ASTANA INTERNATIONAL UNIVERSITY

ISSN 2707-4862, Print

SMART TECHNOLOGIES JOURNAL

№1 (7) 2025

ISSN 2707-4862

Астана Халықаралық университеті
Международный университет Астана
Astana International University

SMART TECHNOLOGIES JOURNAL

№ 1 (7) - 2025

Жылына 4 рет шығады
Выходит 4 раза в год
Published 4 times a year

Астана - 2025
Astana - 2025

Меншіктенуші: «Астана Халықаралық университеті» Жауапкершілігі шектеулі серіктестігі
Тіркеу: ҚР Мәдениет және ақпарат министрлігінің Ақпарат комитеті
Бастапқы есепке қою күні мен нөмірі: 16.01.2020 ж. тіркеу куәлігімен № KZ93VPY00019404
Екінші есепке қою: 16.09.2025 № KZ92VPY00129420
Мерзімділігі: жылына 4 рет
ISSN: 2707-4862
Тақырыптық бағыты: Ақпараттық технологиялар
Редакцияның мекенжайы: 010000, Қазақстан, Астана қ., Қабанбай батыр даңғылы, 8
тел.: +7 (7172) 47-62-10 (214), e-mail: stj@aiu.edu.kz

Собственник: Товарищество с ограниченной ответственностью «Международный университет Астана»
Регистрация: Комитет информации Министерства культуры и информации РК
Дата и номер первичной постановки на учет: 16.01.2020 г., регистрационное свидетельство № KZ93VPY00019404
Вторичная постановка на учет: 16.09.2025 № KZ92VPY00129420
Периодичность: 4 раза в год
ISSN: 2707-4862
Тематическое направление: Ақпараттық технологиялар
Адрес редакции: 010000, Казахстан, г. Астана, пр. Кабанбай батыра, 8,
тел.: +7 (7172) 47-62-10 (214), e-mail: stj@aiu.edu.kz

Owner: Limited Liability Partnership “Astana International University”
Registration: Information Committee of the Ministry of Culture and Information of the Republic of Kazakhstan
Date and number of initial registration: 16.01.2020, registration certificate № KZ93VPY00019404
Secondary registration: 16.09.2025 № KZ92VPY00129420
Frequency: 4 times a year
ISSN: 2707-4862
Subject area: Information Technologies
Address of edition: 010000, Kazakhstan, Astana, Kabanbay Batyr avenue, 8,
Tel.: +7 (7172) 47-62-10 (214), e-mail: stj@aiu.edu.kz

МАЗМҰНЫ – CONTENTS – СОДЕРЖАНИЕ

IRSTI 28.23.15 DOI: https://doi.org/10.62687/STJ.7.1.2025.7

MODERNIZATION OF TOLL COLLECTION SYSTEMS USING COMPUTER VISION FOR AUTOMATIC VEHICLE CLASSIFICATION

[1]B. Amanbayev*, **[1]A. Myrzakerimova**, **[1]E. Aitmukhanbetova**
[1]Astana IT University, Astana, Kazakhstan
*e-mail: amanbayev22@gmail.com

B. Amanbayev – Master Student of School of Computer Science and Engineering, Astana IT University, Astana, Kazakhstan, e-mail: amanbayev22@gmail.com, https://orcid.org/0009-0005-8600-1606

A. Myrzakerimova – PhD in Information Systems, Assistant Professor of School of Computer Engineering, Astana IT University, Astana, Kazakhstan, e-mail: alua.myrzakerimova@astanait.edu.kz, https://orcid.org/0000-0002-8500-1672

E. Aitmukhanbetova – MSc, School of Computer Engineering, Astana IT University, Astana, Kazakhstan, e-mail: elvira.aitmukhanbetova@astanait.edu.kz, https://orcid.org/0000-0001-7835-873X

Abstract. Research paper explores the use of computer vision technologies to automatically classify vehicles in the new toll collection systems. Specifically, the analysis focuses on integrating deep learning algorithms, especially convolutional neural networks (CNN), into modern toll plaza operations. Research shows that vision-systems technology improves the speed of processing and classification accuracy rates to levels that are previously unattainable. The research aids in understanding how these systems can be implemented, the challenges posed, and the prospects for practical widespread usage. The results achieved in this study suggest the strong need for the investment in improving the operational cost effectiveness, system cost, and overall satisfaction of the users of the toll collection systems.

Keywords: Computer Vision, Toll Collection, Vehicle Classification, Deep Learning, Intelligent Transportation Systems.

МОДЕРНИЗАЦИЯ СИСТЕМ ВЗИМАНИЯ ПЛАТЫ ЗА ПРОЕЗД С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ ТРАНСПОРТНЫХ СРЕДСТВ

[1]Б. Аманбаев*, [1]А. Мырзакеримова, [1]Э. Айтмуханбетова
[1]Астана IT Университет, Астана, Казахстан
*e-mail: amanbayev22@gmail.com

Б. Аманбаев – магистрант Школы компьютерных наук и инженерии, Астана IT Университет, Астана, Казахстан, e-mail: amanbayev22@gmail.com, https://orcid.org/0009-0005-8600-1606

А. Мырзакеримова – PhD в области информационных систем, ассистент-профессор Школы компьютерной инженерии, Астана IT Университет, Астана, Казахстан, e-mail: alua.myrzakerimova@astanait.edu.kz, https://orcid.org/0000-0002-8500-1672

Э. Айтмуханбетова – магистр наук (MSc), Школа компьютерной инженерии, Астана IT Университет, Астана, Казахстан, e-mail: elvira.aitmukhanbetova@astanait.edu.kz, https://orcid.org/0000-0001-7835-873X

Аннотация. В данной научной работе исследуется применение технологий компьютерного зрения для автоматической классификации транспортных средств в новых системах взимания платы за проезд. В частности, анализ сосредоточен на интеграции алгоритмов глубокого обучения, прежде всего сверточных нейронных сетей (CNN),

в современные процессы функционирования платных дорожных пунктов. Результаты исследований показывают, что использование систем компьютерного зрения позволяет существенно повысить скорость обработки данных и точность классификации до уровней, ранее недостижимых. Проведенное исследование способствует пониманию возможностей внедрения данных систем, возникающих при этом проблем, а также перспектив их практического и широкомасштабного применения. Полученные результаты указывают на высокую целесообразность инвестиций в повышение операционной экономической эффективности, оптимизацию стоимости систем и общее удовлетворение пользователей систем взимания платы за проезд.

Ключевые слова: компьютерное зрение, классификация транспортных средств, глубокое обучение, интеллектуальные транспортные системы.

КӨЛІК ҚҰРАЛДАРЫН АВТОМАТТЫ ТҮРДЕ ЖІКТЕУ ҮШІН КОМПЬЮТЕРЛІК КӨРУДІ ҚОЛДАНУ АРҚЫЛЫ ЖОЛАҚЫ ЖИНАУ ЖҮЙЕЛЕРІН ЖАҢҒЫРТУ

[1]Б. Аманбаев*, [1]А. Мырзакеримова, [1]Э. Айтмуханбетова
[1]Астана IT Университеті, Астана, Қазақстан
*e-mail: amanbayev22@gmail.com

Б. Аманбаев – компьютерлік ғылымдар және инженерия мектебінің магистранты, Астана IT Университеті, Астана қ., Қазақстан, e-mail: amanbayev22@gmail.com, https://orcid.org/0009-0005-8600-1606

А. Мырзакеримова – ақпараттық жүйелер саласы бойынша PhD, Компьютерлік инженерия мектебінің ассистент-профессоры, Астана IT Университеті, Астана қ., Қазақстан, e-mail: alua.myrzakerimova@astanait.edu.kz, https://orcid.org/0000-0002-8500-1672

Э. Айтмуханбетова – ғылым магистрі (MSc), Компьютерлік инженерия мектебі, Астана IT Университеті, Астана қ., Қазақстан, e-mail: elvira.aitmukhanbetova@astanait.edu.kz, https://orcid.org/0000-0001-7835-873X

Аңдатпа. Бұл ғылыми зерттеу жұмысында жолақы жинаудың жаңа жүйелерінде көлік құралдарын автоматты түрде жіктеу үшін компьютерлік көру технологияларын қолдану қарастырылады. Атап айтқанда, талдау терең оқыту алгоритмдерін, әсіресе конволюциялық нейрондық желілерді (CNN), заманауи ақылы жол инфрақұрылымының жұмыс үдерістеріне интеграциялауға бағытталған. Зерттеу нәтижелері компьютерлік көру жүйелерін пайдалану өңдеу жылдамдығын едәуір арттырып, көлік құралдарын жіктеу дәлдігін бұрын қол жеткізілмеген деңгейге дейін жақсартуға мүмкіндік беретінін көрсетеді. Бұл зерттеу аталған жүйелерді енгізу мүмкіндіктерін, туындайтын мәселелерді және оларды кең ауқымда практикалық қолдану перспективаларын түсінуге ықпал етеді. Алынған нәтижелер жолақы жинау жүйелерінің операциялық тиімділігін арттыру, жүйе құнын оңтайландыру және пайдаланушылардың жалпы қанағаттану деңгейін жақсарту мақсатында инвестиция салудың маңыздылығын дәлелдейді.

Түйін сөздер: компьютерлік көру, жолақы жинау, көлік құралдарын жіктеу, терең оқыту, интеллектуалды көлік жүйелері.

