жылы алкоголь салдарынан 2,4 миллионнан астам адам қайтыс болды, бұл әлемдегі барлық өлім-жітімнің 4,3%-ын және 15-тен 49 жасқа дейінгі ер адамдар арасындағы өлімнің 12,6%-ын құрады. Ғылыми зерттеулер алкогольдің аз мөлшері де жүрек-қан тамыр ауруларының, соның ішінде коронарлық жүрек ауруы, инсульт, жүрек жеткіліксіздігі, гипертензиялық жүрек ауруы, кардиомиопатия, жүрекшелердің фибрилляциясы және аневризма қаупін арттыратынын көрсетті [20].

ЖҚА өлім-жітімін азайту үшін, ең алдымен, алдын алу бағытын дамыту қажет. Алдын алу негізі — денсаулық сақтау жүйесінің ЖҚА даму қауіп факторларын анықтап, оларды түзету қабілетінде жатыр [5,10,11]. Тиісінше, ЖҚА халық денсаулығы деңгейіне әсері ғылыми қауымдастықты осы мәселені шешудің жаңа жолдарын іздеуге итермелейді. Бұл мәселені шешудің бір жолы — медициналық ақпараттық технологияларды дамыту, ол медициналық көмектің барлық сатыларында қолданылып, биоақпараттану, медициналық информатика және биомедициналық информатика сияқты көптеген мамандықтарды қамтиды [21]. Әдебиеттерге сәйкес, ақпараттық технологиялар мен бағдарламалаудың клиникалық қолданылуының жоғары тиімділігі асқынулар мен қолайсыз жағдайлар санын азайтуға, әлеуметтік және экономикалық пайда алуға және өмір сапасын жақсартуға бағытталған. Осы технологияларды клиникалық тәжірибеге енгізудің артықшылықтары соңғы онжылдықтарда белсенді түрде талқыланып келеді [21,22].

[23] еңбегінде автор ақпараттық технологиялардың қарқынды дамуын, оның ішінде медицинада информатикаландыру үдерістерінде маңызды рөлін ашып көрсетеді. Медициналық жүйелерге соңғы IT жетістіктерін енгізу бұл үдерістерге айтарлықтай әлеуметтік мән береді. Машиналық оқыту, жасанды нейрондық желілер және терең оқыту сияқты жасанды интеллект технологиялары ерекше сұранысқа ие болуда. Бұл жұмыс медициналық жүйелерде машиналық оқыту әдістерін қолдану үрдістері мен болашағын бағалауға арналған. Машиналық оқытуды медицинада қолдану маңызды, себебі ол әртүрлі міндеттердің жылдамдығын, сапасын және сенімділігін арттырып, мамандардың жұмысын жеңілдетеді және оларға бағдарламалық қолдау көрсетеді. Жұмыста осы саладағы негізгі жаһандық үрдістер, жүйелерді әзірлеуші компаниялар, сондай-ақ бұл үдерісті шектейтін факторлар талданады. Сонымен қатар, [24] зерттеуіне сәйкес, жасанды интеллект медицинада барған сайын белсенді қолданылуда, және жыл сайын денсаулық сақтау саласына арналған ИИ шешімдерін әзірлейтін компаниялардың саны артып келеді. ИИ дәрігерлерге диагностикада көмек көрсетуді қолдай алады, бірақ оның қолданылуы верификацияланған деректердің жеткіліксіздігі, медициналық құрылғылардың қорғалмағандығы және заңнамалық базаның болмауы сияқты шектеулерге байланысты белгілі бір міндеттермен шектелген. Болашақта әртүрлі дереккөздерден алынған деректерді кешенді түрде талдай алатын жүйелер тиімді болады деп болжануда. Алайда, [25] еңбегінде көрсетілгендей, машиналық оқыту алгоритмдеріне негізделген дәл болжау модельдерін қолдану инфекциялық емес ауруларды, олардың асқынуларын және госпитализация ықтималдығын болжауда жаңа мүмкіндіктер ашады, бұл алдын алу және емдеу шараларын уақтылы тағайындауға мүмкіндік береді. Әдеби шолу мұндай модельдердің кардиологияда, неврологияда, генетикада және басқа салаларда жоғары дәлдігін көрсетеді, ал Random Forest, нейрондық желілер және XGBoost алгоритмдері ең тиімді болып саналады. Бұл алгоритмдерді медициналық ақпараттық жүйелерге енгізу медициналық оқиғаларды болжауды жақсартуға және дербестендірілген медицинаның жаһандық үрдістеріне сәйкес келуге уәде береді. Осы саладағы зерттеулердің артуы машиналық оқыту технологияларын кеңінен қолдану үшін одан әрі зерттеу және оңтайландыру қажеттілігін көрсетеді. Қазіргі уақытта машиналық оқыту және R тілін қолдану ауруларды диагностикалау және болжау, қауіп факторларын анықтау, деректер базасын құру және науқастардың жағдайын бақылау үшін медицинада кеңінен қолданылуда.

Зерттеудің материалдары мен әдістері.

Зерттеу барысында білім деңгейі, жұмыс, жыныс, отбасылық жағдай, мүгедектік, физикалық белсенділік, шылым шегу және алкоголь тұтыну сияқты әлеуметтік факторлар мен коронарлық жүрек ауруы, инфаркттан кейінгі кардиосклероз, созылмалы жүрек жеткіліксіздігі, қант диабеті, дене массасының индексі, глюкоза деңгейі, жалпы холестерин және қан қысымы сияқты клиникалық көрсеткіштер арасында маңызды корреляциялар анықталды.

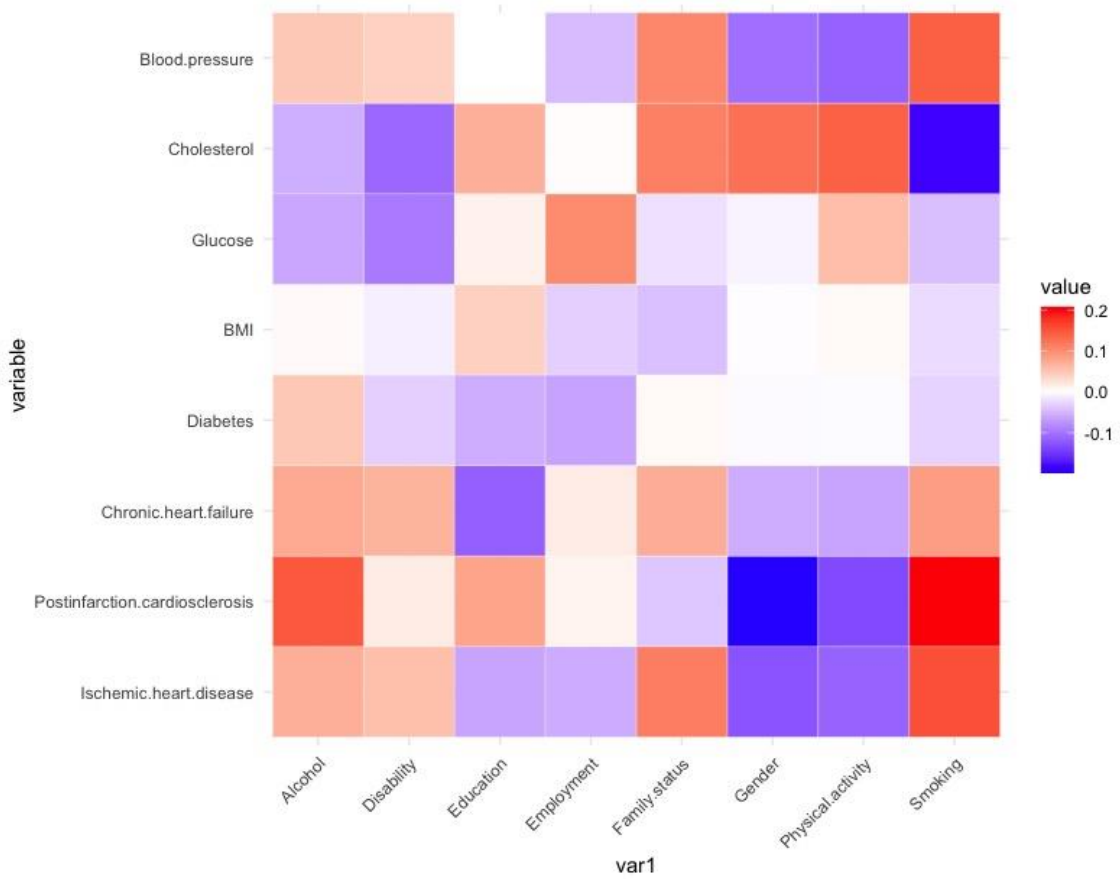
Зерттеу барысында жас және жыныс сияқты өзгермейтін қауіп факторларының жүрек-қантамыр патологиясы мен ЖҚА дамуында маңызды рөл атқаратыны анықталды. Егде және қарт жастағы топтағы әлеуметтік-демографиялық және зертханалық параметрлерді талдау темекі шегу, алкоголь тұтыну, дене массасының индексі (ДМИ), қан қысымы, ашқарындағы холестерин және глюкоза деңгейі сияқты бірқатар скринингтік көрсеткіштер бойынша ауытқулардың бар екенін көрсетті.

Зерттеу топтарындағы қауіп факторларының таралуын зерттегеннен кейін, R бағдарламалау тілі арқылы корреляциялық талдау жүргізілді. Талдау әртүрлі айнымалылар арасындағы қатынастарды бағалауды қамтыды, бұл статистикалық маңызды корреляцияларды анықтауға және қауіп факторлары мен зерттеу нәтижелері арасындағы байланыстың күшін бағалауға мүмкіндік берді. R тілінде бағдарламалау аналитикалық процедураларды орындауда дәлдік пен тиімділікті қамтамасыз етіп қана қоймай, айнымалылар арасындағы қатынастарды жақсы түсіну үшін нәтижелерді визуализациялауға мүмкіндік берді. Деректерді алу және 65-74, 75-89 және 90+ жас топтары бойынша пациенттің әлеуметтік өмірі мен клиникалық деректері (биомаркерлері) арасындағы корреляцияларды есептеу үшін дәстүрлі машиналық оқыту классификаторларымен үйлесетін "RStudio" 2023.09.0+463 нұсқасы қолданылды. Біздің тәсіліміз биомаркерлер арасындағы байланысты табуды қамтыды және осы мақсатта Пирсон корреляция коэффициенті кеңінен қолданылды:

$$r = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^N (y_i - \bar{y})^2}}$$

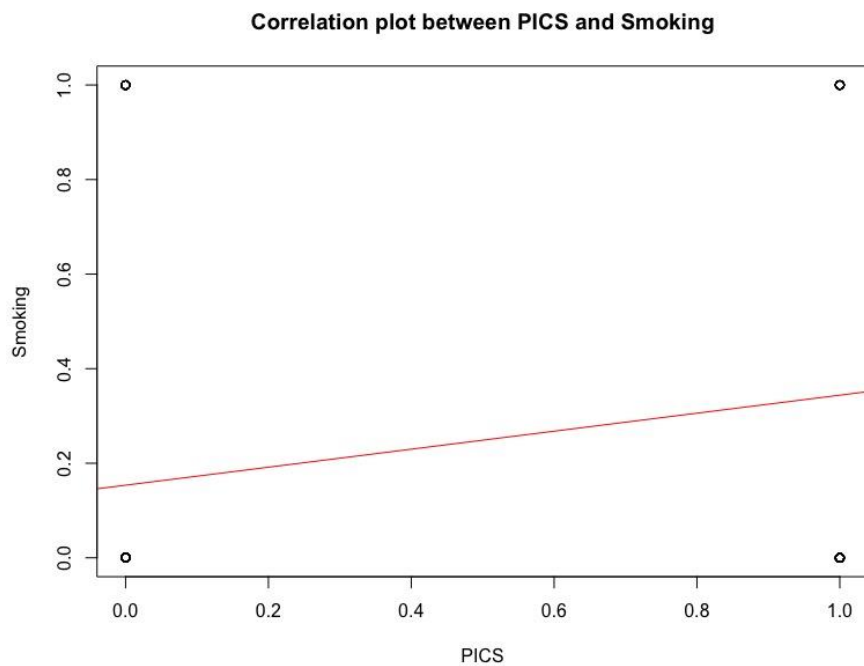
Нәтижелер және оларды талқылау.

Зерттеу барысында білім, жұмыс, жыныс, отбасылық жағдай, мүгедектік, физикалық белсенділік, шылым шегу және алкоголь сияқты әлеуметтік факторлар мен коронарлық жүрек ауруы, инфаркттан кейінгі кардиосклероз, созылмалы жүрек жеткіліксіздігі, қант диабеті, дене массасының индексі, глюкоза деңгейі, жалпы холестерин және қан қысымы сияқты клиникалық деректер арасында маңызды корреляциялар анықталды. Науқастың жынысы, отбасылық жағдайы, білімі, мүгедектігі, жұмысы, физикалық белсенділігі, шылым шегу және алкоголь тұтынуы сияқты әлеуметтік деректер x осіне орналастырылды. Науқастың коронарлық жүрек ауруы (КЖА), инфаркттан кейінгі кардиосклероз (ИКС), жүрек-қантамыр аурулары (ЖҚА), қант диабеті (ҚД), дене массасының индексі (ДМИ), глюкоза, жалпы холестерин (ЖХ) және артериялық гипертензия (АГ) сияқты клиникалық деректері y осіне орналастырылды. 60-74 жас аралығындағы топ үшін негізгі нәтижелер 1-суретте көрсетілген.