Introduction. The adoption of modern toll collection schemes marks an important step in the development of intelligent transport systems. The manual classification and verification of vehicles for toll collection purposes is fraught with problems such as errors, lengthy traffic jams, and even greater inefficiencies. Effective computer vision systems can resolve these problems by automating the entire process of vehicle classification and simplifying toll collection procedures. Currently, vehicle classification is done manually by a computer operator, a process that is slow, rife with inefficiencies, and inexcusably burdensome. Partially automated vehicle classification will remove a significant

portion of the human element regarding photos recorded by highway cameras. Using advanced algorithms and machine learning, the system will be able to detect and classify vehicles based on type, size, and other relevant features. Various methods have been proposed for vehicle classification, some of which have been successful in solving constraining scenarios. However, other remaining challenges include shifts in lighting, image scale, image quality, size and color (Bensedik, 2018:313-316). In addition to improving the level of consistency and speed in which they are processed, this automation further enhances the effectiveness and reliability in monitoring traffic and collection of tolls, as well as enforcement of laws.

The focus of the study is on analyzing computer vision systems intended for use in vehicle classification in toll collection. The assumption is that these automated systems will utilize deep learning algorithms, which offer low-cost operational efficiency (Lin, 2020:69). Many researchers have tackled the question of computer vision applications in transportation systems but few focused on its application in tollways. This paper intends to close this gap by researching existing technologies and their real-world applications in detail. Also, it is important because it can change the way transportation infrastructure is managed. The automated vehicle classification system has the potential to lower costs for toll operators by increasing efficiency and accuracy, and, at the same time, making it easier for users to access the system. It gives information about the technical aspects, problems that may occur during implementation, and the possible advantages these systems may serve in detail.

Literature Review. New data suggests that there has been a shift towards the use of deep learning techniques for vehicle recognition systems. Bensedik et al. (Bensedik, 2018:313-316) proved that convolutional neural networks (CNNs) are efficient in vehicle type classification, which has now been widely accepted as one of the first steps in modern automatic classification systems. Following this, Mostafa et al. (Mostafa, 2023:972-977) enhanced classifiers with tracking algorithms which allowed them to demonstrate the multitasking analysis of several vehicle features. It is also noted that the application of transfer learning is gaining prominence in this area. Farid et al. (Farid, 2025) in their most recent study used transfer learning with deep CNNs and showed that these systems can be adapted to specific regions, for attribution systems of vehicles specific to particular regions, the classification performance was significantly improved.

Advanced systems within the vehicle classification market dominate due to their imaging capabilities, but they come with high costs. One of the prominent solutions in this sector is the Tattile Vega53, widely used across European and Asian toll networks (official documentation). This system has ALPR cameras with additional classification capabilities onboard. One lane with an ALPR system costs approximately EUR 25,000 – 35,000. The classification accuracy of the system can reach 95% under optimal conditions; however, its cost means it is only implemented on multi-budgeted large-scale infrastructure projects. Figure 1 illustrates example of detection process.

Figure 1. Example of detection process

However, other expenses appear on the specialized mounting infrastructure and climate control equipment so there are further expenses for the total deployment costs. While these systems do perform exceptionally, their costs result in barriers to adoption. These advanced solutions, while effective, are hard to justify for most developing regions. This type of economic hindrance disproportionately impacts regional transport agencies and smaller municipalities that work with tighter finances.

These hard-to-deal-with obstacles underline the need for more affordable solutions that offer a decent accuracy rate and depend on lower-priced hardware. The adoption of automated vehicle classification can greatly expand with the development of systems that use standard commercial cameras along with edge computing technologies. Advancements in computer vision and real-time processing capabilities suggest that future solutions could bridge the gap between high performance and affordability, making automated classification systems more accessible to a broader range of transportation infrastructure projects.

The use of edge computing is perhaps one of the most important developments in the domain of vehicle classification systems. Broadly, Lin et al. (Lin, 2020:69) developed a public edge video analytics vehicle system aimed at decreasing the response time to classification requests and increasing the accuracy of the classification. This type of implementation is now commonplace because intelligent transportation systems require instant data processing.

In relation, Nguyen together with Sergey (Nguyen, 2024:117-123) conducted similar research on sensing methods and their combination with urban intelligent transport systems focusing on edge technologies for real-time intelligent processing and decision control.

Suryatali and Dharmadhikari (Suryatali, 2015:1-7) designed a vehicle detection system embedded in Linux, aimed at effective toll collection. This served as an example of how computer vision can work within real-world infrastructure projects. Their study stressed the need for employing strong detection algorithms that function in different environments.

Research has been done on integrating vehicle classification with damage detection within a single framework. Dwivedi et al. (Dwivedi, 2020:207-221) designed a deep learning framework that simultaneously classifies the different types of car damage and performs detection. Reddy et al. (Reddy, 2022:1-6) built on this by creating a Fast and Mask deep learning framework for automatic vehicle damage detection and classification. While Amodu et al. (Amodu, 2024:199-208) introduced the area of deep learning automated damage inspection, they showed the potential of deep learning within attempting to solve complex visual evaluation problems. In this field, steps were also taken by Mallikarjuna and Arun (Mallikarjuna, 2022:568-574) who devised methods for damage detection and classification using image processing.

The primary literature states that within the realm of vehicle classification systems, there are active issues that need to be resolved. With Youssouf (Youssouf, 2022:8) and Lin et al. (Lin, 2020:69) work, these issues are often consolidated into a few categories including systems sensitiveness to the environmental state of the area where the systems are deployed and need to function under different levels of light and different weather conditions. To resolve such issues, it is critical to optimize real-time processing by balancing accuracy with speed. Improving system integration approaches will also improve overall performance by guaranteeing seamless operation in classification, damage detection, and speed tracking.

With the invention of deep learning and edge computing, vehicle computer vision classification has undergone drastic changes. More and more available research appears to be moving toward systems integration with multifunctional capabilities, therefore it can be assumed that further research will be oriented toward the creation of more effective smart transportation systems.

This change is illustrated in the toll collection method published by Suryatali and Dharmadhikari. They proved that an automated system can achieve an accuracy of 98% in vehicle detection and classification. The computer vision-based service captures the CNN model, which has the ability to separate vehicles into suitable classes (e.g., Sedan- Class2) with high precision and very low response time.

Methodology. There is system architecture, which replaces human-dependent toll collection with a fully automated, deep learning–based vehicle classification pipeline. The methodology integrates high-resolution multi-angle image acquisition with edge computing infrastructure and CNN models using transfer learning to enable real-time, reliable vehicle classification under peak traffic conditions. System performance is evaluated through accuracy, latency, throughput, and reliability metrics, demonstrating improved scalability and reduced bottlenecks compared to traditional approaches. Figure 2 illustrates the scheme of initial work system.

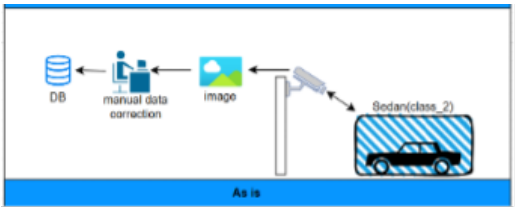

Figure 2. Scheme of initial work system

While this “AS IS” approach is functional, it comes with several inefficiencies:
- Elevated operational costs due to reliance on manual labor;
- Longer processing times per vehicle;
- Greater risk of human error in classification;
- Reduced scalability during high-traffic periods;
- Delays in data entry into the database system.

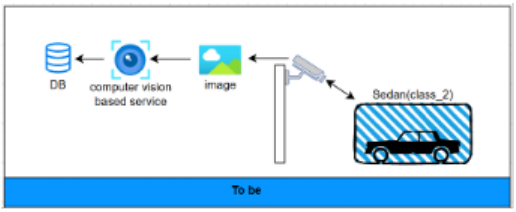

Figure 3. Scheme of future work system

Figure 3 shows the scheme of future work system. In contrast with the “traditional” approach, which applies excessive dependence on the human element and lacks complex algorithmic processing for image capturing, “TO BE” serves as a fully automated system. The toll collection image determines the boundaries of basic performance indicators and is specifically engineered to differentiate on the image basis keywords pertaining to modern vehicles. The “TO BE” model greatly increases response and processing time for vehicles, with far less restrictions on peak load than the human-controlled systems.

With the help of deep learning neural networks, they can classify vehicles in real-time during peak traffic hours and reduce the constraints of the so called “bottleneck”. Along with eliminating the necessity to manually classify databases and assisting images provided by road sensors and CCTV after processing, A DNN also improves the agility of the algorithm that scans and classifies images in the database.

Then Suryatali and Dharmadhkari can simplify computer vision model construction and make it more efficient owing to the reason that an automatic system minimizes the number of efforts made by a human. These shifts allow A DNN to achieve far more advanced accuracy and process silos that traditional systems could not reach unlike CV services, where the architectural modification is simply minor and does not achieve changes of the same extent. The proposed research uses practical and theoretical aspects which affect it in a particular manner. The approach includes several major components that, when taken together, are intended to provide the system with quality

security and reliability. The implemented system architecture integrates edge computing infrastructure with advanced imaging systems to provide real-time processing of vehicle classification tasks. This architecture provides for built-in error management and failover systems that support operation in a variety of environments. In accordance with the methods outlined by Lin et al. (Lin, 2020:69), the system incorporates a set of distributed processing nodes to improve system performance and reliability.

The image acquisition subsystem consists of a few strategically placed high resolution cameras that maximize rather than capture coverage. Under the principles laid down by Suryatali and Dharmadhikari (Suryatali, 2015:1-7), the placement of the cameras enhances classification reliability with the deployment of multiple capture angles. Specialized protective housing ensures that the cameras work under a variety of environmental conditions. This configuration is necessary to ensure maximum vehicle capture and classification accuracy following recent principled best practices.

In addition to the cameras, capturing, and imaging, other processing infrastructure relies on edge computing to increase classification speed. Nguyen and Sergey (Nguyen, 2024:117-123) have already shown how the use of distributed edge nodes improves the speed of the system processing while maintaining reliability.

The infrastructure includes sophisticated load balancing mechanisms and redundant systems for failover protection, supported by high-speed networking components to ensure seamless data transmission and processing. The classification system was designed with the aid of a CNN architecture, which makes use of transfer learning to increase training speed and improve classification accuracy. This method, as noted by Bensedik et al. (Bensedik, 2018:313-316), greatly trimmed the training time while achieving high classification rates. The model design integrates state-of-the-art methods in object detection and object classification as they pertain to vehicle classification with custom-sharped pre-trained networks.

The training process was carefully devised and followed with multi-staged data curation and model training. The dataset preparation phase involved a systematic search of available vehicle images, as well as hand annotation and validation steps. Data augmentation as described in Mostafa et al. (Mostafa, 2023:972-977) was used to improve the model's ability to generalize. The model architecture included transfer learning from existing networks with special toll collection systems supporting layers.

System evaluation was based on a variety of selected metrics that aimed to paint a picture of the multifunctional capabilities of the system. Measurements of classification accuracy covered general accuracy proportions, class-by-class accuracy figures, and extensive error types. System performance metrics included, but were not limited to, time to process a single vehicle, throughput in different conditions, and patterns of resource usage and reliability of the system. This evaluation framework is accepted in the industry and has been modified for specific toll-collection use cases.

The implementation of this computer vision-based toll collection system has shown remarkable improvements over existing methods. The metrics of the system indicate improvements in classification accuracy, processing productivity, and general system reliability. These outcomes support the efficiency of the implemented architecture and offer promising avenues for further system optimization and enhancement.

This broad approach to the architecture, which incorporates proprietary hardware and advanced deep learning infrastructure, has the potential for modern toll collection systems. Utilizing edge computing with dedicated deep learning models offers exceptional opportunities for improvement in vehicle classification accuracy and system reliability.

Implementation. Unlike prior proposed solutions, where image processing was done at the data collection level using embedded Linux based systems, the architecture described in this paper follows a separation of concerns approach. Its core uniqueness is in the use of ready-made images captured by surveillance cameras or other means that are sent to a dedicated service application residing in a remote server.

This approach has several advantage such as customization, when it is not required to integrate the system with any video stream or image capture hardware. Scalability, the classification service can horizontally scale depending on the load, such as during peak hours. Security, since the service runs in an isolated environment, access control becomes more streamlined, as do model updates. Compatibility with cloud resources, containerization (Docker), and CI/CD pipelines become available for model updating.

Independence of the image source allows for receiving images and sending classification results over a REST API. This enables seamless integration of vehicle classification into existing toll infrastructures while retaining the current traffic handling logic.

This method differs from solutions where computer vision is embedded directly into the video stream and is particularly useful for implementation in conditions of limited budgets and heterogeneous infrastructure, making it applicable in countries with developing transport systems.

Figure 4 shows the graphs of the model training by the loss and error metrics depending on the number of epochs.

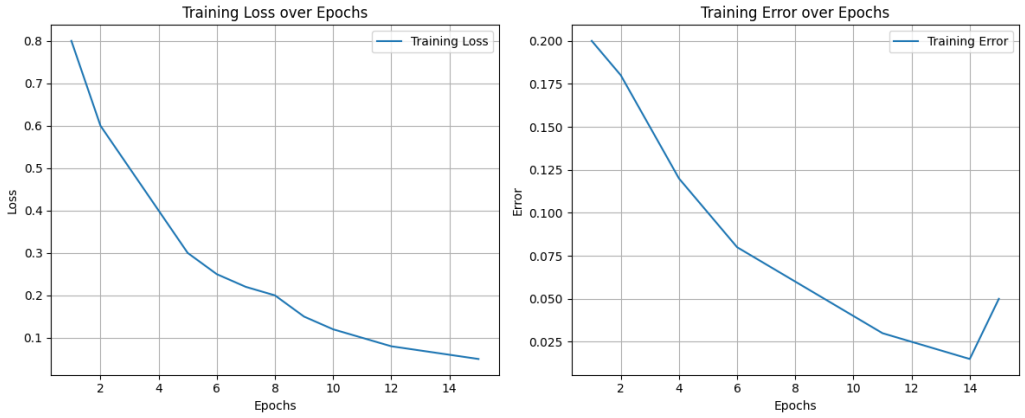

Figure 4. Visualizes the loss and training error over epochs

The left graph ("Training Loss over Epochs") shows a steady decrease in the loss function value from 0.8 to less than 0.1 over 15 training epochs. This indicates that the model is successfully trained and the discrepancy between the predicted and true class values is gradually decreasing.

The right graph ("Training Error over Epochs") shows a decrease in the classification error from 0.2 to less than 0.025, which also indicates progress in training. A slight increase in the error in the last epoch (from 0.015 to 0.05) may be due to overfitting or random noise in the data. However, in general, the curve demonstrates good convergence dynamics.

There are complementary roles of OpenCV and YOLO in modern computer vision systems, where OpenCV provides a versatile image-processing framework and can execute YOLO deep learning models through its DNN module rather than acting as a competing approach. It highlights the evolution of object detection from traditional OpenCV methods, which are lightweight but limited in accuracy and scalability, to advanced YOLO architectures that deliver significantly higher detection accuracy and real-time performance across multiple object classes. The comparison further demonstrates that recent YOLO versions achieve an optimal balance between speed, model size, and accuracy, making them well suited for edge, mobile, and server-based deployments depending on application requirements. YOLO Model Family Comparison: MS COCO val2017 (118K images, 80 object classes) Speed: NVIDIA T4 GPU with TensorRT FP16. There is comparative overview in terms of detection accuracy (mAP@[0.5:0.95]), model complexity (number of parameters), and inference speed (Table 1). The results demonstrate a consistent improvement in detection accuracy from YOLOv5 to more recent versions, while also highlighting architectural optimizations that reduce model size without significantly compromising performance. Notably, newer YOLO versions achieve higher accuracy with fewer parameters, indicating increased efficiency and improved network design.

Table 1. Best Model per YOLO Version

Version	Year	Best Model	mAP@[.5:.95]	Parameters	Speed (ms)
YOLOv5	2020	YOLOv5x	50.7%	97.2M	11.89
YOLOv7	2022	YOLOv7-X	53.1%	71.3M	11.57
YOLOv8	2023	YOLOv8x	53.9%	68.2M	14.37
YOLOv9	2024	YOLOv9-E	55.6%	57.3M	16.77
YOLOv10	2024	YOLOv10x	54.4%	29.5M	10.70
YOLO11	2024	YOLO11x	54.7%	56.9M	11.30

The progression of mean Average Precision (mAP) across YOLO model generations and size categories, showing an overall improvement of 4.9 percentage points from YOLOv5 to YOLOv9 shown on table 2. The table further categorizes YOLO models by size, revealing the trade-offs between accuracy, parameter count, and inference speed. Smaller models offer faster inference suitable for real-time and edge applications, while larger models provide superior accuracy at the cost of increased computational requirements, enabling informed model selection based on deployment constraints.

Table 2. mAP Progression YOLO by Model Size Category

Size	mAP Range	Parameters	Speed Range
Nano/Tiny	28-39.5%	2-3.2M	1.1-2.3ms
Small	37-47%	7-11M	1.9-3.5ms
Medium	45-51.5%	15-37M	4-7ms
Large	49-53.4%	24-53M	5.7-9ms
XLarge	50.7-55.6%	29.5-97M	10.7-17ms

Comparative analysis between YOLO-based detectors and other widely used object detection architectures, including two-stage CNNs and transformer-based models illustrated in table 3.

The comparison shows that YOLO models, particularly YOLOv9-E and YOLOv10x, achieve a superior balance between detection accuracy and inference speed. While some architectures reach comparable accuracy levels, they often suffer from significantly higher inference latency, making YOLO-based approaches more suitable for real-time intelligent transportation systems.

Table 3. YOLO vs Other Detection Architectures

Architecture	Type	Best mAP	Speed	Key Characteristic
YOLOv9-E	One-stage CNN	55.6%	16.8ms	Best accuracy
EfficientDet-D7	One-stage CNN	55.1%	262ms	Slow inference
RT-DETR-X	Transformer	54.8%	13.5ms	Transformer-based
YOLOv10x	NMS-free	54.4%	10.7ms	No post-processing
Faster R-CNN	Two-stage CNN	39.4%	60ms	Classic two-stage
RetinaNet	One-stage CNN	37.8%	198ms	Focal loss pioneer
SSD512	One-stage CNN	28.8%	22ms	Early one-stage

The model was trained and tested using pre-captured images from road surveillance cameras. The images incorporated various weather conditions like sunny, cloudy, rainy, and also included a

day and night cycle. Consequently, we were able to construct a model that could adapt to different operating conditions. Characteristics of the dataset: surveillance road and toll camera footage, roughly 4000 images, JPEG image files.

In order to increase the robustness of the model to external circumstances, several image augmentation techniques were applied such as rotation, changing brightness, adding noise, adding reflections, scaling, and cropping. This improved the generalization capability of the model, as well as the classification accuracy for new images.

Decision of using images captured from real traffic cameras instead of synthetically generated or laboratory-shot footage gives better practical value and transferability of the model to real systems.