1 сурет – 65-74 жас тобындағы негізгі нәтижелер

Корреляция коэффициентінің мәні -0.1 мен 0.2 аралығында өзгереді. Біздің деректерге сәйкес, инфаркттан кейінгі кардиосклероз (ИКС) пен шылым шегу арасында жақсы корреляция анықталды ($r=0.15$) (2-сурет).

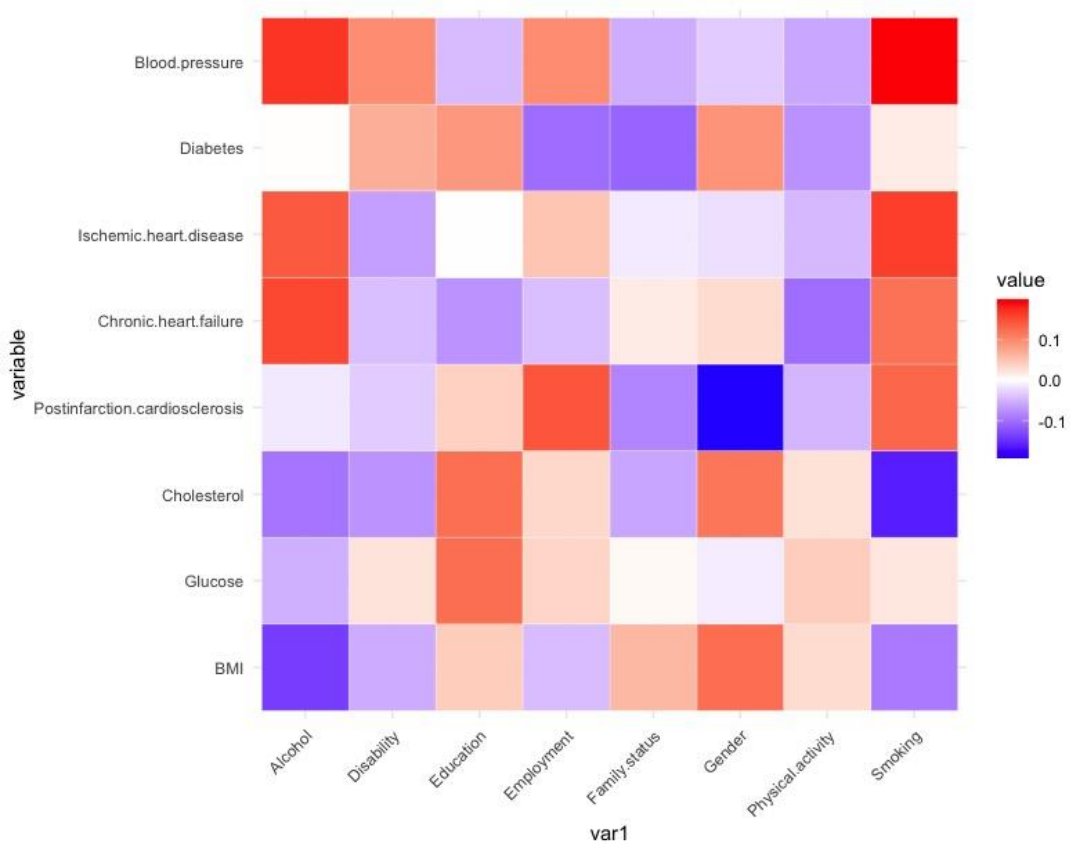


2 сурет – ИКС пен шылым шегу арасындағы корреляция графигі

Шылым шегу мен коронарлық жүрек ауруы (КЖА) арасында оң корреляция байқалады ($r = 0.15$). Дәл осындай байланыс инфаркттан кейінгі кардиосклероз (ИКС) пен алкоголь арасында да байқалады, бұл жүрек денсаулығын сақтау үшін зиянды әдеттерден аулақ болу қажеттілігін көрсетеді. Физикалық белсенділік пен жалпы холестерин деңгейі (ОХ) арасында оң корреляция анықталды ($r = 0.1$), бұл қан холестеринін бақылауда жүйелі жаттығудың маңыздылығын көрсетеді. Дене массасының индексі (ДМИ) мен жыныс, сондай-ақ қант диабеті мен отбасылық жағдай арасында байланыс анықталған жоқ.

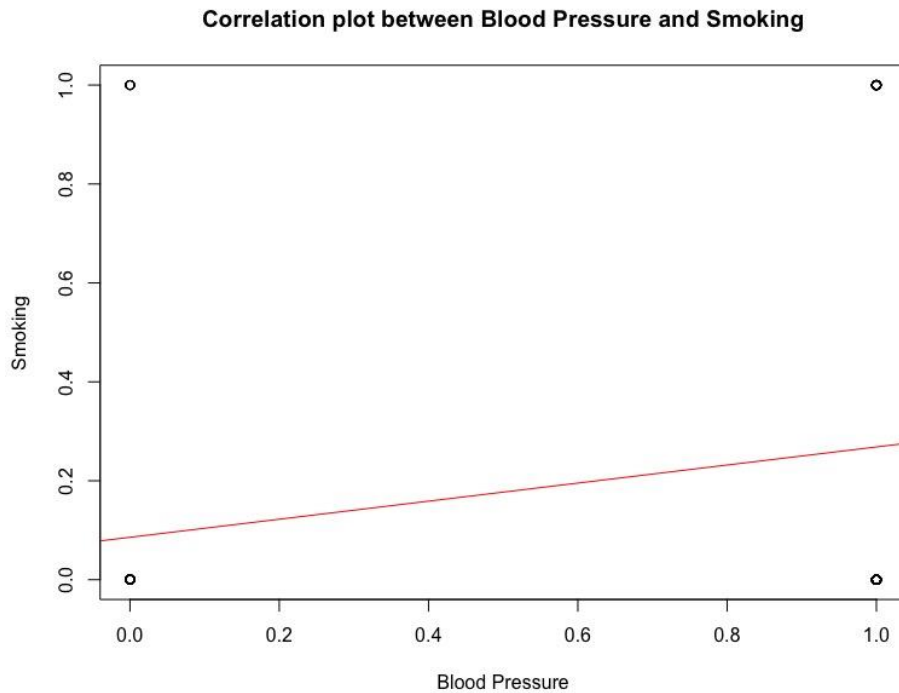
Алайда, біздің зерттеуде жалпы холестерин мен шылым шегу арасында кері байланыс ($r = -0.1$), сондай-ақ инфаркттан кейінгі кардиосклероз (ИКС) пен жыныс арасында кері байланыс анықталды (6-сурет). Бұл нәтижелер 65-74 жас аралығындағы адамдар арасында жүргізілген зерттеу барысында жиналған деректерді талдау нәтижесін көрсетеді.

75-89 жас санаты үшін нәтижелер төмендегідей:



3 сурет – 75-89 жас тобындағы негізгі нәтижелер

Бұл топта корреляция коэффициенті -0.1 мен 0.1 аралығында өзгереді. Қан қысымы мен шылым шегу арасында, сондай-ақ алкоголь тұтыну арасында жақсы корреляция байқалады ($r=0.1$). Бұл алкогольді көп тұтыну мен шылым шегу қан қысымының жоғарылауымен байланысты болуы мүмкін екенін көрсетеді. Яғни, адам неғұрлым көп алкоголь тұтынса және шылым шексе, оның қан қысымы соғұрлым жоғары болады (4-сурет).

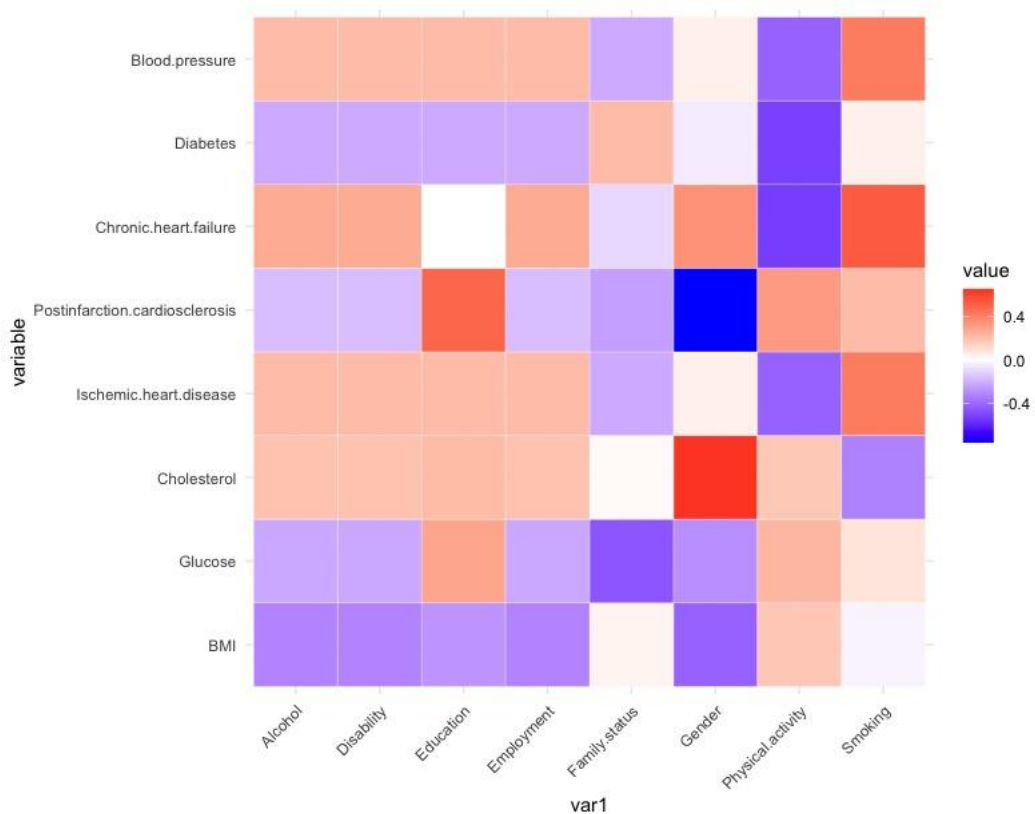


4 сурет – Қан қысымы мен шылым шегу арасындағы корреляция графигі

Біздің зерттеуімізде коронарлық жүрек ауруы мен созылмалы жүрек жеткіліксіздігі де алкогольмен оң байланыс көрсетеді ($r=0.1$). Нәтижелеріміз созылмалы жүрек жеткіліксіздігі деңгейі мен алкогольді тұтыну арасында статистикалық маңызды оң байланыс бар деген болжамды қолдайды, яғни алкогольді көп тұтыну созылмалы жүрек жеткіліксіздігінің даму немесе өршу қаупінің жоғарылауымен байланысты. Сонымен қатар, коронарлық жүрек ауруының пациенттің білім деңгейімен байланысы жоқ екені және қант диабеті (ҚД) шылым шегу және алкоголь сияқты жаман әдеттермен байланысты емес екені байқалды ($r=0$). Сондай-ақ, осы топта инфаркттан кейінгі кардиосклероз бен жыныс арасындағы кері байланыс сақталатынын атап өтуге болады.

Деректерді талдау нәтижелері глюкоза деңгейі мен білім деңгейі арасында қызықты корреляцияны көрсетті. Нәтижелер білім деңгейі қан глюкозасының деңгейіне әсер ететінін және қант диабеті мен басқа да метаболикалық аурулардың даму қаупін бағалағанда әлеуметтік-экономикалық факторларды ескеру қажеттігін көрсетеді. Бұл қорытындылар 75-89 жас аралығындағы зерттеу қатысушыларынан жиналған деректерге негізделген.

Жас шамасының денсаулыққа әсері туралы талқылауымызды жалғастыра отырып, үлкен жас тобын (90+) қарастырайық және осы категорияда қандай факторлар негізгі рөл атқаратынын қарастырайық. Біз корреляция коэффициенті -0.4 -тен 0.4 -ке дейін өзгеруі мүмкін екенін анықтадық, бұл айнымалылар арасындағы байланыстың күші мен бағытын көрсетеді. Нәтижелер төменде көрсетілген.



5 сурет – 90 жастан асқан топ үшін негізгі нәтижелер

Алынған деректерді талдай отырып, біздің зерттеуіміз жалпы холестерин деңгейі мен жыныс арасындағы қызықты нәтижелерді анықтады ($r=0.4$). Жалпы холестерин деңгейі мен әйел жынысы арасында оң корреляция байқалды, бұл холестерин деңгейі жоғары әйелдердің жүрек-қантaмыр ауруларының даму қаупінің артуы мүмкін екенін көрсетеді. Бұл нәтиже жүрек-қантaмырлық қауіп факторларын бағалауда және алдын алу мен емдеуге жеке көзқарас ұсынуда жыныстық айырмашылықтарды ескеру қажеттігін көрсетеді.

Айта кететін жайт, осы жас категориясында, сондай-ақ алдыңғы категорияларда инфаркттан кейінгі кардиосклероз бен жыныс арасындағы кері корреляция сақталады ($r=-0.4$). Сондай-ақ, зерттеу шылым шегу мен созылмалы жүрек жеткіліксіздігінің даму қаупі арасында айтарлықтай оң корреляцияны анықтады ($r=0.3$). Шылым шегетін адамдарда СЖЖ (созылмалы жүрек жеткіліксіздігі) даму немесе асқыну қаупі шылым шекпейтіндерге қарағанда жоғары. Бұл шылым шегудің жүрек-қантaмыр денсаулығына тигізетін ауыр зардаптарын және жүрек ауруларының алдын алу үшін темекі эпидемиясын бақылаудың маңыздылығын көрсетеді.