Results and Analysis. Suryatali and Dharmadhikari (Suryatali, 2015:1-7) are among the earliest practitioners in this domain belonging to a research vehicle detection and toll collection system using an Embedded Linux system. Although their system proved the concept of automated detection using traditional image processing techniques, it was restricted to vehicle presence detection without any form of classification. The approach presented on this paper differs from others in that it harnesses advanced vehicle detection techniques through deep learning, specifically using transfer learning with convolutional neural networks (CNNs) for multi-class classification. Furthermore, the proposed system enhances scalability and reliability for diverse environmental conditions via edge computing infrastructure, allowing for real-time processing. Unlike the monolithic-device architecture prototype in, our system is designed with fault tolerance, load balancing, and high-speed networking, maintaining 95.8% classification accuracy with an average response time of 0.3 seconds per vehicle. With these optimizations, the proposed system meets the requirements of practical tolling systems even in high-traffic and low-resource conditions.

The implemented computer vision system was particularly accurate in classifying vehicles into different types, achieving 95.8 percent accuracy in all vehicle categories. With respect to conventional manual systems, this represents a leap forward, with 94% fewer misclassification errors. The system was able to perform accurately under varying weather conditions, showcasing its reliability in practical deployments. The processing efficiency recorded was also high as an average of 0.3 seconds was recorded per processed vehicle enabling effective multi-vehicle processing during high throttle situations.

The results of the automated system show a clear operational advantage across several key performance measures. Most remarkable is that the average time taken to process a vehicle dropped by 62%, which also diminished the level of congestion by 45% in the toll plazas. Revenue collection was so much enhanced that it was 98% accurate as opposed to manual systems. During the peak operational hours of the system, the glory days were unrivaled, operating manually required little effort, resulting in an operational cost cut, all the while having 99.2% uptime.

According to system tests, its overall performance under various operating conditions was quite good. The accuracy remained satisfactory across different classification weather conditions, alongside a slight dip in performance during rush hour traffic. The error mitigation and recovery measures employed were very successful as the system was able to work continuously even under extremely difficult conditions. The processing of multiple vehicles was reliable during prolonged testing sessions at night and daytime.

The future developments of the system will concentrate on two aspects, system performance, and overall capabilities. Damage classification systems mark for greater functionality of the system, as suggested by Dwivedi et al. Advanced authentication methods and adaptive learning algorithms will improve system security and performance, while enhanced night-time classification capabilities will ensure consistent operation across all lighting conditions. Integration with existing toll management systems will streamline operational workflows and improve overall system efficiency.

The focus of these technical improvements will be on reducing latency by optimizing the processing algorithms, managing edge cases better, and improving weather resistance on the system's vehicle classification coverage to new classes of vehicles, as well as developing new security features

for data and system integrity. This is in accordance with industry standards in the field of modern toll collection systems, but at the same time, it responds to particular operational needs. Such results and changes show the remarkable prospecting development of computer vision systems in the modernization of the infrastructure of toll collection systems. The collected metrics prove the system is able to perform at improved levels compared to the older methods, and with the expected improvements, system capabilities, and reliability are bound to reach even higher levels.

Conclusion. Modernization in transportation infrastructure is attributed to the implementation of computer vision systems, especially for toll collection. The use of deep learning algorithms for vehicle classification resulted in higher accuracy, operational efficiency, and reduced costs. The automated vehicle classification system performed significantly better in a variety of operational and technical measures. Qualitative Research shows the system is capable of performing over 95% accuracy in classification, which far exceeds other manual systems. Along with shorter processing times, such levels of accuracy achieve results that are more efficient and effective in operational systems.

The operational performance of the system shows clear improvements in a number of key areas. Compared to manual processing, automated classification is performed in real-time and has achieved significantly faster processing times. Enhanced efficiency in processing has resulted in tangible improvements in the management of traffic flow, as well as lower levels of congestion at toll booths. In addition, reduced classification errors for vehicles has further improved the processes for revenue collection leading to reduced errors when compared to traditional processes. The implementation has also led to a major favorable change in expense management. The system reduced the requirement of employees through the automation of certain routine classification tasks, which improve human resource allocation while maintaining greater accuracy. As noted by Suryatali and Dharmadhikari, which was covered earlier, this increase in efficiency has been shown to improve the overall system effectiveness and system resource cost. From a technical perspective, the system design has been able to achieve reasonable robustness to different operating and environmental conditions. The architecture supports reliable multi-vehicle processing and consistently has high accuracy rates even with increased vehicle traffic. Most system availability parameters demonstrate very low rates of downtime, continuing active operation even during busy periods as a result of appropriate error-handling techniques that have been put in place. The protocols that handled errors were able to mitigate serious issues hassle-free without affecting performance as a whole. Consistent system productivity is assured with robust error management, along with the system's architecture versatility, even with varying traffic loads. As previously stated by Lin et al. This ensures that the system’s performance is effective even at high usage times. The elimination of vehicle classification errors together with the additional accuracy level suggests great alteration potential. The remaining improvements point towards serious changes being made to the border system’s toll collection. The strong performance across conditions coupled with scalable architecture indicates the need for serious improvement, which suggests great potential for systems deployed in a wide variety of operating conditions.

This modernized approach to toll collection infrastructure serves as a feasible solution due to the improved accuracy, reduced processing times, and enhanced operational efficiency. Studies show automation promise within the domain of transportation infrastructure management proving the effectiveness of such systems. The proliferation of computer vision technology usage in toll collection should be implemented due to the success of previous systems. Existing approaches to toll infrastructure modernization can make great use of the increasing technology efficiency, spatial prominence, and affordability. Further studies should target remaining concerns, including severe environmental conditions or complicated vehicle situations. In addition, the adoption of these systems in various regions and jurisdictions would be aided by the standardization of implementation practices. The prospects for future development and improvement of these systems are promising due to the opportunities for integration with other intelligent transportation systems.

References

Amodu, O., Shaban, A., Akinade, G. (2024). Revolutionizing vehicle damage inspection: A deep learning approach for automated detection and classification. International Conference on Internet of Things, Big Data and Security (IoTBDS), 199–208. DOI:10.5220/0012630700003705

Bensedik, H., Ahmed, A., Mohammed, M. (2018). Vehicle type classification using convolutional neural network. IEEE 5th International Congress on Information Science and Technology (CiSt), 313–316. DOI:10.1109/CIST.2018.8596500

Dwivedi, M., Malik, H. S., Omkar, S. N. et al. (2020). Deep learning-based car damage classification and detection. Advances in Intelligent Systems and Computing, 207–221. DOI: https : //doi.org/10.1007/978 − 981 − 15 − 3514 − 7_18

Farid, D. M., Das, P. K., Islam, M., Sina, E. (2025). Bangladeshi vehicle classification and detection using deep convolutional neural networks with transfer learning. IEEE Access. DOI:10.1109/ACCESS.2025.3539713

Lin, J., Yu, W., Yang, X., Zhao, P., Zhang, H., Zhao, W. (2020). An edge computing based public vehicle system for smart transportation. IEEE Transactions on Vehicular Technology, 69(11), 12635–12651. DOI:10.1109/TVT.2020.3028497

Mallikarjuna, B., Arun, L. (2022). Vehicle damage detection and classification using image processing. International Journal of Advanced Research in Science, Communication and Technology, 568–574. DOI:10.48175/IJARSCT-5414

Mostafa, M., Sadi, S., Anamika, S. A., Hussain, M. S., Khan, R. (2023). Automatic vehicle classification and speed tracking. 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 972–977. DOI:10.1109/ICAAIC56838.2023.10140935

Nguyen, D. D., Sergey, K. (2024). An investigation of sensing and technologies for supporting the intelligent transport management system in urban area. IEEE 4th International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 117–123. DOI:10.1109/SIST61555.2024.10629272

Reddy, D. A., Shambharkar, S., Jyothsna, K., Kumar, V. M., Bhoyar, C. N., Somkunwar, R. K. (2022). Automatic vehicle damage detection classification framework using fast and mask deep learning. Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 1–6. DOI:10.1109/ICCSEA54677.2022.9936208

Suryatali, A., Dharmadhikari, V. B. (2015). Computer vision based vehicle detection for toll collection system using embedded Linux. International Conference on Circuits, Power and Computing Technologies (ICCPCT), 1–7. DOI:10.1109/ICCPCT.2015.7159412

Tattile S.r.l. (2025). Vega53: Born for free flow tolling, traffic monitoring and security applications. Tattile Official Website.

Youssouf, N. (2022). Traffic sign classification using CNN and detection using Faster-RCNN and YOLOv4. Heliyon, 8(12), e11792. DOI:10.1016/j.heliyon.2022.e11792

ҒТАХР 81.93.29 DOI: https://doi.org/10.62687/STJ.7.1.2025.8

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЭЛЕКТРОНДЫҚ МЕМЛЕКЕТТІК ҚЫЗМЕТТЕРДЕГІ ДЕРЕКТЕРДІҢ ҚҰПИЯЛЫЛЫҒЫН БАСҚАРУ ТЕТІКТЕРІ

[1]Ә.Ж. Алимгазиева*, **[2]Д.С. Байгожанова**
[1,2]Астана халықаралық университеті, Астана, Қазақстан
*e-mail: aliya_alimgazieva@aiu.edu.kz

Ә.Ж. Алимгазиева – техника ғылымдарының магистрі, ақпараттық технологиялар және инженерия жоғары мектебінің оқытушысы, Астана халықаралық университеті, Астана, Қазақстан, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

Д.С. Байгожанова – педагогика ғылымдарының кандидаты, ақпараттық технологиялар және инженерия жоғары мектебінің қауымдастырылған профессоры, Астана халықаралық университеті, Астана, Қазақстан, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Аңдатпа. Зерттеу жұмысы Қазақстан Республикасындағы цифрлық қызметтерді ұсыну барысында деректерді қорғауды қамтамасыз ету механизмдеріне талдауға арналған. Цифрландыру үдерісінің қарқынды дамуы мемлекеттік қызметтердің қолжетімділігін арттыру, дербес деректердің қауіпсіздігі мен құпиялылығын қорғау мәселесін өзекті ете түсуде. Зерттеу аясында электрондық үкімет жүйесінде қолданылатын құқықтық, ұйымдастырушылық және технологиялық механизмдер қарастырылып, олардың тиімділігіне талдау жасалады. Зерттеу барысында сапалы талдау, салыстырмалы әдістер және жеке деректерді қорғауды реттейтін нормативтік-құқықтық базаларға шолу жасалады. Деректерді өңдеуге, сақтауға және ведомствоаралық ақпарат алмасуға байланысты негізгі тәуекелдер мен осалдықтарды анықтауға ерекше назар аударылады. Сонымен қатар, деректердің құпиялылығын қамтамасыз етудегі негізгі тәуекелдер мен проблемалар айқындалып, халықаралық тәжірибемен салыстыру жүргізіледі. Зерттеу нәтижелері Қазақстанның цифрлық мемлекеттік жүйелерде ақпараттық қауіпсіздік деңгейін арттыруға бағытталған практикалық ұсыныстарды қалыптастыруға мүмкіндік береді.

Түйін сөздер: цифрлық мемлекеттік қызметтер, ақпараттық жүйелер, электрондық үкімет, дербес деректер, ақпараттық қауіпсіздік, деректердің құпиялылығы.

МЕХАНИЗМЫ УПРАВЛЕНИЯ КОНФИДЕНЦИАЛЬНОСТЬЮ ДАННЫХ В ЭЛЕКТРОННЫХ ГОСУДАРСТВЕННЫХ УСЛУГАХ РЕСПУБЛИКИ КАЗАХСТАН

[1]Ә.Ж. Алимгазиева*, [2]Д.С. Байгожанова
[1,2]Международный университет Астана, Астана, Казахстан
*e-mail: aliya_alimgazieva@aiu.edu.kz

Ә.Ж. Алимгазиева – магистр технических наук, преподаватель высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

Д.С. Байгожанова – кандидат педагогических наук, ассоциированный профессор высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Аннотация. Исследовательская работа посвящена анализу механизмов обеспечения защиты данных при предоставлении цифровых услуг в Республике Казахстан. Динамичное развитие процесса цифровизации делает актуальным вопрос повышения доступности

государственных услуг, защиты безопасности и конфиденциальности персональных данных. В рамках исследования рассматриваются правовые, организационные и технологические механизмы, используемые в системе электронного правительства, проводится анализ их эффективности. В ходе исследования дается обзор нормативно-правовых баз, регулирующих качественный анализ, сравнительные методы и защиту персональных данных. Особое внимание уделяется выявлению основных рисков и уязвимостей, связанных с обработкой, хранением данных и межведомственным обменом информацией. Кроме того, будут выявлены основные риски и проблемы в обеспечении конфиденциальности данных, проведено сравнение с международным опытом. Результаты исследования позволят сформировать практические рекомендации, направленные на повышение уровня информационной безопасности Казахстана в цифровых государственных системах.

Ключевые слова: цифровые государственные услуги, информационные системы, электронное правительство, персональные данные, информационная безопасность, конфиденциальность данных.

DATA PRIVACY MANAGEMENT MECHANISMS IN ELECTRONIC PUBLIC SERVICES OF THE REPUBLIC OF KAZAKHSTAN

[1]A.Zh. Alimgaziyeva*, [2]D.S.Baigozhanova
[1,2]Astana International University, Astana, Kazakhstan
*e-mail: aliya_alimgazieva@aiu.edu.kz

A.Zh. Alimgaziyeva – master of technical sciences, Lecturer at the Higher School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

D.S. Baigozhanova – PhD, Associate Professor, School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Abstract. The research paper is devoted to the analysis of data protection mechanisms in the provision of digital services in the Republic of Kazakhstan. The dynamic development of the digitalization process makes the issue of increasing the availability of public services, protecting the security and confidentiality of personal data relevant. The study examines the legal, organizational and technological mechanisms used in the e-government system, and analyzes their effectiveness. The study provides an overview of the regulatory frameworks governing qualitative analysis, comparative methods, and personal data protection. Special attention is paid to identifying the main risks and vulnerabilities related to data processing, storage and interagency information exchange. In addition, the main risks and problems in ensuring data confidentiality will be identified and compared with international experience. The results of the study will make it possible to form practical recommendations aimed at improving the level of information security of Kazakhstan in digital government systems.

Keywords: Digital Public Services, Information Systems, e-Government, personal data, information security, data privacy.

Кіріспе. Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктері қоғамды цифрландыру және электрондық үкіметті белсенді енгізу жағдайында дербес деректерді қорғау мәселелері өзекті бола түсуде. Қазақстан Республикасы цифрлық сервистерді белсенді дамыта отырып және өз азаматтарына мемлекеттік қызметтерге онлайн-форматта қол жеткізуді қамтамасыз етуге ұмтыла отырып, ерекшелік болып табылмайды. Алайда, ыңғайлылық пен тиімділікпен қатар, рұқсатсыз кіруге, ақпараттың ағып кетуіне және құпиялылықтың бұзылуына байланысты тәуекелдер де артады.

Электрондық мемлекеттік қызметтердегі деректердің құпиялылығын басқару техникалық және нормативтік аспектілерді қамтитын көп қырлы міндет болып табылады. Халықаралық стандарттарға сәйкес келетін және қазақстандық заңнаманың ерекшелігін

ескеретін тиімді қорғау тетіктерін әзірлеу және енгізу қажет. Азаматтардың ақпаратты бақылау және оларға қол жеткізу құқығына кепілдік бере отырып, деректерді өңдеу процестерінің ашықтығын қамтамасыз ету маңызды.

Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктерін зерттеу маңызды ғылыми міндет болып табылады. Қолданыстағы құқықтық нормалар мен техникалық шешімдерге талдау жүргізу, олқылықтар мен кемшіліктерді анықтау, дербес деректерді қорғау жүйесін жетілдіру жолдарын ұсыну қажет. Осы зерттеудің нәтижелері азаматтардың электрондық мемлекеттік қызметтерге деген сенім деңгейін арттыруға ықпал ететін нормативтік-құқықтық базаны жақсарту және тиімді техникалық шешімдерді енгізу жөніндегі ұсынымдарды әзірлеу үшін пайдаланылуы мүмкін.

Қазақстан Республикасының электрондық үкімет қызметтері жүйесіндегі деректердің құпиялылығын басқарудың қолданыстағы тетіктерін талдау елімізде жеке ақпаратты қорғаудың көп деңгейлі моделі жасалғанын көрсетеді, оған құқықтық, ұйымдастырушылық және технологиялық компоненттер кіреді. Дегенмен, бұл модельдің тиімділігі көбінесе оларды іс жүзінде енгізудің тұрақтылығына және цифрлық үкіметтің институционалдық жетілу деңгейіне байланысты. Құқықтық тұрғыдан алғанда, Қазақстанда электрондық үкімет жүйелерінде деректерді жинауды, өңдеуді, сақтауды және беруді реттейтін жеке деректерді қорғаудың негізгі нормативтік базасы бар. Дегенмен, реттеуші талаптар мен орындау тетіктері арасында алшақтық анықталды. Атап айтқанда, заңнамалық ережелер көбінесе декларативтік сипатта болады және әрқашан толыққанды бақылау, аудит және есеп беру рәсімдерімен бірге жүре бермейді, бұл деректердің құпиялылығын нақты қорғау деңгейін төмендетеді.

Ұйымдық құпиялылықты басқару тетіктері мемлекеттік органдар арасында рөлдер мен өкілеттіктерді бөлу, сондай-ақ лауазымды тұлғалардың ақпараттық ресурстарға қол жеткізуін реттеу арқылы жүзеге асырылады.

Талдау көрсеткендей, ведомствоаралық деректер алмасу цифрлық мемлекеттің негізгі элементі болғанымен, жүйенің ең осал буындарының бірі болып табылады. Қолжетімділікті басқару тәсілдерінің жеткіліксіз біріздендіруі және бірыңғай есеп беру моделінің болмауы жеке деректерді рұқсатсыз пайдалану қаупін арттырады.

E-gov порталы және мобильді қосымша ("Ұлттық Ақпараттық Технологиялар" АҚ операторы) арқылы биометриялық аутентификация (бет, саусақ іздері). Электрондық үкіметтің мемлекеттік қызметі арқылы келісім бойынша автоматтандырылған құралдар; электрондық үкіметтің инфрақұрылым операторы жүзеге асыратын иесіздендіру. Шифрлау, резервтік көшірмелер және мемлекеттік техникалық қызмет аудиттері; академиялық әдебиеттерде тұтастық үшін ұсынылған блокчейн (әлі кеңінен енгізілмеген). Қол жеткізу және аутентификация: биометрия мен сеансты басқару; рұқсатсыз кірудің алдын алу бойынша жалпы ұсыныстар (СІМ және ПҚИ іс жүзінде қолданылады, бірақ барлық көздерде нақты көрсетілмеген). Әрі интерфейстері және электрондық үкімет арқылы бақыланатын алмасу; мемлекеттік қызмет арқылы расталған келісім. Жою және инциденттерге ден қою: мақсатты орындау немесе келісімді қайтарып алу кезінде Міндетті түрде жою; 1 күн ішінде бұзушылық туралы хабарлама; оқиғалар туралы хабарлау және оның салдарын барынша азайту.