Зерттеуімізде білім деңгейі мен созылмалы жүрек жеткіліксіздігінің болуы арасында статистикалық маңызды байланыс анықталмады ($r=0$). Бұл нәтиже біздің үлгімізде СЖЖ даму қаупін бағалауда білім деңгейі маңызды фактор емес екенін көрсетуі мүмкін. Сондай-ақ, біздің зерттеуде жалпы холестерин деңгейі мен отбасылық жағдай арасында маңызды байланыс анықталған жоқ ($r=0$). Бұл нәтиже біздің зерттеудегі қатысушылардың холестерин деңгейіне отбасылық жағдайдың ықпалының жоқтығын көрсетеді.

Алайда, физикалық белсенділік пен қант диабеті, созылмалы жүрек жеткіліксіздігі деңгейі мен қан қысымы арасында орташа кері байланыс анықталды ($r=-0.3$). Бұл нәтижелер жүрек-қантaмыр ауруларының алдын алу мен емдеуге арналған ұсыныстарға физикалық белсенділікті қосу қажеттілігін және халық денсаулығын сақтау үшін салауатты өмір салтының маңыздылығын қолдайды. Бұл қорытындылар 90 жастан асқан зерттеу қатысушыларынан жиналған деректерді талдау нәтижелеріне негізделген. Осы бірегей жас

тобын таңдау егде жаста ұзақ өмір сүру мен өмір сапасына әсер ететін факторларды тереңірек түсінуге мүмкіндік береді.

Соңғы онжылдықтардағы әлемдегі демографиялық үрдістер егде жастағы пациенттердің мәселесін айқын көрсетті. Халықтың жас құрамы егде және қарт адамдардың басым болуына қарай өзгеруде. Қазіргі уақытта әлем халқының 10%-дан астамын егде жастағы адамдар құрайды. Жақын арада бұл көрсеткіш 30%-ға дейін өседі деп болжануда. Қазіргі таңда терапевтік көмекке жүгінетіндердің шамамен 90%-ын егде және қарт адамдар құрайды. Олардың көпшілігі артериялық гипертензия, бас және мойынның негізгі артерияларының атеросклерозы, ишемиялық жүрек ауруы сияқты жүрек-қантамыр ауруларына шалдығуда. Бүгінгі күні егде жастағы адамдарда жүрек-қантамырлық оқиғалар қаупі мен қартаюға әсер ету бойынша ауқымды заманауи клиникалық зерттеулер жеткіліксіз.

Осылайша, бағдарламалау арқылы жүргізілген зерттеуіміз егде жастағы топта шылым шегу мен коронарлық жүрек ауруы (КЖА), инфаркттан кейінгі кардиосклероз (ИКС) арасында айтарлықтай корреляцияны анықтады. Шылым шегу ЖҚА (жүрек-қантамыр аурулары) және оның асқынуларының даму қаупін арттырып, қартаюға да әсер етеді. Шылым шегу кез келген жаста және жыныста ЖҚА даму қаупін арттырады [28,29,30]. Көптеген зерттеулерге сүйене отырып, авторлар барлық жас топтарындағы шылым шегушілер арасында КЖА және ИКС жағдайларының көпшілігі шылым шегумен байланысты деген қорытындыға келді, бұл қазіргі уақытта қолжетімді басқа клиникалық зерттеулердің нәтижелерімен сәйкес келеді. Егде жастағы топта қан қысымы мен шылым шегу, алкоголь тұтыну арасында жақсы корреляция анықталды. Сондай-ақ, біздің зерттеуімізде алкоголь тұтынудың ИБС және ЖҚА дамуына әсері ($r=0.1$) көрсетілді. Көптеген зерттеулер ұзақ уақыт бойы күнделікті алкоголь тұтыну коронарлық жүрек ауруы, артериялық гипертензия, ишемиялық және геморрагиялық инсульттер, жүрекшелер фибрилляциясының дамуымен байланысты екенін дәлелдеді. Дегенмен, "Алкоголь тұтыну мен белгілі бір жүрек-қантамыр ауруларының нәтижелері арасындағы байланыс: жүйелі шолу және мета-анализ" сияқты кейбір зерттеулер алкогольдің ЖҚА дамуына алдын алу әсері бар екенін көрсетті. Осылайша, ЖҚА дамуына алкоголь тұтынудың әсерін одан әрі зерттеу қажет.

90 жастан асқан адамдарды бағалаған кезде шылым шегу мен созылмалы жүрек жеткіліксіздігінің даму қаупі арасында айтарлықтай оң корреляция анықталды, сондай-ақ қант диабеті, ЖҚА және АГ (артериялық гипертензия) ағымына төмен физикалық белсенділіктің әсері табылды.

Қорытынды.

Осылайша, біз 65-74 жас, 75-89 жас және 90 жастан асқан жас топтары бойынша клиникалық деректер (биомаркерлер) мен пациенттің әлеуметтік өмірі арасындағы корреляцияларды дәстүрлі машиналық оқыту классификаторларымен үйлестіріп есептей алдық. Бұл нәтижелер жүрек-қантамыр ауруларының алдын алу үшін барлық жас топтарында физикалық белсенділіктің маңыздылығын көрсетеді. Тұрақты дене жаттығулары денсаулықты сақтап, осы аурулардың даму қаупін азайтудың тиімді тәсілі болады.

Нәтижелер көрсеткендей, осы жас топтарының әрқайсысы өзіне тән ерекшеліктер мен қажеттіліктерге ие, сондықтан олардың әл-ауқатын қолдау және жақсарту үшін жеке тәсілдерді әзірлеу маңызды. Сондай-ақ таңдалған екі математикалық модельді (1)-(3) болашақтағы осыған ұқсас зерттеулер үшін эксперимент ретінде қарастыруға болады, себебі олардың нәтижелері бір-біріне өте жақсы сәйкес келеді.

Бұл саладағы одан әрі зерттеулер ересек және егде жаста белсенді әрі салауатты өмірді ұзартудың тиімді стратегияларын анықтауға көмектесуі мүмкін.

Әдебиеттер тізімі

1. United Nations, Department of Economic and Social Affairs, Population Division. (2022). *World population prospects 2022: Summary of results*. New York.
2. World Health Organization. (2020). *WHO fact sheet: Physical activity*. Geneva: World Health Organization.
3. Paskaleva, T., Tornyoova, B., Dragusheva, S., & Petleshkova, P. (2019). Modifiable risk factors for premature aging. *Biomedical Research*, 30(3), 426–431.
4. Pristrom, M. S., Pristrom, S. L., & Semenenkov, I. I. (2017). Starenie fiziologicheskoe i prezhdvremennoe. Sovremenniy vzglyad na problemu [Physiological and premature aging: A modern view of the problem]. *Mezhdunarodnye obzory: klinicheskaya praktika i zdorov'ye*, 5–6.
5. World Heart Federation. (2023). *World heart report 2023: Confronting the world's number one killer*. Geneva, Switzerland.
6. Lindstrom, M., De Cleene, N., Dorsey, H., et al. (2022). Global burden of cardiovascular diseases and risks collaboration, 1990–2021. *Journal of the American College of Cardiology*, 80(25), 2372–2425.
7. National Health Service. (n.d.). Ischaemic heart disease (coronary heart disease). Retrieved from <https://www.nhs.uk/conditions/coronary-heart-disease/>
8. Chazova, I. E. (2014). Rasprostranennost' faktorov riska serdechno–sosudistyykh zabolevaniy v Rossiiskoi populyatsii bol'nykh AG [Prevalence of cardiovascular risk factors in the Russian hypertensive population]. *Kardiologiya*, 54(10), 4–6.
9. Medlinks.ru. (2013). *Serdechno-sosudistyye zabolevaniya, krupnaya epidemiya XXI veka* [Cardiovascular diseases, a major epidemic of the 21st century]. Retrieved from <http://www.medlinks.ru/article>
10. Russian Society of Cardiology. (2018). Cardiovascular prevention 2017: National guidelines. *Russian Journal of Cardiology*, (6), 7–122.
11. Ageeva, E. S., & Berseneva, O. A. (2014). The role of risk factors in assessing the development of cardiovascular diseases. *Bulletin of Khakass State University*, 8, 6–9.
12. Aleksandrov, A. A., Rozanov, V. B., Zvolinskaya, E. Yu., & Pugoeva, Kh. S. (2016). The frequency of risk factors and the likelihood of developing fatal cardiovascular diseases among men aged 42–44 years. *Cardiovascular Therapy and Prevention*, 15(4), 38–43.
13. World Health Organization. (2023). *The global burden of disease: 2004 update*. Geneva: WHO.
14. Crea, F., Battipaglia, I., & Andreotti, F. (2015). Sex differences in mechanisms, presentation and management of ischaemic heart disease. *Atherosclerosis*, 241(1), 157–168. <https://doi.org/10.1016/j.atherosclerosis.2015.04.802>
15. Gökler, M. E., Buğrul, N., Metintaş, S., & Kalyoncu, C. (2015). Adolescent obesity and associated cardiovascular risk factors of rural and urban life (Eskisehir, Turkey). *Central European Journal of Public Health*, 23(1), 20–25.
16. Drapkina, O. M., & Shepel, R. N. (2015). Gipodinamia – bolezni veka: nizkaya fizicheskaya aktivnost' kak faktor riska [Hypodynamia as a risk factor for cardiovascular diseases and premature aging]. *Kardiologiya: novosti, mneniya, obuchenie*, (3).
17. World Health Organization. (2014). *Physical inactivity: A global public health problem*. Retrieved July 23, 2014, from http://www.who.int/dietphysicalactivity/factsheet_inactivity/en/index.html
18. Mendis, S., Puska, P., & Norrving, B. (Eds.). (2011). *Global atlas on cardiovascular disease prevention and control*. Geneva: World Health Organization, World Heart Federation, & World Stroke Organization.
19. Huxley, R., & Woodward, M. (2011). Cigarette smoking as a risk factor for coronary heart disease in women compared with men: A systematic review and meta-analysis of prospective cohort studies. *The Lancet*, 378(9799), 1297–1309.

20. World Heart Federation. (2022). *No amount of alcohol is good for the heart*. Retrieved from <https://world-heart-federation.org/news/no-amount-of-alcohol-is-good-for-the-heart-says-world-heart-federation>
21. Evdokimov, I. V., Kovalenko, M. A., & Melekh, D. A. (2017). Upravlenie razrabotkoi i vnedreniem uchetnoy informatsionnoy sistemy [Management of development and implementation of an information system]. *Nauchnoe Obozrenie: Ekonomicheskie Nauki*, (4), 34–39.
22. Serdyukov, A. G., Naberezhnaya, I. B., & Zakharov, D. A. (2008). Sotsiologicheskoe obosnovanie vnedreniya telemeditsinskikh tekhnologii v praktiku [Sociological justification of telemedicine technologies]. *Zamestitel' glavnogo vracha*, (2), 12–20.
23. Fayzrakhmanov, A., et al. (2020). Mashinnoe obuchenie v meditsine: evolyutsiya i perspektivy [Machine learning in medicine: evolution and perspectives].
24. Bursov, A. I. (2019). Primenenie iskusstvennogo intellekta dlya analiza meditsinskikh dannykh [Application of artificial intelligence for medical data analysis]. *Al'manakh klinicheskoi meditsiny*, 47(7), 630–633. Retrieved from <https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-dlya-analiza-meditsinskih-dannykh>
25. Gusev, A. V., et al. (2021). Mashinnoe obuchenie na laboratornykh dannykh dlya prognozirovaniya zabolevaniy [Machine learning on laboratory data for disease prediction]. *Farmakoekonomika. Sovremennaya farmakoekonomika i farmakoepidemiologiya*, 14(4), 581–592.

ИСПОЛЬЗОВАНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПРИЗНАКОВ ПРЕЖДЕВРЕМЕННОГО СТАРЕНИЯ

Аннотация. *Преждевременное патологическое старение чаще всего связано с сердечно-сосудистыми заболеваниями, которые возникают из-за совокупности социально-экономических, метаболических, поведенческих и экологических факторов риска. Эти факторы включают гендерные различия, возраст, высокое кровяное давление, ожирение, низкую физическую активность, курение, чрезмерное употребление алкоголя, повышенные уровни холестерина и глюкозы, а также сахарный диабет. Все процессы в организме человека отражаются в биохимических и иммунологических анализах, которые могут быть маркерами преждевременного старения сердечно-сосудистой системы.*

Авторы исследовали связи между социальными факторами, такими как уровень образования, работа, пол, семейное положение, инвалидность, физическая активность, курение и употребление алкоголя, и клиническими показателями, такими как ишемическая болезнь сердца (ИБС), постинфарктный кардиосклероз (ПИКС), хроническая сердечная недостаточность (ХСН), сахарный диабет (СД), индекс массы тела (ИМТ), уровень глюкозы, общий холестерин (ОХ) и артериальное давление (АД). Кроме того, была выявлена корреляция между клиническими данными (биомаркерами) и социальными аспектами жизни пациентов в возрастных группах 65-74 года, 75-89 лет и старше 90 лет.

Ключевые слова: *Искусственный интеллект, машинное обучение, маркеры преждевременного старения, сердечно-сосудистые заболевания, иммунное старение, прогнозирование.*

USING MACHINE LEARNING TO IDENTIFY SIGNS OF PREMATURE AGING

Abstract. *Premature pathological aging is often associated with cardiovascular diseases, which result from a combination of socio-economic, metabolic, behavioral, and environmental risk factors. These factors include gender differences, age, high blood pressure, obesity, low physical activity, smoking, excessive alcohol consumption, elevated cholesterol and glucose levels, and diabetes. All processes in the human body are reflected in biochemical and immunological analyses, which can serve as markers of premature aging of the cardiovascular system.*

The authors studied the relationships between social factors such as education, employment, gender, marital status, disability, physical activity, smoking, and alcohol consumption, and clinical indicators such as ischemic heart disease (IHD), post-infarction atherosclerosis (PICS), chronic heart failure (CHF), diabetes mellitus (DM), body mass index (BMI), glucose level, total cholesterol (TC), and blood pressure (BP). Additionally, correlations were identified between the clinical data (biomarkers) and the social life of patients aged 65–74 years, 75–89 years, and over 90 years.

Keywords: *artificial intelligence, machine learning, premature aging markers, cardiovascular diseases, immune aging, forecasting.*

Авторлар туралы мәлімет

Сулейменова Мадина Утегеновна	Әл-Фараби атындағы Қазақ ұлттық университеті, докторант E-mail: madekin940@gmail.com
Абзалиев Қуат Баяндыевич	Әл-Фараби атындағы Қазақ ұлттық университеті, профессор E-mail: abzaliyev_kuat@mail.ru
Абзалиева Сымбат Абулхайровна	Әл-Фараби атындағы Қазақ ұлттық университеті, профессор E-mail: abzaliyeva.symbat@gmail.com
Мұхаммеджанова Динаргүл Мұратбекқызы	Әл-Фараби атындағы Қазақ ұлттық университеті, докторант E-mail: m.dinargul.14@gmail.com

Сведение об авторах

Сулейменова Мадина Утегеновна	Казахский Национальный Университет имени Аль-Фараби, докторант, E-mail: madekin940@gmail.com
Абзалиев Қуат Баяндыевич	Әл-Фараби атындағы Қазақ ұлттық университеті, профессор E-mail: abzaliyev_kuat@mail.ru
Абзалиева Сымбат Абулхайровна	Әл-Фараби атындағы Қазақ ұлттық университеті, профессор E-mail: abzaliyeva.symbat@gmail.com
Мухаммеджанова Динаргүл Мұратбековна	Казахский Национальный Университет имени Аль-Фараби, докторант, E-mail: m.dinargul.14@gmail.com

Information about the authors

Suleimenova Madina Utegenovna	Farabi University, doctoral student, E-mail: madekin940@gmail.com
Abzaliyev Kuat Bayandiyevich	Farabi University, professor, E-mail: abzaliyev_kuat@mail.ru
Abzaliyeva Symbat Abulkhaironva	Farabi University, professor, E-mail: abzaliyeva.symbat@gmail.com
Mukhammejanova Dinargul Muratbekkyzy	Farabi University, doctoral student, E-mail: m.dinargul.14@gmail.com



УДК 004.9

МРНТИ 20.01.01

https://doi.org/10.53364/24138614_2025_38_3_17

Р. Оспанов¹, Е. Сейткулов¹, Н. Ташатов¹, Б. Ергалиева¹, К. Утебаев²

¹Евразийский национальный университет им. Л.Н.Гумилева,
Астана, Казахстан

²Филиал Национального исследовательского ядерного университета «МИФИ»,
Алматы, Казахстан

*E-mail: ergalieva_banu@mail.ru

ВЫБОР ОПТИМАЛЬНЫХ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПРОТОКОЛА КОНСЕНСУСА В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Задача выбора оптимальных механизмов консенсуса блокчейна в сетях Интернета вещей может быть рассмотрена как задача многокритериального принятия решений. Целью данной работы является определение наиболее подходящего метода многокритериального принятия решений в рамках этой задачи. В настоящее время существует множество различных методов многокритериального анализа. Кроме того, появляются новые методы, а уже существующие продолжают развиваться. В таких условиях представляется очень важным правильно определить наиболее подходящий метод многокритериального принятия решений для рассматриваемой задачи. Предполагается, что такой правильный выбор даст большую уверенность в объективности и точности при оценке и принятии решений. Это также существенно, учитывая, что рассматриваемая задача характеризуется большим количеством альтернатив (множество различных протоколов консенсуса) и большим количеством критериев (например, энергопотребление, пропускная способность, устойчивость к атакам, задержка обработки транзакций и т.п.). В настоящее время существуют открытые программные инструменты, предназначенные для автоматизации процесса выбора наиболее подходящих методов многокритериального принятия решений. Такие системы поддержки принятия решений помогают аналитикам и исследователям в различных сферах применения многокритериального анализа. В данной работе представлен подход к выбору оптимальных методов многокритериального принятия решений, основанный на применении такого специализированного программного обеспечения в случае задачи выбора оптимального механизма консенсуса для IoT. Как результат, были выбраны известные методы TOPSIS, VIKOR, а также их интервальные и нечеткие модификации. Дополнительно, для взвешивания критериев был выбран метод аналитической иерархии (АИР). Практическим применением этого результата стала разработка системы выбора оптимального протокола консенсуса для сетей Интернета вещей на основе блокчейна, а также соответствующей программной реализации на языке Python.

Ключевые слова: технологии распределенного реестра, блокчейн, протокол консенсуса, Интернет вещей, методы многокритериального принятия решений.

Введение.

Как известно к сетям Интернета вещей (IoT) предъявляются различные высокие требования (ограничения на вычислительные ресурсы, высокая динамичность сетевых узлов, необходимость обеспечения безопасности при хранении и передаче данных и т.п.). Это следует учитывать при решении задачи выборе оптимальных механизмов консенсуса, применяемых в технологиях распределенных реестров, в сетях Интернета вещей. Таким образом, это весьма сложная и комплексная задача, при решении которой необходимо учитывать множество разнообразных и зачастую противоречивых критериев, таких как, например, устойчивость к атакам, задержка обработки транзакций, энергопотребление, пропускная способность и т.п. В таких сложных условиях методы многокритериального принятия решений могут помочь в поиске и оценке возможных альтернатив решения в подобных задачах. Применение таких методов может помочь в решении задачи выбора наиболее подходящего протокола консенсуса.

Целью данной работы является выбор наиболее подходящего метода многокритериального принятия решений для определения оптимального консенсусного механизма для сетей Интернета вещей, основанных на применении технологий распределенного реестра. Ранее в работах [1], [2] были рассмотрены первоначальные этапы этой задачи, заключающиеся в составлении набора альтернатив, и далее набора критериев для оценивания альтернатив. Для достижения поставленной цели данной работы был избран подход, состоящий в применении специализированного программного обеспечения. В настоящее время существуют специализированные инструменты MCDA Methods Selection Software (MCDA-MSS) [3] и WEighting Methods Selection Software (WEMSS) [4], которые автоматизируют процесс выбора оптимального метода. С помощью этих программ можно подобрать наиболее подходящие методы для выбора протокола консенсуса.

Материалы и методы.

Далее рассмотрим детально процесс работы с программой MCDA-MSS.

Для того чтобы определиться с тем, какой метод или, возможно, несколько методов многокритериального принятия решений подходит для рассматриваемой задачи, необходимо ответить на ряд вопросов, состоящий из четырех групп. Каждый вопрос имеет несколько вариантов ответов, в том числе и ответ «не знаю» (т.е. допускается, что пользователь может и не знать на момент работы с инструментом как ответить на вопрос). К вопросам и ответам имеются поясняющие их смысл описания. При выборе ответов на часть вопросов или на все вопросы автоматически появляется список методов, которые система рекомендует для рассматриваемой задачи. Причем для каждого метода дается описание со списком соответствующих этому методу ответов на вопросы. Выбранные ответы будут выделены жирным шрифтом.

Первая группа вопросов называется «Формулировка проблемы». Ответы на них помогают определиться, к какому типу относится рассматриваемая задача, и какую структуру она имеет.

Первый вопрос группы помогает определиться с типом рекомендации по решению задачи, рассматриваемой пользователем системы. Доступны следующие ответы: «ранжирование», «сортировка», «кластеризация», «выбор». Тип «ранжирование» означает, что рассматриваемые альтернативы упорядочиваются от наиболее предпочтительной альтернативы к наименее предпочтительной. Тип «сортировка» означает, что выполняется назначение альтернатив предопределенным классам предпочтений (от наиболее предпочтительной альтернативы к наименее предпочтительной). Тип «кластеризация» означает, что выполняется разделение альтернатив на группы в соответствии с некоторой мерой подобию или отношением предпочтения. Тип «выбор» означает, что выполняется выбор наиболее предпочтительного подмножества альтернатив.

К каждому из этих вариантов системой предлагаются дополнительные вопросы. Так, например, в случае выбора «ранжирования» пользователю предлагается ответить на два дополнительных вопроса. В одном из них выясняется, какой порядок альтернатив запрашивается: «частичный» или «полный». «Частичный» порядок допускает отношение несравнимости, это имеет преимущество в том, что выделяет альтернативы, которые значительно отличаются друг от друга. А в случае «полного» порядка все альтернативы упорядочены от лучших к худшим, без какой-либо возможности несравнимости. В следующем вопросе выясняется, какая шкала, ведущая к рекомендации, запрашивается: «порядковая» или «количественная». При «порядковой» шкале рекомендация основана на бинарных отношениях, где только порядок альтернатив имеет значение. При «количественной» шкале окончательная рекомендация обусловлена оценкой, где расстояния между оценками всех альтернатив имеют количественное значение.

В случае выбора «сортировки» пользователю предлагаются три дополнительных вопроса. В одном из них выясняется, какой порядок классов запрашивается: «частичный» или «полный». В случае «частичного» порядка допускается отношение несравнимости между классами принятия решений, это имеет преимущество в том, чтобы выделить классы, которые значительно отличаются друг от друга. При «полном» порядке все классы упорядочены от лучшего класса к худшему, без какой-либо возможности несравнимости. В следующем вопросе выясняется, какая шкала, ведущая к рекомендации, запрашивается: «порядковая» (рекомендация основана на бинарных отношениях, где только задание классов альтернатив имеет значение) или «количественная» (окончательная рекомендация обусловлена оценкой, где расстояния между оценками всех альтернатив имеют количественное значение). И в третьем вопросе определяется, какая требуется мощность классов: «с ограничениями» (в этом случае учитываются ограничения на количество альтернатив, которые могут быть заданы в каждом классе) или «без ограничений» (не включает ограничения на количество альтернатив, которые могут быть заданы в каждом классе).

В случае выбора «кластеризации» появляется еще один дополнительный вопрос, в котором определяется, какой требуется тип кластеризации: «неупорядоченные кластеры» или «упорядоченные кластеры». Первый тип означает, что альтернативы группируются на основе парных отношений предпочтений без установления порядка в результирующих кластерах. Второй тип означает, что альтернативы группируются на основе парных отношений предпочтений с установлением порядка в полученных кластерах.

Для типа «выбор» появляется дополнительный вопрос, в котором определяется, какая требуется мощность альтернатив: «с ограничениями» (в этом случае учитываются ограничения на количество выбираемых альтернатив) или «без ограничений» (не включает ограничения на количество выбираемых альтернатив).

Следующий вопрос после вопроса о типе рекомендации по решению – это вопрос о характере набора альтернатив. Доступны следующие варианты: «стабильный» и «возрастающий». Вариант «стабильный» означает, что новых альтернатив не предвидится и не добавляется в набор, а второй вариант означает, что новые альтернативы продолжают появляться по мере развития контекста принятия решения.

В следующем вопросе группы определяется, какова структура используемых для оценки критериев. Доступные варианты ответов: «плоская» и «иерархическая» структуры. «Плоская» структура означает, что все критерии находятся на одном уровне. «Иерархическая» структура означает, что критерии организованы по уровням, иерархически, от общих критериев до детализированных.

Далее следует вопрос, с помощью которого пользователь может определиться с типом характеристик критериев: «детерминированный» или «неопределенный». Тип «детерминированный» означает, что входные данные являются точными. В случае выбора этого ответа появляется еще один дополнительный вопрос, в котором определяется тип

детерминированных характеристик: «за альтернативу» (это относится к характеристикам альтернативы по критерию) или «сравнение относительной характеристики» (это относится к характеристикам альтернативы по критерию относительно характеристик другой альтернативы по тому же критерию). Тип «неопределенный» означает, что входные данные не являются точными. В случае выбора этого ответа появляется еще один дополнительный вопрос, в котором определяется тип неопределенных характеристик. Аналогично предыдущему вопросу доступны варианты «за альтернативу» и «сравнение относительной характеристики».

В следующем вопросе определяется, каково знание предпочтения для значений каждого критерия. Варианты: «известно» или «следует обнаружить». Первый вариант означает, что порядок предпочтения известен. Второй вариант означает, что порядок предпочтения относительно характеристик неизвестен и должен быть обнаружен. Если знание предпочтения для значений каждого критерия является «известным», то пользователю предлагается определить тип известного порядка предпочтения для критериев: «монотонный» или «немонотонный». «Монотонный» порядок определяется как постоянно неубывающий или невозрастающий по отношению к предпочтениям по критериям. «Немонотонный» порядок определяется как неубывающий или невозрастающий в разных областях шкалы характеристик в отношении предпочтений по критериям.

Наконец последний вопрос первой группы предназначен для определения статуса полноты набора критериев. Статус может быть определен как «полный» или «неполный». В первом случае все критерии, имеющие отношение к рассматриваемой задаче и имеющие влияние на рекомендацию, определены на этапе моделирования проблемы и включены в набор критериев. Во втором случае, по крайней мере, один критерий, имеющий отношение к рассматриваемой задаче и имеющий потенциальное влияние на рекомендацию, не включен в набор критериев.

На следующем рисунке показана часть интерфейса с вопросами первой группы (Рис.1).

Section 1: Here you can define how the problem is framed by (i) choosing the type of decision-making challenge under consideration and (ii) describing the criteria used to assess the alternatives.		
Problem statement What type of decision recommendation is requested?	I don't know ▾	(117)
Set of alternatives What is the nature of the problem in relation to the alternatives that constitute the set?	I don't know ▾	(205)
Criteria structure What is the structure of the criteria used for the assessment?	I don't know ▾	(204)
Evaluation of alternatives on the criteria What is the type of performance of the criteria?	I don't know ▾	(204)

Рисунок 1 – MCDA-MSS: часть интерфейса с вопросами первой группы

Вторая группа вопросов называется «Модель предпочтений». С помощью них можно выяснить, какой тип модели следует применить к рассматриваемой задаче.