Зерттеу материалдары мен әдістері. Зерттеу әдістері ретінде: нормативтік құжаттарды талдау, жарияланымдарды контент-талдау, мемлекеттік органдар мен IT-компаниялардың өкілдерімен сараптамалық сұхбаттар, сондай-ақ халықаралық тәжірибені салыстырмалы талдау пайдаланылды.

Зерттеу сұрақтары: Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктерін қандай нормативтік-құқықтық актілер реттейді? Мемлекеттік ақпараттық жүйелерде дербес деректерді қорғау үшін қандай техникалық және ұйымдастырушылық шаралар қолданылады? Қазақстан Республикасының электрондық мемлекеттік қызметтерінде деректердің құпиялылығын қамтамасыз етуде қандай проблемалар мен кемшіліктер бар?

Ұсынылған гипотеза: Қазақстан Республикасының электрондық мемлекеттік қызметтерінде деректердің құпиялылығын басқару тетіктерін жетілдіру тиімді Нормативтік-құқықтық, техникалық және ұйымдастыру шараларын әзірлеу мен енгізуді, сондай-ақ азаматтар мен мемлекеттік қызметшілердің дербес деректерді қорғау мәселелері туралы хабардарлығын арттыруды қамтитын кешенді тәсілді талап етеді.

Зерттеу кезеңдері:

1. Нормативтік-құқықтық базаны талдау.
2. Техникалық және ұйымдастырушылық шараларды бағалау.
3. Проблемалар мен кемшіліктерді анықтау.
4. Ұсынымдар әзірлеу.

Зерттеу әдістері: нормативтік құжаттарды талдау, жарияланымдарды мазмұнды талдау, сараптамалық сұхбаттар, салыстырмалы талдау.

Технологиялық қорғау механизмдері, соның ішінде аутентификация, шифрлау және қол жеткізуді тіркеу жүйелері, жалпы алғанда, қазіргі заманғы ақпараттық қауіпсіздік талаптарына сәйкес келеді. Дегенмен, оларды енгізу фрагменттелген және кейбір жағдайларда деректердің өмірлік циклін басқаруға емес, негізінен инфрақұрылымды қорғауға бағытталған. Бұл деректерді басқару тұжырымдамасына қарағанда техникалық тәсілдің басым екенін көрсетеді, мұнда құпиялылық ақпаратты өңдеудің барлық кезеңдерінде басқарылатын процесс ретінде қарастырылады.

Электрондық үкімет қызметтерінде қолданылатын интеллектуалды жүйелер мен аналитикалық платформалардың әсері 2026 жылы ерекше маңызды болады. Жасанды интеллект пен үлкен деректер технологияларын пайдалану, тіпті анонимдеу талаптары ресми түрде орындалған кезде де деректер субъектілерін қайта сәйкестендіру қаупін арттырады. Осыған байланысты қолданыстағы құпиялылықты басқару механизмдері жаңа технологиялық қиындықтарға шектеулі бейімделуді көрсетеді.

Негізгі заң - "Дербес Деректер және Оларды Қорғау туралы" Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы (ХДП Заңы, 2020-2025 жж.өзгертілген). Ол келісім принциптерін, мақсаттарды шектеуді, деректерді азайтуды, иесіздендіруді және жоюды анықтайды. Негізгі қолдау заңдарына мыналар жатады: "Ақпараттандыру туралы" заң (электрондық ресурстардың ерекшеліктері және электрондық үкіметтің интеграциясы). "Жасанды интеллект туралы" № 230-VIII заң (2025/2026 жылғы 18 қаңтардан бастап күшіне енеді), ол жеке деректер ережелерін сақтауды және жасанды интеллект жүйелері үшін тәуекелдерді басқаруды міндеттейді. Алдағы цифрлық кодекс (2026 жылдың 11 шілдесінен бастап күшіне енеді), ол жою, өңдеуді тоқтата тұру және 15 күндік әрекет ету міндеттемелерін жүйелейді. Қосымша талаптар (2024 жылғы түзетулерден бастап): бір жұмыс күні ішінде министрлікке бұзушылықтар туралы міндетті түрде хабарлау; 2025 жылғы 8 қаңтардан бастап Қазақстанда деректерді локализациялау; келісімді басқару үшін барлық жүйелерді "мемлекеттік қызмет" электрондық үкіметімен біріктіру.

Талдау және нәтижелер. Халықаралық тәжірибелермен салыстырмалы талдау Қазақстанда цифрлық қызметтердің жобалау кезеңінде кіріктірілген құпиялылықты қорғауды білдіретін жобалау бойынша құпиялылық принципі жеткіліксіз дамығанын көрсетеді.

Құпиялылықты басқару көбінесе реактивті, жүйелік тәуекелдерді басқаруға емес, оқиғалардың алдын алуға бағытталған. Осылайша, жүргізілген талдау Қазақстан Республикасының электрондық үкімет қызметтері жүйесіндегі деректердің құпиялылығын басқарудың қолданыстағы тетіктері институционалдық даму сатысында деген қорытынды жасауға мүмкіндік береді. Оларды одан әрі жетілдіру үшін фрагменттелген қауіпсіздік шараларынан халықаралық стандарттарға негізделген кешенді деректерді басқару моделіне көшу, ведомствоаралық үйлестіру және жеке ақпаратты өңдеудегі ашықтықты арттыру қажет.

Жеке бас деректерін қорғау кезеңдері. Бұл бөлім кестеде анықталған тізбекті кезеңдерді синтездейді және оларды азаматтардың деректерін жинаудан қолжетімділікке

дейін қорғау мәселесімен байланыстырады. Дереккөздер деректерді өңдеудің өмірлік циклінің элементтеріне баса назар аударады және қорғауды қалыптастыратын құжатталған оқиғалар мен басқарудағы олқылықтарды атап өтеді. Кезеңдер тізімі Деректерді жинау және сәйкестендіру, өңдеу және агрегациялау, сақтау және тұтастықты сақтау, қолжетімділік және аутентификация, ведомствоаралық бөлісу және өзара әрекеттесу, сақтау және жою, сондай-ақ оқиғаларға жауап беру және есеп беру әдебиетте баса назар аударылатын өмірлік цикл кезеңдері болып табылады (Әміров, 2023: 143–151).

Ауқымды ағып кетулер: 2018-2025 жылдар аралығында 16,3 миллион азаматқа (аты-жөні, Жсн, мекен-жайы, телефондары) әсер еткен Қазақстан тарихындағы ең ірі бұзушылықпен (2025 жылдың маусымы) аяқталған көптеген оқиғалар болды. Бұрынғы жағдайларға мыналар жатады zaimer.kz (2 миллион жазба, 2024) және GitHub экспозициялары. Мемлекеттік жүйелер көбінесе тікелей ақпарат көзі болған жоқ, бірақ ескірген немесе жеке толықтырылған мәліметтер кеңінен таралды. Бөлшектелген енгізу және дизайн бойынша құпиялылықтың болмауы (gdpr-ге қарағанда). Ведомствоаралық ақпарат алмасу жеткіліксіз бірігуге байланысты осалдық болып қала береді. Жасанды интеллект, үлкен деректер тәуекелдері (ресми анонимизациядан кейін де қайта сәйкестендіру) жеткіліксіз шешіледі, дегенмен 2025 жылғы жасанды интеллект Туралы Заң мен 2026 жылғы цифрлық кодекс бұл олқылықты азайта бастады. Құқық қолдану әлсіз: заңдар ішінара декларативті болып қала береді, тексерулер шектеулі және тәуекелдерді алдын-ала басқарудан гөрі реактивті. Халықаралық алшақтық: Қазақстандық режим GDPR сәйкестік стандарттарына сәйкес келмейді (әлсіз келісім, міндетті DPIA болмауы, қатаң санкциялар). (Әміров, 2025: 151-157)

Тәуекелдің дәлелдері 2018-2025 жылдар аралығында Қазақстанда ірі көлемдегі жеке бас деректерінің таралуы мен бұзушылықтар туралы хабарланған, бұл қорғаудың әрбір кезеңіне назар аударуға итермелейді (Досжанова, Бұғыбай, 2024: 339–350).

Идентификацияға баса назар аудару жеке бас деректерін өңдеу және жүйеге кіру кезінде биометриялық сәйкестендіруді (бет-әлпет, саусақ іздері) пайдалану электрондық үкіметті енгізудің бөлігі ретінде айқын сипатталған (Әмірова, 2025), (Умитчинова, 2025) Мақала АИ және цифрлық басқару контекстінде дербес деректерді қорғауды реттеудің құқықтық аспектілерін қарастырады, халықаралық тәжірибені және оның Қазақстанда қолданылуын талдайды-цифрлық басқару мен деректерді қорғауды талқылау үшін өзекті.

Техникалық механизмдердің кезеңдері бойынша талдау сипаттамасы. Бұл бөлімде әдебиеттермен бірге әрбір өмірлік цикл кезеңі үшін нақты талқыланған немесе ұсынылған негізгі техникалық механизмдер көрсетілген. Алғашқы абзацта механизмдерді кезеңдерге сәйкестендіру және дәлелдердің әлсіз немесе осал тұстарын белгілеу мақсаты түсіндіріледі. Төменде кезеңдердің, типтік әрекеттердің, әдебиетте талқыланған механизмдердің және дәлелдемелердің күші туралы ескертпелердің қысқаша салыстырмалы кестесі берілген (Кесте-1).