С помощью первого вопроса этой группы пользователь системы может определиться с тем, каким образом входная информация/данные о характеристиках должны использоваться искомым методом или методами. Доступны следующие ответы: «качественно», «количественно» и «относительно».

В случае варианта «качественно» рассматривается только порядок характеристик. При выборе этого варианта возможен выбор типа метода на основе качественных характеристик: «основанный на характеристиках» (при оценке качества характеристик, назначенных отдельным альтернативам, рассматривается только их порядок без интерпретации различий или соотношений характеристик) или «основанный на парных сравнениях» (сравниваются характеристики альтернатив в паре, интерпретируя только их порядок относительно их качества).

Во втором варианте для выражения силы предпочтения используются различия между характеристиками. При выборе этого варианта возможен выбор типа метода на основе количественных характеристик: «линейный», «кусочно-линейный» или «нелинейный». В случае «линейного» типа применяется линейная функция для определения того, насколько предпочтительны различные характеристики по критериям. В случае «кусочно-линейного» типа применяется кусочно-линейная функция (с линейной интерполяцией между контрольными точками) для определения того, насколько предпочтительны различные характеристики по критериям. В случае «нелинейного» типа применяется произвольно нелинейная функция для определения того, насколько предпочтительны различные характеристики по критериям.

При варианте «относительно» для выражения силы предпочтения используются относительные сравнения характеристик. При выборе этого варианта возможен выбор типа метода на основе сравнений: «порядковый» (относительные сравнения характеристик используются для выражения интенсивности предпочтений в порядковых терминах) или «относительный» (относительные сравнения характеристик используются для выражения интенсивности предпочтений в терминах отношения).

На следующем рисунке показана часть интерфейса с вопросами второй группы (Рис.2).

Section 2: Here you can define what type of model you would like to apply, accounting for (i) how the input data is used by the method, (ii) comparison of criteria performances, (iii) compensation between the criteria performances, (iv) aggregation of the criteria evaluations, and (v) the capacity of the MCDA methods to deal with inconsistent preference information.

Scale used by the method(s)
How should the input information/performance data be used by the method(s)?

Qualitative-based method(s) type
What type of method that only considers the qualitative information from the criteria performances should be selected?

Comparison of performances
How should the comparison of the performances on the criteria be performed?

qualitatively ▾	(129)
<input type="checkbox"/> I don't know (205)	
<input checked="" type="checkbox"/> qualitatively (129)	(83)
<input type="checkbox"/> quantitatively (93)	
<input type="checkbox"/> relatively (1)	
I don't know ▾	(89)

Рисунок 2 – MCDA-MSS: часть интерфейса с вопросами второй группы

В следующем вопросе группы рассматривается сравнение характеристик. Пользователь может выбрать следующие ответы:

1) показатели преобразуются с помощью подхода нормализации на основе данных, а затем сравниваются (в этом случае показатели по всем критериям приводятся к одинаковой шкале перед агрегацией с помощью метода нормализации на основе данных);

2) показатели сравниваются лицом, принимающим решение, относительно градуированной силы предпочтения (в этом случае сравнения выполняются лицом, принимающим решение, который должен выбрать одно значение из шкалы, которая заранее определена);

3) показатели сравниваются лицом, принимающим решение, относительно неградуированной силы предпочтения (в этом случае сравнения выполняются лицом, принимающим решение, чья сила предпочтения не определена заранее в наборе значений);

4) сырые характеристики сравниваются напрямую (в этом случае показатели сравниваются лицом, принимающим решение, относительно неоцененной силы предпочтения).

Следующий вопрос касается весов критериев. Пользователь системы может определить, следует ли использовать веса критериев для дифференциации роли критериев в процедуре агрегации, ведущей к окончательной рекомендации по решению. Пользователь может дать положительный или отрицательный ответ.

В следующем вопросе выясняется, следует ли использовать пороги парного сравнения по каждому критерию для моделирования несовершенного знания характеристик критериев и/или для характеристики чувствительности предпочтений лица, принимающего решение, при сравнении двух альтернатив по одному критерию. Пользователь также может дать положительный или отрицательный ответ. Положительный ответ означает, что используются пороговые значения в сравнениях альтернатив по критериям для выражения различий в показателях, которые имеют значение для безразличия и предпочтения, или можно наложить вето на всеобъемлющее отношение предпочтения. Отрицательный ответ означает, что использование пороговых значений в показателях при сравнении альтернатив по критериям не требуется, поскольку каждая ненулевая разница показателей означает предпочтение для лица, принимающего решение.

Следующий вопрос касается взаимодействия между критериями. Определяется, следует ли рассматривать взаимодействия между критериями как отражение неаддитивной природы предпочтений. В случае положительного ответа показатели альтернатив по некоторым критериям влияют на восприятие лица, принимающего решение, ценности показателей по другим критериям, что означает, что эти два набора критериев являются преимущественно зависимыми. В отрицательном случае критерии являются преимущественно независимыми, что означает, что при построении комплексного отношения предпочтений значения показателей по отдельным критериям не зависят от показателей альтернатив по любому другому критерию.

Далее следует вопрос, следует ли использовать профили критериев, не соответствующие рассматриваемым альтернативам, для получения рекомендации по решению. В случае положительного ответа многокритериальные профили — это фиктивные альтернативы, с которыми сравниваются реальные альтернативы для разработки окончательной рекомендации по решению. В случае отрицательного ответа нет необходимости определять многокритериальные профили, служащие фиктивными альтернативами, с которыми сравниваются реальные альтернативы для разработки окончательной рекомендации по решению.

Следующий вопрос касается компенсации между критериями. Выясняется, в какой степени хорошая характеристика по критерию может компенсировать плохую характеристику по другому критерию. Доступны варианты: «никак», «частично» или «полностью». В случае первого варианта никакая хорошая характеристика по критерию не может компенсировать плохую характеристику по другому критерию. Второй вариант означает, что хорошая характеристика по критерию может частично компенсировать плохую характеристику по другому критерию. Третий означает, что хорошая характеристика по критерию может полностью компенсировать плохую характеристику по другому критерию.

В следующем вопросе, выясняется, можно ли агрегировать характеристики по стандартным методам для предоставления рекомендаций для принятия решения. Положительный ответ означает, что показатели по нескольким критериям суммируются с помощью метода для предоставления рекомендаций по решению. Отрицательный означает,

что показатели по нескольким критериям не суммируются с помощью метода для предоставления рекомендации по принятию решения.

В случае положительного ответа определяется тип агрегации оценок нескольких критериев, а именно, какой подход следует использовать для агрегации нескольких критериев для предоставления рекомендации по решению: «функция подсчета», «бинарные отношения» или «правила». При подходе «функция подсчета» функция, которая агрегирует отдельные показатели критериев, используется для определения общего качества каждой альтернативы; относится к методам, которые используют показатели по каждому критерию и агрегируют нормализованные данные для построения рекомендации по решению. В случае «бинарных отношений» попарные сравнения альтернатив используются для разработки комплексной оценки каждой альтернативы. При подходе «правила» показатели агрегируются с помощью правил принятия решений, обычно выражаемых в форме утверждений "если ..., то ...".

Следующий вопрос, должен ли метод многокритериального принятия решений быть способным обрабатывать несоответствующую информацию о предпочтениях: «да» (метод должен быть способен обрабатывать противоречивую информацию о предпочтениях) или «нет» (не обязательно, чтобы метод был способен обрабатывать противоречивую информацию о предпочтениях).

В случае положительного ответа возникает дополнительный вопрос о том, какой тип несоответствующей информации о предпочтениях должен быть способен обрабатывать метод: «только нарушение доминирования», «только другие типы несоответствий, не включая доминирование» или «нарушение доминирования и другие типы несоответствий». В первом случае обрабатываются несоответствия, подразумеваемые только нарушением отношения доминирования предпочтениями пользователя. Во втором случае обрабатываются несоответствия, подразумеваемые исключительно внутренне конфликтующими предпочтениями пользователя. В третьем случае обрабатываются несоответствия между предпочтениями пользователя и моделью предпочтений, не способной их воспроизвести (включая нарушение доминирования).

Третья группа вопросов называется «Выявление предпочтений». Вопросы этой группы предназначены для определения типа, модальности и частоты предпочтений модели.

На следующем рисунке показана часть интерфейса с вопросами третьей группы (Рис.3).

The screenshot shows a section titled "Section 3: Here you can define what type of preferences information you can provide, how and with what frequency." It contains three questions with corresponding dropdown menus and counts:

Question	Selected Option	Count
Type of preferences elicitation What type of preference information is provided?	direct	129
Specify criteria weights Do you want to specify the weights of the criteria?	direct (129)	86
Specify per-criterion pairwise comparison thresholds Do you want to specify the per-criterion pairwise comparison thresholds?	I don't know	86

Рисунок 3 – MCDA-MSS: часть интерфейса с вопросами третьей группы

В первом вопросе группы определяется, какой тип информации о предпочтениях предоставляется: «прямой» или «непрямой». Тип «прямой» означает, что параметры модели задаются непосредственно лицом, принимающим решение. Тип «непрямой» означает, что параметры модели выводятся на основе косвенных (локальных или целостных) суждений экспертов/лиц, принимающих решение.

В случае выбора первого типа появляется ряд дополнительных вопросов. Есть ли необходимость указывать веса критериев? И если да, то, какие типы весов использовать (точные или неточные)? Есть ли необходимость указывать пороги парного сравнения по каждому критерию? И если да, то какой тип порогов парного сравнения следует использовать? Есть ли необходимость указывать информацию о взаимодействиях критериев? И если да, то, какой тип взаимодействия следует обрабатывать? И есть ли необходимость указывать профили критериев?

Следующим вопросом группы определяется, с какой частотой предоставляется информация о предпочтениях: «разовая» (все предпочтения предоставляются в начале процесса выявления) или «возрастающая» (предпочтения предоставляются последовательно, в разных итерациях).

И последний вопрос определяет, включать ли уровень достоверности предпочтений при предоставлении параметров. И если да, то он может указать уровни достоверности (например, для назначения, например, «абсолютно уверен», «уверен», «слегка уверен»).

Последняя группа вопросов называется «Использование отношения предпочтений, заданного моделью предпочтений». Определяет стратегию, используемую для получения и улучшения рекомендаций по принятию решений. В последней группе изначально один вопрос, в котором следует выбрать один из двух следующих типов использования отношения предпочтения, заданного моделью предпочтения: «однозначная рекомендация» или «анализ изменчивости выходных данных». В первом варианте обеспечивается однозначный результат для выбранной формулировки проблемы. Второй вариант рассматривает, насколько изменчивой может быть рекомендация, когда есть неопределенность относительно производительности альтернатив и/или представления предпочтений лица, принимающего решение, предполагаемой моделью предпочтений.

В случае выбора первого варианта возникает еще один вопрос о типе использования модели предпочтений с однозначной рекомендацией. Возможны два варианта: однозначная рекомендация, основывающаяся на анализе изменчивости выходных данных, и однозначная рекомендация, не основывающаяся на анализе изменчивости выходных данных. Первый вариант означает, что предоставляется единая, точная рекомендация, при этом, все еще учитывая, насколько изменчивой может быть рекомендация, когда есть неопределенность относительно характеристик альтернатив и/или представления предпочтений лица, принимающего решение, предполагаемой моделью предпочтений. Второй вариант означает, что не учитывается, насколько изменчивой может быть рекомендация, когда есть неопределенность относительно производительности альтернатив и/или представления предпочтений лица, принимающего решение, предполагаемой моделью предпочтений.

После выбора каждого из этих вариантов системой предлагается выявить желаемый тип модели предпочтений для получения рекомендации по решению. При однозначной рекомендации, основывающейся на анализе изменчивости выходных данных возможны «компромиссный» и «репрезентативный» типы, а при однозначной рекомендации, не основывающейся на анализе изменчивости выходных данных – «одионый» (для получения рекомендации используется только одна модель) и «множественный» (для получения рекомендации используется несколько моделей).

В свою очередь при выборе «одионого» типа далее можно уточнить тип: «детерминированный» или «репрезентативный». Тип «детерминированный» означает, что экземпляр модели предпочтений с точными значениями параметров либо напрямую указывается лицом, принимающим решение, либо определяется методом (в последнем случае не существует других возможных экземпляров модели предпочтений). Тип «репрезентативный» означает, что экземпляр модели предпочтений с точными значениями параметров либо выбирается методом, либо напрямую выбирается лицом, принимающим решение, (в обоих случаях не существует других возможных экземпляров модели

предпочтений). Также в свою очередь «репрезентативный» тип может быть «алгоритмическим» или «с прямым участием». В первом случае метод выбирает один из многих возможных экземпляров модели предпочтений, используя некоторую predetermined procedure, правило или алгоритм. Во втором случае лицо, принимающее решение, выбирает один из многих возможных экземпляров модели предпочтений, используя интерактивное программное обеспечение.

В случае выбора типа «анализ изменчивости выходных данных» возникает вопрос о том, каким образом необходимо проводить анализ изменчивости выходных данных. Возможные варианты: «экстремальные результаты со всеми совместимыми моделями» и «распределение результатов с помощью выборки совместимых моделей». Первый вариант означает, что все совместимые экземпляры модели предпочтений рассматриваются с помощью методов математического программирования (т. е. необходимых/возможных отношений). Второй вариант означает, что выборка всех совместимых экземпляров модели предпочтений, полученных с помощью стохастического моделирования, например, Монте-Карло.

Таким образом, в результате получения ответов на вышеописанные вопросы пользователь может получить список рекомендуемых методов. Однако возможен случай, когда список будет пустой. В настоящее время база данных MCDA-MSS содержит более 205 методов многокритериального принятия решений и 156 ключевых характеристик принятия решений. MCDA-MSS может быть полезной для исследователей и практиков, работающих в области многокритериального принятия решений [5], [6], [7].

При работе с системой WEMSS пользователь аналогичным образом на ряд интерактивных вопросов, сгруппированных в три раздела. В результате получения ответов пользователь получает список рекомендуемых методов взвешивания. В настоящее время база данных WEMSS содержит 35 методов взвешивания и 50 ключевых характеристик принятия решений.

На следующем рисунке показана часть интерфейса WEMSS с вопросами первой группы (Рис.4).

Section 1: They shape the operational capabilities of the required method

Meaning of weights What meaning should the weights have?	I don't know ▾	(19)
Temporal discounting Should the method allow for the inclusion of discounting?	I don't know ▾	(35)
Cultural differentiations Should the method account for different cultural backgrounds of the affected population?	I don't know ▾	(35)

Рисунок 4 – WEMSS: часть интерфейса с вопросами первой группы

Результаты и обсуждение.

Проведенные исследования привели к следующим качественным результатам. В процессе работы с инструментом MCDA-MSS отвечая на предлагаемые системой вопросы, были определены основные характеристики, которым должен удовлетворять выбираемый метод многокритериального принятия решений. Весь процесс работы с системой имеет вид дерева вопросов с вариантами ответов (Рис.5.).

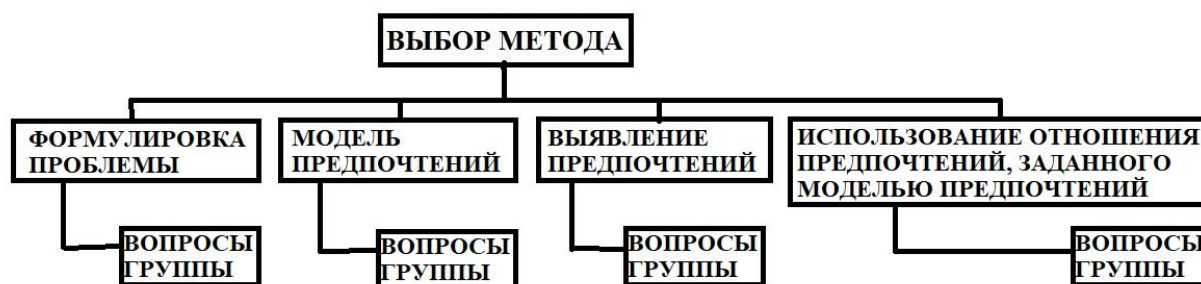


Рисунок 5 – Дерево вопросов системы MCDA-MSS

В итоге системой были предложены следующие варианты: TOPSIS [8], Fuzzy TOPSIS [9], TOPSIS interval [10], TOPSIS interval and fuzzy [11], VIKOR [12], Fuzzy VIKOR [13].

Метод TOPSIS (анг. Technique for Order of Preference by Similarity to Ideal Solution) является известным методом многокритериального принятия решений, который основан на вычислении расстояний между каждой альтернативой и идеальной альтернативой, а также между каждой альтернативой и анти-идеальной альтернативой. Метод VIKOR (серб. ViseKriterijumska Optimizacija I Kompromisno Resenje, означает «Многокритериальная оптимизация и компромиссное решение») – это также известный метод многокритериального принятия решений. В этом методе учитываются компромиссные решения. Он может быть полезен, когда имеется набор противоречивых критериев. Методы Fuzzy TOPSIS и Fuzzy VIKOR является расширением метода TOPSIS, и работает с нечеткими данными. Метод может применяться в том случае, когда критерии оцениваются с некоторой степенью неопределенности, т.е., например, вместо точных числовых значений указываются значения типа "низкое", "среднее", "высокое". Метод TOPSIS interval также является расширением метода TOPSIS, который работает с интервальными данными, т.е. когда оценки критериев выражены не точными числовыми значениями, а диапазонами возможных значений. Метод TOPSIS interval and fuzzy является более сложным расширением метода TOPSIS, который работает как с интервальными, так и нечеткими данными.

Таким образом, характер входных данных в рассматриваемой задаче многокритериального принятия решений влияет на окончательный выбор из предложенных системой MCDA-MSS методов. Если имеющиеся входные данные являются четкими и детерминированными, и необходимо найти альтернативу, ближайшую к идеальной альтернативе, то можно выбрать метод TOPSIS. Если входные данные являются четкими и детерминированными, и важно учитывать компромисс между критериями, то можно выбрать метод VIKOR. Если входные данные являются нечеткими, и требуется строгое упорядочивание критериев, то можно выбрать метод Fuzzy TOPSIS. Если входные данные являются нечеткими, и важны компромиссные решения, то можно выбрать метод Fuzzy VIKOR. Если данные являются интервальными, то можно выбрать метод TOPSIS interval. Если же данные включают как интервальные, так и нечеткие данные, то можно выбрать метод TOPSIS interval and fuzzy.

В процессе работы с инструментом WEMSS был определен оптимальный метод взвешивания критериев. В контексте данной задачи наилучшим выбором оказался метод аналитической иерархии (АИП, Analytic Hierarchy Process) [14].

Практическим применением и результатом проведенных исследований является то, что на основе выбранных оптимальных методов многокритериального принятия решений была разработана система выбора оптимального протокола консенсуса для сетей Интернета вещей, основанная на применении технологий распределенного реестра, а также соответствующая программная реализация на языке Python. Получено авторское свидетельство (Свидетельство об авторском праве, № 62332 от 23.09.2025 года).

Разработанный программный инструмент реализует следующий функционал. Инструмент предоставляет пользователю возможность выбрать:

- 1) Добавлять, редактировать и удалять в базу данных альтернативы (протоколы консенсуса), которые подходят или частично подходят для IoT.
- 2) Добавлять, редактировать и удалять в базу данных критерии оценки альтернатив.
- 3) Применять выбранные методы мультикритериального принятия решений для выбора оптимального протокола консенсуса для сетей Интернета вещей на основе блокчейна.

В базу данных системы был внесен следующий список альтернатив: Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Importance (PoI), Proof of Supply Chain Share (PoSCS), Credit-Based Proof of Work (CBPoW), RapidChain, OmniLedger, Raft, Practical Byzantine Fault Tolerance (PBFT), dPBFT, Proof of Elapsed Work and Luck (PoEWAL), Microchain, Proof of Elapsed Time (PoET), Tangle, Ripple Protocol Consensus Algorithm (RPCA), Stellar Consensus Protocol (SCP), CBCIoT, Proof of Block & Trade (PoBT), Proof of Accumulated Trust (PoAT), hierarchical and location-aware consensus protocol LH-Raft, Proof of Chance (PoCh), Honesty-based Distributed Proof of Authority (HDPoA), Proof of Reputation X, Proof of X-repute.

На следующем рисунке показана часть интерфейса с разделом «Альтернативы и Критерии» (Рис.6).

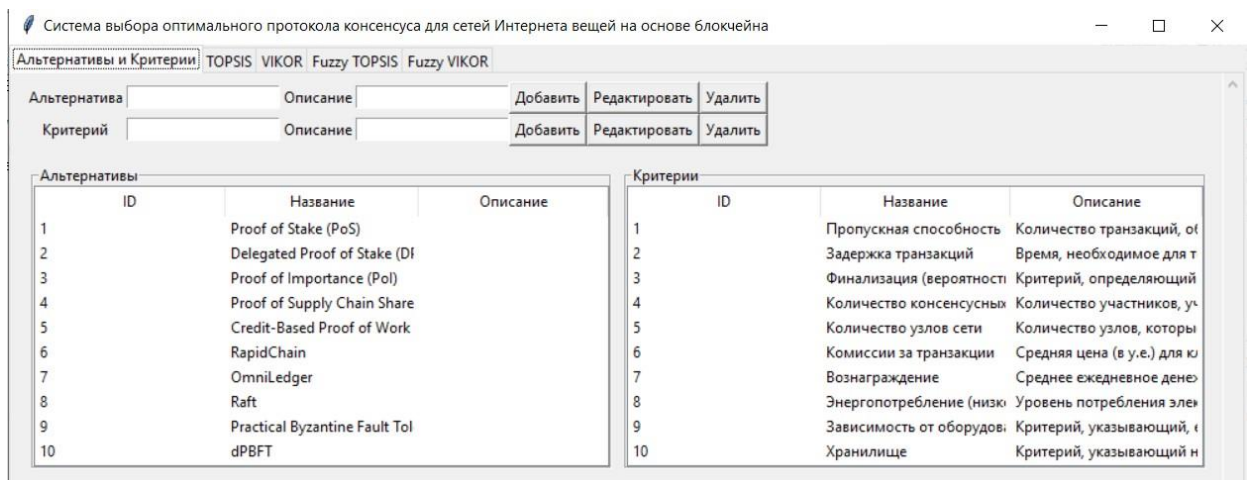


Рисунок 6 – Часть интерфейса система выбора оптимального протокола консенсуса

Далее был составлен и внесен в базу данных следующий список критериев: пропускная способность (C_1 - транзакций в секунду (TPS), C_2 - задержка транзакций (с), C_3 - финализация (вероятностная/детерминированная)), децентрализация (C_4 - количество консенсусных узлов, C_5 - количество узлов сети), стимулирование (C_6 - комиссии за транзакции (у.е./транзакции), C_7 - вознаграждение (у.е. в день)), устойчивость (C_8 - энергопотребление (низкое/среднее/высокое), C_9 - зависимость от оборудования (нет/да), C_{10} - хранилище), безопасность (C_{11} - отказоустойчивость, C_{12} - атака 51% (Уязвимый/Безопасный), C_{13} - двойная трата (Уязвимый/Сложный/Безопасный)).

Пользователь системы с помощью созданной базы данных имеет возможность определять список альтернатив $A = \{A_1, A_2, \dots, A_m\}$, список критериев $C = \{C_1, C_2, \dots, C_n\}$, список весов соответствующих критериев $W = \{w_1, w_2, \dots, w_n\}$, где $w_j \in [0,1]$, $\sum_{j=1}^n w_j = 1$. Также определяется тип каждого критерия (положительный или отрицательный). В случае критерия положительного типа, чем больше его значение, тем лучше альтернатива, а в случае критерия отрицательного типа, чем меньше его значение, тем лучше альтернатива. В случае, когда значения некоторого критерия выражаются в словесно (например, "низкое", "среднее", "высокое"), они преобразовываются в числовые значения с помощью

специальных шкал (например, девятибалльная шкала Саати). Далее, каждая альтернатива оценивается по каждому критерию, и из полученных оценок формируется матрица решений $X = [x_{ij}]_{m \times n}$. В случае применения нечетких методов определяется список нечетких весов соответствующих критериев $\tilde{W} = \{\tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n\}$, где \tilde{w}_j , $j = 1, \dots, n$ – нечеткие треугольные числа, тип каждого критерия (положительный или отрицательный). Задается шкала перевода лингвистических оценок в нечеткие треугольные числа. Далее, каждая альтернатива оценивается по каждому критерию, используя числовые коды лингвистических оценок, и из полученных оценок формируется матрица решений $X = [x_{ij}]_{m \times n}$. Затем матрица решений $X = [x_{ij}]_{m \times n}$ преобразовывается в нечеткую матрицу решений $\tilde{X} = [\tilde{x}_{ij}]_{m \times n}$, где $\tilde{x}_{ij} = (a_{ij}, b_{ij}, c_{ij})$, $i = 1, \dots, m$, $j = 1, \dots, n$ – соответствующие оценкам x_{ij} нечеткие треугольные числа. Далее на основе определенных данных выполняются вычисления, предусмотренные выбранным пользователем методом.

Использование MCDA-MSS и WEMSS имеет ряд преимуществ. Во-первых, это некоторая степень автоматизации процесса выбора оптимальных методов многокритериального принятия решений. Во-вторых, это возможность учитывать множество различных параметров, что, в свою очередь, снижает риск появления субъективных ошибок при принятии решений. В-третьих, это гибкость инструмента за счет обширных баз данных MCDA-MSS и WEMSS. Кроме того, MCDA-MSS дает возможность пользователю выбирать из списка нескольких альтернативных методов, и в дальнейшем проводить их сравнительный анализ.

Однако этот подход имеет и некоторые ограничения. Во-первых, функционирование систем MCDA-MSS и WEMSS запрограммировано на основе встроенных алгоритмов, и, очевидно, не может полностью заменить экспертный анализ. В системе используется фиксированная таксономия, которая определяет прохождение пользователем по дереву вопросов данных систем. Для этого требуется полное и объективное понимание пользователем анализируемой задачи. И в случае несоответствия анализируемой задачи заложенным в системе алгоритмам возможны ошибочные рекомендации систем. Кроме того, с течением времени возможно появление необходимости модернизации таксономии и обновления в целом систем. Во-вторых, функционирование систем напрямую зависят от исходных данных пользователя, и, следовательно, любые ошибочные данные могут привести к неправильным рекомендациям систем. Существует зависимость от квалификации, знаний и опыта пользователя. В-третьих, функционирование систем зависит от их баз данных, которые могут устаревать в связи с тем, что появляются новые методы, а существующие развиваются. И если эти базы своевременно не обновлять, то возможны ошибочные и не актуальные рекомендации систем. Таким образом, работа с этими системами требует от их пользователя понимания методов многокритериального принятия решений, предварительного изучения функционала систем, а также критического отношения к полученным рекомендациям систем. Одним из возможных способов преодоления перечисленных ограничений является применение технологий искусственного интеллекта, в частности, машинного обучения.