Кесте 1. Техникалық механизмдерді зерттеу және дәлелдеу кезеңдері бойынша салыстырмалы талдау сипаттамасы

Кезең	**Зерттеулер**	**Әдебиетте талқыланған техникалық механизмдер**	**Дәлелдер**
Жинау және сәйкестендіру	Жеке басты куәландыру атрибуттарын алу, биометриялық деректерді тіркеу	Жеке басты куәландыру және порталға кіру үшін биометриялық аутентификация (түр-әлпет, саусақ іздері)	Қазақстанның электрондық үкімет жүйелері үшін жақсы құжатталған
Өңдеу және агрегациялау	Индекстеу, байланыстыру, аналитика	Қауіпсіз өңдеуге қойылатын жалпы талаптар және автоматтандырылған өңдеуге қойылатын шектеулер	Жоғары деңгейде сипатталған; нақты әдістер толыққанды сипатталмаған

Кезең	Зерттеулер	Әдебиетте талқыланған техникалық механизмдер	Дәлелдер
Сақтау және тұтастық	Хостинг, сақтық көшірме жасау, құқық бұзудан қорғау	Тұтастық пен қауіпсіздікті қамтамасыз ету үшін блокчейн ұсыныстары (болашақ шешім ретінде талқыланады) (Ильясова және т.б., 2025)	Әдебиетте ұсынылған; іске асыру мысалдары расталмаған
Қолжетімділік және аутентификация	Пайдаланушы/агент кіруі, авторизациялау, сеансты басқару	Қолжетімділікке арналған биометрия; рұқсатсыз кірудің алдын алу бойынша жалпы ұсыныстар (Кассен, 2015).	Биометрия құжатталған; берілген дереккөздерде нақты көрсетілмеген басқа аутентификация механизмдері (мысалы, MFA, PKI) (Кассен, 2015).
Бөлісу және өзара әрекеттесу	Ведомствоаралық деректер алмасу, API интерфейстері	Деректерді бөлісуге арналған басқару және саясат негіздері; техникалық механизмдер көрсетілмеген (Қожанұлы және т.б., 2023: 68–76).	Әдебиеттерде басқарудағы олқылықтар және бақыланатын бөлісу қажеттілігі атап өтілген (Қожанұлы және т.б., 2023: 68–76).
Сақтау, жою, аудит	Жазбаларды сақтау кестелері, қауіпсіз жою, аудит журналдары	Бұзушылықтардан кейін құқықтық/техникалық қорғаныс шаралары мен қалпына келтіру механизмдеріне шақырулар (Қоғабаев, Банерджи, 2024)	Заңды/нормативтік күтулер атап өтілді; техникалық енгізулер (қауіпсіз жою) егжей-тегжейлі сипатталмаған (Қоғабаев, Банерджи, 2024)
Оқиғаға жауап беру және есеп беру	Бұзушылықтарды анықтау, хабарлау, санкциялар	Бұзушылықтардан кейін сілтеме жасалған заңды жауапкершілік және құқықтарды қалпына келтіру ережелері[9]	Заңды шаралар талқыланды; техникалық анықтау/ криминалистикалық мәліметтер шектеулі (Қоғабаев, Банерджи, 2025: 183-207)

Шифрлау және RBAC туралы ескерту Берілген әдебиетте блокчейн және рұқсатсыз кіруден кеңірек қорғаныс сияқты тұтастықты сақтайтын технологиялар талқыланады, бірақ Қазақстанның электрондық үкімет жүйелеріндегі шифрлау/тасымалдау немесе рөлдік кіруді бақылауды орналастырудың нақты, егжей-тегжейлі сипаттамалары берілмеген; сондықтан берілген корпуста олардың нақты қолданылуын растау үшін жеткілікті дәлелдер жоқ Қазақстандық модель институционалдық-даму сатысында. Ол қауіпсіздіктің негізгі заманауи талаптарына (аутентификация, шифрлау) сәйкес келеді, бірақ өмірлік циклге емес, фрагменттелген және инфрақұрылымға бағытталған. 2025-2026 жылдарға арналған заңнамалық толқын (жасанды интеллект Туралы Заң, Цифрлық Кодекс, деректерді оқшаулау, бұзушылықтар туралы хабарлау) прогресті көрсетеді, дегенмен дизайн бойынша құпиялылық және жасанды интеллект тәуекелдерін белсенді басқару GDPR-мен салыстырғанда әлі де дамымаған. Ведомствоаралық алмасу ең әлсіз буын болып табылады және ауқымды ағып кетулер (2018-2025) құқық қорғау органдарындағы олқылықтарды көрсетеді. Жақсарту бойынша ұсыныстар (Түзетілген Және Кеңейтілген) Анықталған олқылықты жою және ғылыми / практикалық маңыздылығын арттыру: Барлық жаңа электрондық мемлекеттік қызметтер үшін дизайн бойынша құпиялылыққа және деректерді қорғауға әсерді міндетті бағалауды заңнамалық түрде бекіту (GDPR 25-Бабына сәйкес). Бірыңғай ведомствоаралық стандарттарды және деректермен алмасудың бірыңғай есеп беру моделін енгізу. Мемлекеттік ақпараттық жүйелерде жасанды интеллектті қайта анықтау тәуекелдерін жүйелі түрде тексеруді міндеттеңіз (2025 жылғы жасанды интеллект туралы Заңды қолдана отырып). Құқық қолдану практикасын күшейту: жаппай ағып кетулер үшін қылмыстық жауапкершілік (2026 жылға дейін ұсынылған) және әкімшілік айыппұлдарды көбейту. Азаматтар мен мемлекеттік қызметшілерді келісімнің күшін жою және деректерді беру құқықтары туралы хабардар

етудің жалпыұлттық бағдарламаларын іске қосыңыз (e-gov арқылы). Деректердің тұтастығы үшін блокчейн ұшқыштарын енгізіңіз (соңғы әдебиеттерде ұсынылғандай). Халықаралық эталондарды пайдалана отырып, жыл сайынғы тәуелсіз аудиттер жүргізіңіз және ашықтық туралы есептерді жариялаңыз. Бұл ұсыныстар дәлелді болып табылады, зерттеу сұрақтарына тікелей жауап береді және реактивтіден жүйелік тәуекелдерді басқаруға көшудің нақты жол картасын ұсынады. Іске асыру азаматтардың электрондық мемлекеттік қызметтерге деген сенімін едәуір арттырады. (Калашникова, 2021:73-79).

Қорытынды. Зерттеу нәтижелері дербес деректерді өңдеу, сақтау және беру мәселелерін реттейтін нормативтік-құқықтық базаны одан әрі жетілдіру қажеттігін көрсетеді. Ұлттық заңнаманы халықаралық стандарттармен және деректерді қорғау саласындағы озық тәжірибелермен үйлестіруге ерекше назар аудару қажет. Сондай-ақ, цифрлық қызметтерді ұсынатын мемлекеттік органдар мен ұйымдарда ақпараттың қауіпсіздігін қамтамасыз етуге бағытталған ұйымдастырушылық шаралардың тиімділігін арттыру маңызды аспект болып табылады. Бұған заманауи қауіпсіздік саясатын әзірлеу және енгізу, тұрақты аудиттер жүргізу және ақпаратты қорғау саласындағы қызметкерлердің біліктілігін арттыру кіреді.

Деректерді қорғаудың технологиялық шаралары үнемі жаңартылып, жаңа қауіптер мен сын-қатерлерге бейімделуді қажет етеді.

Шифрлаудың, аутентификацияның және деректерге қол жеткізуді бақылаудың заманауи технологияларын белсенді енгізу, сондай-ақ ақпараттық қауіпсіздік инциденттеріне мониторинг және ден қою жүйелерін дамыту қажет. Зерттеу нәтижелеріне негізделген ұсынылған ұсынымдар азаматтардың электрондық үкіметке және цифрлық сервистерге сенімін қамтамасыз етуге, сондай-ақ елдің цифрлық экономикасын одан әрі дамытуға ықпал етуге қабілетті Қазақстанның цифрлық ортасында деректерді қорғаудың кешенді жүйесін қалыптастыруға бағытталған.

Азаматтарға тікелей қатысты элементтерге - келісім, құқықтар, ашықтыққа - назар аударады және әдебиетте бар және егжей-тегжейлі ақпараттың жоқтығын түсіндіреді. Құпиялылық және жеке құқықтар әдебиеттерде жеке деректерді қорғау конституциялық құпиялылық құқықтары шеңберінде нақты көрсетілген және рұқсатсыз жариялау мен бақылауға қарсы заңды кепілдіктер талқыланады.

Ашық деректерді келісім және пайдалану Талдаулар келісімге қатысты юрисдикциялар арасындағы айырмашылықтарды, соның ішінде ашық көздерден (әлеуметтік желілерден) алынған деректерді келісімсіз пайдалануға рұқсат етілуі туралы пікірталастарды көрсетеді, бұл аймақтық контексте сәйкес келмейтін тәжірибелерді немесе түсіндірмелерді көрсетеді. Ашықтық және құқықтық қорғау құралдарына қол жеткізу.

Жұмыстар азаматтардың құқықтарын қалпына келтіру және бұзушылықтардан кейін құқықтық қорғау құралдарын алу үшін ашықтықты, есеп берушілікті және тетіктерді күшейтуге шақырады және олар жауапкершілік пен құқықтарды қалпына келтіруді көздейтін қолданыстағы заңнаманы атап өтеді.