В целом, использование таких программных инструментов, как MCDA-MSS и WEMSS, для решения сложных задач выбора в области технологий распределенного реестра для IoT имеет большой потенциал, и может быть полезным при разработке специализированных интеллектуальных систем поддержки принятия решений в области технологий распределенного реестра.

Заключение.

В данной работе представлен эффективный подход по выбору оптимальных методов многокритериального принятия решений, состоящий в использовании систем MCDA-MSS и WEMSS. С помощью этих специализированных был составлен список ряда методов

(TOPSIS, Fuzzy TOPSIS, TOPSIS Interval, TOPSIS Interval and Fuzzy, VIKOR и Fuzzy VIKOR, а также АНР) для решения задачи выбора оптимального протокола консенсуса в сетях IoT.

Этот подход имеет ряд достоинств, таких как автоматизация процесса выбора методов, возможность учитывать множество различных параметров, гибкость. Однако имеются и некоторые ограничения: зависимость функционирования систем от встроенных алгоритмов, зависимость от исходных данных пользователя, зависимость актуальности баз данных систем. В целом, рассмотренный подход показывает потенциал использования таких программных инструментов для решения сложных задач выбора в области технологий распределенного реестра для IoT. Можно считать, это может быть полезным при разработке специализированных интеллектуальных систем поддержки принятия решений в области технологий распределенного реестра. А также возможна будущая интеграция с технологиями искусственного интеллекта, которая повысит эффективность и адаптивность принимаемых решений, особенно в условиях высокой неопределенности данных и изменяющихся требований к протоколам консенсуса в сетях IoT.

***Благодарность.** Работа выполнена при финансовой поддержке КН МНВО РК, No AP23487259.*

Список литературы

1. Оспанов, Р., Сейткулов, Е., Ташатов, Н., Ергалиева, Б., Сергазин, Г. (2024). Об альтернативах по методу многокритериального принятия решений при выборе протокола консенсуса блокчейна для сетей Интернета Вещей. Вестник КазАТК, 134(5), 426-436. <https://doi.org/10.52167/1609-1817-2024-134-5-426-436>
2. Оспанов, Р., Сейткулов, Е., Ташатов, Н., Ергалиева, Б., Сергазин, Г. (2024). О разработке критериев оценки альтернатив по методу многокритериального принятия решений при выборе протокола консенсуса блокчейна для сетей Интернета Вещей. Вестник КазАТК, 135(6), 263-271. <https://doi.org/10.52167/1609-1817-2024-135-6-263-271>
3. MCDA-MSS (MCDA Methods Selection Software). [Электронный ресурс]. - Режим доступа: <https://mcda.cs.put.poznan.pl/index.php> (дата обращения: 29.03.2025).
4. WEMSS (WEighting Methods Selection Software). [Электронный ресурс]. - Режим доступа: <https://mcda.cs.put.poznan.pl/wemss/index.php> (дата обращения: 29.03.2025).
5. Cinelli, M., Kadziński, M., Miebs, G., Gonzalez, M., Słowiński, R. (2022). Recommending multiple criteria decision analysis methods with a new taxonomy-based decision support system. European Journal of Operational Research, 302(2), 633-651. <https://doi.org/10.1016/j.ejor.2022.01.011>
6. Cinelli, M., Kadziński, M., Gonzalez, M., Słowiński, R. (2020). How to support the application of multiple criteria decision analysis? Let us start with a comprehensive taxonomy. Omega, 96, 102261. <https://doi.org/10.1016/j.omega.2020.102261>
7. Online workshop on the Multiple Criteria Decision Analysis Methods Selection Software. [Электронный ресурс]. - Режим доступа: <https://www.universiteitleiden.nl/en/events/2023/10/online-workshop-on-the-multiple-criteria-decision-analysis-methods-selection-software> (дата обращения: 29.03.2025).
8. Bilbao-Terol, A., Arenas-Parra, M., Cañal-Fernández, V., Antomil-Ibias, J. (2014). Using TOPSIS for assessing the sustainability of government bond funds. Omega, 49, 1-17. <https://doi.org/10.1016/j.omega.2014.04.005>
9. Nădăban, S., Dzitac, S., Dzitac, I. (2016). Fuzzy TOPSIS: A General View. Procedia Computer Science, 91, 823-831. <https://doi.org/10.1016/j.procs.2016.07.088>
10. Jahanshahloo, G.R., Hosseinzadeh Lotfi, F., Izadikhah, M. (2006). An algorithmic method to extend TOPSIS for decision-making problems with interval data. Applied Mathematics and Computation, 175(2), 1375-1384. <https://doi.org/10.1016/j.amc.2005.08.048>
11. Chen, T.-Y., Tsao, C.-Y. (2008). The interval-valued fuzzy TOPSIS method and experimental analysis. Fuzzy Sets and Systems, 159(11), 1410-1428. <https://doi.org/10.1016/j.fss.2007.11.004>

12. Opricovic, S. (1998). Multicriteria Optimization of Civil Engineering Systems. PhD Thesis, Faculty of Civil Engineering, Belgrade, 302 p.
13. Opricovic, S. (2011). Fuzzy VIKOR with an application to water resources planning. *Expert Systems with Applications*, 38(10), 12983-12990. <https://doi.org/10.1016/j.eswa.2011.04.097>
14. Saaty, T.L. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1), 9-26. [https://doi.org/10.1016/0377-2217\(90\)90057-I](https://doi.org/10.1016/0377-2217(90)90057-I)

References

1. Ospanov, R., Seitkulov, E., Tashatov, N., Ergaliyeva, B., Sergazin, G. (2024). Ob al`ternativax po metodu mnogokriterial`nogo prinyatiya reshenij pri vy`bore protokola konsensusa blokchejna dlya setej Interneta Veshhej. *Vestnik KazATK*, 134(5), 426-436. <https://doi.org/10.52167/1609-1817-2024-134-5-426-436>
2. Ospanov, R., Seitkulov, E., Tashatov, N., Ergaliyeva, B., Sergazin, G. (2024). O razrabotke kriteriev ocenki al`ternativ po metodu mnogokriterial`nogo prinyatiya reshenij pri vy`bore protokola konsensusa blokchejna dlya setej Interneta Veshhej. *Vestnik KazATK*, 135(6), 263-271. <https://doi.org/10.52167/1609-1817-2024-135-6-263-271>
3. MCDA-MSS (MCDA Methods Selection Software) from <https://mcda.cs.put.poznan.pl/index.php>
4. WEMSS (WEighting Methods Selection Software) from <https://mcda.cs.put.poznan.pl/wemss/index.php>
5. Cinelli, M., Kadziński, M., Miebs, G., Gonzalez, M., Słowiński, R. (2022). Recommending multiple criteria decision analysis methods with a new taxonomy-based decision support system. *European Journal of Operational Research*, 302(2), 633-651. <https://doi.org/10.1016/j.ejor.2022.01.011>
6. Cinelli, M., Kadzinski, M., Gonzalez, M., Słowinski, R. (2020). How to support the application of multiple criteria decision analysis? Let us start with a comprehensive taxonomy. *Omega*, 96, 102261. <https://doi.org/10.1016/j.omega.2020.102261>
7. Online workshop on the Multiple Criteria Decision Analysis Methods Selection Software from <https://www.universiteitleiden.nl/en/events/2023/10/online-workshop-on-the-multiple-criteria-decision-analysis-methods-selection-software>
8. Bilbao-Terol, A., Arenas-Parra, M., Cañal-Fernández, V., Antomil-Ibias, J. (2014). Using TOPSIS for assessing the sustainability of government bond funds. *Omega*, 49, 1-17. <https://doi.org/10.1016/j.omega.2014.04.005>
9. Nădăban, S., Dzitac, S., Dzitac, I. (2016). Fuzzy TOPSIS: A General View. *Procedia Computer Science*, 91, 823-831. <https://doi.org/10.1016/j.procs.2016.07.088>
10. Jahanshahloo, G.R., Hosseinzadeh Lotfi, F., Izadikhah, M. (2006). An algorithmic method to extend TOPSIS for decision-making problems with interval data. *Applied Mathematics and Computation*, 175(2), 1375-1384. <https://doi.org/10.1016/j.amc.2005.08.048>
11. Chen, T.-Y., Tsao, C.-Y. (2008). The interval-valued fuzzy TOPSIS method and experimental analysis. *Fuzzy Sets and Systems*, 159(11), 1410-1428. <https://doi.org/10.1016/j.fss.2007.11.004>
12. Opricovic, S. (1998). Multicriteria Optimization of Civil Engineering Systems. PhD Thesis, Faculty of Civil Engineering, Belgrade, 302 p.
13. Opricovic, S. (2011). Fuzzy VIKOR with an application to water resources planning. *Expert Systems with Applications*, 38(10), 12983-12990. <https://doi.org/10.1016/j.eswa.2011.04.097>
14. Saaty, T.L. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1), 9-26. [https://doi.org/10.1016/0377-2217\(90\)90057-I](https://doi.org/10.1016/0377-2217(90)90057-I)

ИОТ ЖЕЛІЛЕРІНДЕГІ КОНСЕНСУС ХАТТАМАСЫН АНЫҚТАУ ҮШІН МАМАНДАНДЫРЫЛҒАН БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАНЫ ҚОЛДАНА ОТЫРЫП, КӨП КРИТЕРИАЛДЫ ТАЛДАУДЫҢ ОҢТАЙЛЫ ӘДІСТЕРІН ТАҢДАУ

***Аңдатпа:** Интернет желісіндегі блокчейн консенсусының оңтайлы механизмдерін таңдау мәселесін шешім қабылдаудың көп критерийлі мәселесі ретінде қарастыруға болады. Бұл жұмыстың мақсаты осы мәселе аясында көп критерийлі шешім қабылдаудың ең қолайлы әдісін анықтау болып табылады. Қазіргі уақытта мультикритериалды талдаудың көптеген әртүрлі әдістері бар. Сонымен қатар, жаңа әдістер пайда болып, барлары дамып келеді. Мұндай жағдайларда қарастырылып отырған мәселе бойынша көп критериалды шешім қабылдаудың ең қолайлы әдісін дұрыс анықтау өте маңызды болып көрінеді. Мұндай дұрыс таңдау бағалау мен шешім қабылдауда объективтілік пен дәлдікке үлкен сенімділікті қамтамасыз етеді деп күтілуде. Қарастырылып отырған мәселе көптеген баламалармен (көптеген әртүрлі консенсус хаттамалары) және көптеген критерийлермен (мысалы, энергияны тұтыну, өткізу қабілеті, шабуылдарға төзімділік, транзакцияларды өңдеу кідірісі және т.б.) сипатталатынын ескерсек, бұл да маңызды. Қазіргі уақытта көп критериалды шешім қабылдаудың ең қолайлы әдістерін таңдау процесін автоматтандыруға арналған ашық бастанқы бағдарламалық құралдар бар. Мұндай шешімдерді қолдау жүйелері талдаушылар мен зерттеушілерге мультикритериалды талдауды қолданудың әртүрлі салаларында көмектеседі. Бұл жұмыс IoT үшін оңтайлы консенсус механизмін таңдау мәселесі жағдайында осындай мамандандырылған бағдарламалық қамтамасыз етуді пайдалану негізінде көп критериалды шешім қабылдаудың оңтайлы әдістерін таңдау тәсілін ұсынады. Нәтижесінде белгілі TOPSIS, VIKOR әдістері, сонымен қатар олардың интервалдық және анық емес модификациялары таңдалды. Сонымен қатар, критерийлерді салмақтау үшін аналитикалық иерархиялық процесс (АHP) әдісі таңдалды.*

***Түйін сөздер:** бөлінген тізілім технологиялары, блокчейн, консенсус протоколы, заттар интернеті, көп критериалды шешім қабылдау әдістері.*

SELECTION OPTIMAL MULTICRITERIA ANALYSIS METHODS USING SPECIALISED SOFTWARE TO DETERMINE CONSENSUS PROTOCOL IN INTERNET OF THINGS NETWORKS

***Abstract:** The task of selecting optimal blockchain consensus mechanisms in the IoT networks can be considered as a multi-criteria decision-making task. The goal of this paper is to determine the most appropriate method of multi-criteria decision-making for this task. Currently, there are many different methods of multi-criteria analysis. In addition, new methods are emerging, and the existing ones continue to evolve. In such conditions, it seems very important to correctly determine the most appropriate method of multi-criteria decision-making for the task at hand. It is assumed that such a correct choice will provide greater confidence in the objectivity and accuracy of evaluation and decision-making. This is also important given that the task at hand is characterized by a large number of alternatives (many different consensus protocols) and a large number of criteria (e.g., energy consumption, throughput, attack resistance, transaction processing delay, etc.). Currently, there are open source software tools designed to automate the process of selecting the most appropriate methods of multi-criteria decision-making. Such decision support systems help analysts and researchers in various areas of multi-criteria analysis application. This paper presents an approach to selecting optimal methods for multi-criteria decision making based on the use of such specialized software in the case of the problem of selecting the optimal consensus mechanism for IoT. As a result, the well-known TOPSIS, VIKOR methods, as well as their interval and fuzzy modifications, were selected. Additionally, the analytical hierarchy process (AHP) method was selected for weighting the criteria.*

Keywords: *distributed ledger technologies, blockchain, consensus protocol, Internet of Things, multi-criteria decision making methods.*

Сведение об авторах

Руслан Оспанов	научный сотрудник, ЕНУ им. Л.Н.Гумилева, E-mail: ospanovrm@gmail.com
Ержан Сейткулов	к.ф.-м.н., главный научный сотрудник, ЕНУ им. Л.Н.Гумилева, E-mail: yerzhan.seitkulov@gmail.com
Нурлан Ташатов	к.ф.-м.н., главный научный сотрудник, ЕНУ им. Л.Н.Гумилева, E-mail: yerzhan.seitkulov@gmail.com
Бану Ергалиева	научный сотрудник, ЕНУ им. Л.Н.Гумилева, E-mail: ergalieva_banu@mail.ru
Куат Утебаев	магистрант филиала НИЯУ МИФИ, Алматы.

Авторлар туралы мәлімет

Руслан Оспанов	ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, E-mail: ospanovrm@gmail.com
Ержан Сейткулов	ф.-м.ғ.к., бас ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, E-mail: yerzhan.seitkulov@gmail.com
Нурлан Ташатов	п.ғ.д., бас ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, E-mail: tash.nur@mail.ru
Бану Ергалиева	ғылыми қызметкер, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, E-mail: ergalieva_banu@mail.ru
Куат Утебаев	магистрант, Ұлттық зерттеу ядролық университетінің филиалы, Алматы.

Information about the authors

Ruslan Ospanov	Researcher, L.N. Gumilyov Eurasian National University, ospanovrm@gmail.com
Yerzhan Seitkulov	Ph.D, Chief Researcher, L. N. Gumilyov Eurasian National University, E-mail: yerzhan.seitkulov@gmail.com
Nurlan Tashatov	Ph.D., Chief Researcher, L. N. Gumilyov Eurasian National University, E-mail: tash.nur@mail.ru
Banu Yergaliyeva	researcher, L. N. Gumilyov Eurasian National University E-mail: ergalieva_banu@mail.ru
Kuat Utebayev	master student, Almaty Branch of the National Research Nuclear University

МАЗМУНЫ/СОДЕРЖАНИЕ/ CONTENTS

<i>ӘУЕ КӨЛІГІ ЖӘНЕ ТЕХНОЛОГИЯЛАР</i>	
<i>ВОЗДУШНЫЙ ТРАНСПОРТ И ТЕХНОЛОГИИ</i>	
<i>AIR TRANSPORT AND TECHNOLOGY</i>	
Рысбекова А. А., Мендакулов Ж. К., Кенбеилова С.Ж. АНАЛИЗ МЕЖДУНАРОДНОЙ НОРМАТИВНОЙ БАЗЫ ПО НОРМИРОВАНИЮ ОПАСНЫХ ВОЗДЕЙСТВИЙ ЗВУКОВЫХ И УЛЬТРАЗВУКОВЫХ КОЛЕБАНИЙ	6
Исмаилов Д.В., Ксенофонов Д.А., Зикирьяев Н.Б., Кабдуллин А.А. АНТИДРОНОВЫЙ КОМПЛЕКС ДЛЯ ОБНАРУЖЕНИЯ, ПОДАВЛЕНИЯ И ПОРАЖЕНИЯ ЦЕЛЕЙ	22
Әбдіматов Т.Д., Васильев И.В. ТРЕБОВАНИЯ К ХАРАКТЕРИСТИКАМ ПЕРСПЕКТИВНОГО ПРИБОРА ДЛЯ УЛЬТРАЗВУКОВОЙ ДИАГНОСТИКИ МЕХАНИЗМОВ	32
Levchenko N., Bakirov B. CREATION OF A "SMART" OCCUPATIONAL SAFETY MANAGEMENT SYSTEM IN CIVIL AVIATION IN THE CONTEXT OF THE "SOCIETY 5.0" CONCEPT	47
<i>ЛОГИСТИКА, ТАСЫМАЛДАУДЫ ҰЙЫМДАСТЫРУ, КӨЛІКТЕГІ ҚАУІПСІЗДІК</i>	
<i>ЛОГИСТИКА, ОРГАНИЗАЦИЯ ПЕРЕВОЗОК, БЕЗОПАСНОСТЬ НА ТРАНСПОРТЕ</i>	
<i>LOGISTICS, TRANSPORTATION ORGANIZATION, TRANSPORT SECURITY</i>	
Серик Ш., Асылбекова И.Ж. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ АВИАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОТКРЫТИИ НОВЫХ РЕЙСОВ АВИАКОМПАНИЙ РЕСПУБЛИКИ КАЗАХСТАН	57
<i>КОМПЬЮТЕРЛІК ҒЫЛЫМДАР, АСПАП ЖАСАУ ЖӘНЕ АВТОМАТТАНДЫРУ</i>	
<i>КОМПЬЮТЕРНЫЕ НАУКИ, ПРИБОРОСТРОЕНИЯ И АВТОМАТИЗАЦИЯ</i>	
<i>COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION</i>	
Rakhimzhanov D., Belginova S. TRANSFORMER MODELS FOR PASSENGER REVIEWS CLASSIFICATION: A STUDY USING RUBERT AND XLM-ROBERTA	67
Хомпыш А., Сақан Қ.С., Алғазы К., Абишева А.Ж. «EM CHIPER» БЛОКТЫ ШИФРЛАУ АЛГОРИТМІНІҢ КРИПТОБЕРІКТІЛІГІН ЗЕРТТЕУ	82
Кабдрахманова З. Г., Глебалдинова А.С., Карменова М.А., Кумаргажанова С.К., Карымсакова И.Б. ПРИМЕНЕНИЕ ТЕКСТУРНОГО АНАЛИЗА ПРИ КЛАССИФИКАЦИИ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ	94
Dzhsupbekova G., Ordabayeva G., Beketova A., Vaispay G. APPLYING ARTIFICIAL INTELLIGENCE METHODS TO DETECT NETWORK TRAFFIC ANOMALIES	105
Адилжанова С.А., Құрасбек А.Н., Кенжебаева М.О. ПРИМЕНЕНИЕ LLM В КИБЕРБЕЗОПАСНОСТИ: ОБЗОР ПРИЛОЖЕНИЙ И УЯЗВИМОСТЕЙ LLM	118
Ryabchenko I., Anayatova R., Tulekova G., Koshekov A., Kuanov Y. MODELING SEMANTIC RELATIONSHIPS OF AVIATION TERMS: VECTOR SPACES AND LANGUAGE MODELS	137
Mukashova A., Tussupov J., Mukhanova A., Makhatova V., Kurmangaziyeva L. INTELLIGENT COMPETENCE AND LEARNING OUTCOMES MANAGEMENT SYSTEM: ADAPTING EDUCATIONAL PROGRAMS TO THE LABOR MARKET	150
Ыбрайымбай Б. Қ., Адилжанова С.А., Черикбаева Л. Ш. ЭНЕРГЕТИКАЛЫҚ НЫСАНДАР ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ АРҚЫЛЫ DDOS ШАБУЫЛДАРЫНАН ҚОРҒАУ ЖҮЙЕСІН ӨЗІРЛЕУ	160
Lamasheva Zh. B., Makhazhanova U.T., Kassekeyeva A.B., Iskakov Y.K.	173

MULTINOMIAL NAIVE BAYES FOR KAZAKH LANGUAGE SPAM DETECTION: A CASE STUDY WITH MORPHOLOGICAL ANALYSIS	
Фазылова А., Алипбаев К., Оразалиева А., Аден А. ТЕОРЕТИЧЕСКОЕ И ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ АЭРОДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК И МЕХАНИЧЕСКОЙ УСТОЙЧИВОСТИ РОТОРА ДАРЬЕ	185
Сулейменова М.У., Абзалиев К.Б., Абзалиева С.А., Мұхаммеджанова Д.М. ЕРТЕ ҚАРТАЮ БЕЛГІЛЕРІН АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНУ	195
Оспанов Р., Сейткулов Е., Ташатов Н., Ергалиева Б., Утебаев К. ВЫБОР ОПТИМАЛЬНЫХ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПРОТОКОЛА КОНСЕНСУСА В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ	207

CONTENTS

<i>AIR TRANSPORT AND TECHNOLOGY</i>	
Rysbekova A.A., Mendakulov Zh. K., Kenbeilova S.Zh. ANALYSIS OF THE INTERNATIONAL REGULATORY FRAMEWORK FOR THE REGULATION OF HAZARDOUS EFFECTS OF SOUND AND ULTRASONIC VIBRATIONS	6
Ismailov D., Xenofontov D., Zikiryaev N., Kabdullin A. ANTI-DRONE COMPLEX FOR DETECTION, SUPPRESSION, AND DESTRUCTION OF TARGETS	22
Abdimatova T.D., Vassilyev I.V. REQUIREMENTS FOR THE CHARACTERISTICS OF A PROSPECTIVE DEVICE FOR ULTRASONIC DIAGNOSTICS OF MECHANISMS	32
Levchenko N., Bakirov B. CREATION OF A "SMART" OCCUPATIONAL SAFETY MANAGEMENT SYSTEM IN CIVIL AVIATION IN THE CONTEXT OF THE "SOCIETY 5.0" CONCEPT	47
<i>LOGISTICS, TRANSPORTATION ORGANIZATION, TRANSPORT SECURITY</i>	
Assilbekova I. Zh., Serik Sh. ORGANIZATIONAL MEASURES TO ENSURE AVIATION SECURITY AT THE OPENING OF NEW FLIGHTS OF AIRLINES OF THE REPUBLIC OF KAZAKHSTAN	57
<i>COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION</i>	
Rakhimzhanov D., Belginova S. TRANSFORMER MODELS FOR PASSENGER REVIEWS CLASSIFICATION: A STUDY USING RUBERT AND XLM-ROBERTA	67
Khompysh A., Sakan K., Algazy K., Abisheva A. Zh. STUDY OF CRYPTOCURRENCY OF THE BLOCK CIPHER ALGORITHM «EM CHIPER»	82
Kabdrakhmanova Z., Tlebalidina A., Karmenova M., Kumargazhanova S., Karymsakova I. APPLICATION OF TEXTURE ANALYSIS IN MEDICAL IMAGE CLASSIFICATION	94
Dzhshupbekova G., Ordabayeva G., Beketova A., Baispay G. APPLYING ARTIFICIAL INTELLIGENCE METHODS TO DETECT NETWORK TRAFFIC ANOMALIES	105
Kurasbek A., Kenzhebayeva M., Adilzhanova S. THE USE OF LLM IN CYBERSECURITY: OVERVIEW OF LLM APPLICATIONS AND VULNERABILITIES	118
Ryabchenko I., Anayatova R., Tulekova G., Koshekov A., Kuanov Y. MODELING SEMANTIC RELATIONSHIPS OF AVIATION TERMS: VECTOR SPACES AND LANGUAGE MODELS	137
Mukashova A., Tussupov J., Mukhanova A., Makhatova V., Kurmangazyeva L. INTELLIGENT COMPETENCE AND LEARNING OUTCOMES MANAGEMENT SYSTEM: ADAPTING EDUCATIONAL PROGRAMS TO THE LABOR MARKET	150
Ybraiymbay B., Adilzhanova S., Cherikbayeva I. DEVELOPMENT OF A DDOS ATTACK PROTECTION SYSTEM FOR ENERGY FACILITIES USING MACHINE LEARNING METHODS	160
Lamasheva Zh. B., Makhazhanova U.T., Kassekeyeva A.B., Iskakov Y.K. MULTINOMIAL NAIVE BAYES FOR KAZAKH LANGUAGE SPAM DETECTION: A CASE STUDY WITH MORPHOLOGICAL ANALYSIS	173
Fazylova A., Alipbayev K., Orazaliyeva A., Aden A. THEORETICAL AND NUMERICAL MODELING OF AERODYNAMIC CHARACTERISTICS AND MECHANICAL STABILITY OF THE DARRIER ROTOR	185

Suleimenova M., Abzaliyev K., Abzaliyeva S., Mukhammejanova D. USING MACHINE LEARNING TO IDENTIFY SIGNS OF PREMATURE AGING	195
Ospanov R., Seitkulov Y., Tashatov N., Yergaliyeva B., Utebayev K. SELECTION OPTIMAL MULTICRITERIA ANALYSIS METHODS USING SPECIALISED SOFTWARE TO DETERMINE CONSENSUS PROTOCOL IN INTERNET OF THINGS NETWORKS	207

Азаматтық авиация академиясының Жаршысы

Ғылыми журнал

2015 жылдан бастап шыға бастады

Қазақстан Республикасы Мәдениет және ақпарат министрлігінде тіркеліп, 2025 жылдың 31 қаңтарында мерзімді баспасөз басылымын, ақпараттық агенттікті және желілік басылымды қайта есепке қою туралы Куәлігі берілді (№ KZ89VPY0011238)

Вестник Академии гражданской авиации

Научный журнал

Издается с 2015 г.

Зарегистрирован Министерством культуры и информации Республики Казахстан
Свидетельство № KZ89VPY0011238 от 31 января 2025 г.

Bulletin of Civil aviation Academy

Scientific journal

Published since 2015

It is registered by the Ministry of Culture and Information of the Republic of Kazakhstan.
Certificate no. KZ89VPY0011238 dated January 31, 2025

Жауапты редактор: А. Т. Макеева

Ответственный редактор: А.Т. Макеева

Responsible editor: A.T. Makeeva

Басылымға 29.09.2025 ж. қол қойылды.

Формат 205*290. Өлшемі - баспа табақшасы. Таралымы 50 дана.

Издание подписано 29.09.2025 г.

Формат 205*290. Размер –печатная пластина. Тираж 50 экз.

The publication was signed on, September 29, 2025.

The format is 205*290. The size is a printed plate. Edition of 50 copies

Азаматтық авиация академиясы. 050039, Алматы қаласы, Закарпатская көшесі,44

Академия гражданской авиации. 050039, г. Алматы, ул. Закарпатская,44

Academy of Civil Aviation. 44 Zakarpatskaya St., 050039, Almaty