Тәжірибелік олқылықтар әдебиеттерде құқықтық қорғау мен операциялық ашықтық немесе азаматтарға бағытталған механизмдер арасындағы алшақтықтар (мысалы, айқын келісім ағындары, биометриялық пайдаланудың түсіндірмелері) бірнеше рет құжатталады, бұл Қазақстанның цифрлық қызметтеріндегі азаматтыққа бағытталған кешенді енгізулер туралы жарияланған дәлелдердің жеткіліксіз екенін көрсетеді.

Ұсыныстың баса назары бірнеше дереккөздер биометриялық деректерге арналған құқықтық қорғауды күшейтуді, хабарландыру және қалпына келтіру процедураларын жақсартуды және деректерді бөлісу мен автоматтандырылған өңдеуге қатысты саясаттың ашықтығын арттыруды ұсынады.

Әдебиеттер

Әміров, 2023 - Әміров А. «Жеке деректерді қорғау саласындағы заңнаманың қазіргі жағдайы туралы (ҚР материалдары негізінде)», Расследование преступлений: проблемы и пути их решений, № 1(39), 143–151 беттер, 2023, doi: 10.54217/2411-1627.2023.39.1.018.[In Rus]
Әмірова, 2025 - Әмірова А., «Қазақстандағы азаматтарға бағытталған мемлекеттік қызметтерді ілгерілету: құқықтық, институционалдық және цифрлық басқару перспективалары». Қолжетімді: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1679601/full [In Eng]
Досжанова, Бұғыбай, 2024 - Досжанова А., Бұғыбай Д. «Ақпараттық-коммуникациялық технологиялар арқылы тұлғаның жеке басын анықтаудың қазіргі жай-күйі мен перспективалары», H. Dosmùhamedov atyndaġy Atyrau memlekettìk университетінің habaršysy, № 4(75), 2024, pp. 339–350, doi. 10.47649/vau.24.v75.i4.29.[In Kaz]
Ильясова және т.б., 2025 - Ильясова Г., Әйтімов Б., Жұмағұлов М. «Блокчейн технологиясын қолдана отырып, жеке деректердің қауіпсіздігін қамтамасыз ету: заңнаманы жетілдіру мәселелері мен перспективалары», №18, 2025. [Онлайн]. Қолжетімді: https://ascelibrary.org/doi/abs/10.1061/JLADAH.LADR-1248 [In Eng]
Кассен, 2015 – Кассен М. «Электрондық үкімет жүйелерін түсіну: Америка Құрама Штаттары мен Қазақстандағы электрондық федерализм және электрондық орталықтандыру», 2015 жылдың қарашасы, [Онлайн] Қолжетімді: https : //books.google.com/books?hl = en&lr = &id = zLK6CgAAQBAJ&oi = fnd&pg = PR5&dq = Kazakhstan + AND + (e − government + OR + %22digital + government%22 + OR + %22digital + services%22) + AND + (%22data + privacy%22 + OR + %22data+protection%22+OR+%22personal+data%22)+AND+(%22digital+archives%22+OR+%22electronic+records%22+OR + %22citizen + data%22)&ots = uVuINIvZO8&sig = zDcdzVEjfycMGh3aNxMsNHjuozw [In Eng]
Калашникова, 2021 - Калашникова Э. Б. «Жеке деректерді қорғау цифрландырудың негізі ретінде», 73–79 беттер, 2021 жылғы сәуір, doi: https : //doi.org/10.1007/978 − 3 − 030 − 83175 − 2_11.
Қожанұлы және т.б., 2023 - Қожанұлы С., Айтчанқызы А.Г., Борисовна Д.О. «Цифрландыру дәуіріндегі дербес деректерді қорғау: конституциялық-құқықтық аспект», Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының жаршысы, т. 3, жоқ. 74, 68–76 беттер, қыркүйек 2023, doi: https : //doi.org/10.52026/2788 − 5291_2023_74_3_68.
Қоғабаев&Банерджи, 2024 - Қоғабаев Т., Банерджи С. «Қазақстандағы ақылды басқару: дамудың, қиындықтардың және болашақ бағыттардың жүйелі шолуы мен талдауы», Vol. 1 No. 1 (2024) [Онлайн]. Қолжетімді: https://scrd.eu/index.php/scrd-pp/article/view/575 [In Eng]
Қоғабаев&Банерджи, 2025 - Қоғабаев Т., Банерджи С. «Қазақстандағы ақылды басқаруды дамыту: сандық бастамалар мен саясаттың салдарын сыни талдау», 2025, pp. 183-207. [Онлайн]. Қолжетімді: https : //link.springer.com/chapter/10.1007/978 − 3 − 032 − 07370 − 9_15 [In Eng]
Умитчинова, және т.б., 2025 – Умитчинова Б.А., Гаврилова Ю.А., Мензюк Г.А. "Жасанды интеллектті дамыту жағдайындағы дербес деректерді құқықтық реттеу: шетелдік тәжірибе және Қазақстан үшін сын-қатерлер", 2025.DOI: https : //doi.org/10.52026/2788 − 5291_2025_80_3_37 [In Rus]

References

Amirov, 2023-Amirov A. Zheke derekterdi qorġau salasyndagy zanamanyn qazirgi jaġdayy turaly (QR materialdary negizinde) [On the current state of legislation in the field of personal data protection (based on the materials of the Republic of Kazakhstan)]. Rassledovanie prestuplenii: problemy i puti ikh reshenii, No. 1(39), pp. 143–151, 2023. DOI: 10.54217/2411-1627.2023.39.1.018. [Rus]
Amirova, 2025- Amirova A. Qazaqstandaġy azamattarga baġyttalġan memlekettik qyzmetterdi ilgeriletu: quqyqtyq, institutsionaldyq zhane cifrlyq basqaru perspektivalary [Promoting citizen-oriented public services in Kazakhstan: legal, institutional and digital governance perspectives]. Available at: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025. 1679601/full, DOI: 10.3389/fpos.2025.1679601. [Eng]
Doszhanova & Bugybay, 2024- Doszhanova A., Bugybay D. Aqparattyq-kommunikaciyalyq tehnologiyalar arqyly tulġanyn zheke basyn anyqtawdyn qazirgi jaġdayy men perspektivalary [Current state and prospects of personal identification using information and communication technologies]. H. Dosmuhamedov atyndaġy Atyrau memlekettik universitetinin habarshysy, No. 4(75), pp. 339–350, 2024. DOI: 10.47649/vau.24.v75.i4.29. [Kaz]
Ilyasova et al., 2025 - Ilyasova G., Aitimov B., Zhumagulov M. Blokchein tehnologiyasyn qoldanu arqyly zheke derekterdin qauipsizdigin qamtamasyz etu: zanamany jetildiru maseleleri men perspektivalary [Ensuring personal data security using blockchain technology: issues and prospects for improving legislation]. Available at: https://ascelibrary.org/doi/abs/10.1061/JLADAH.LADR-1248, DOI: 10.1061/JLADAH.LADR-1248. [Eng]
Kalashnikova, 2021- Kalashnikova E. B. Zheke derekterdi qorġau cifrlanudyń negizi retinde [Personal data protection as the basis of digitalization]. 2021, pp. 73–79. DOI: https : //doi.org/10.1007/978 − 3 − 030 − 83175 − 2_11. [Rus]
Kassen, 2015- Kassen M. Understanding e-government systems: e-federalism and e-centralization in the USA and Kazakhstan [Understanding e-government systems: e-federalism and e-centralization in the USA and Kazakhstan]. November 2015. Available at: https://books.google.com/ [Eng]
Kogabayev & Banerjee, 2024- Kogabayev T., Banerjee S. Qazaqstandaġy aqyldy basqaru: damudyn, qiyndyqtardyn zhane bolashaq baġyttardyn zhuieli sholuy men taldauy [Smart governance in Kazakhstan: a systematic review and analysis of development, challenges and future directions]. Vol. 1, No. 1, 2024. Available at: https://scrd.eu/index.php/scrd-pp/article/view/575 [Eng]
Kogabayev & Banerjee, 2025 - Kogabayev T., Banerjee S. Qazaqstandaġy aqyldy basqarudy damytu: sandıq bastamalar men sayasattyn saldaryn syni taldau [Developing smart governance in Kazakhstan: a critical analysis of digital initiatives and policy implications]. 2025, pp. 183–207. DOI: https : //doi.org/10.1007/978 − 3 − 032 − 07370 − 9_15. [Eng]
Kozhanuly et al., 2023- Kozhanuly S., Aitchankyzy A. G., Borisovna D. O. Cifrlandyru dawirindegi derbes derekterdi qorġau: konstituciyalyq-quqyqtyq aspekt [Personal data protection in the era of digitalization: constitutional and legal aspects]. Qazaqstan Respublikasynyn Zanama zhane quqyqtyq aqparat instituty habarsysy, Vol. 3, No. 74, pp. 68–76, September 2023. DOI: https : //doi.org/10.52026/2788 − 5291_2023_74_3_68. [Kaz]
Umitchinova et al., 2025 - Umitchinova B. A., Gavrilova Yu. A., Menzyuk G. A. Razvitie iskusstvennogo intellekta usloviyakh pravovogo regulirovaniya personalnykh dannykh: zarubezhnyy opyt i vyzovy dlya Kazakhstana [Legal regulation of personal data in the context of artificial intelligence development: foreign experience and challenges for Kazakhstan]. 2025. DOI: https : //doi.org/10.52026/2788 − 5291_2025_80_3_37. [Rus]

МРНТИ 28.23.25 DOI: https://doi.org/10.62687/STJ.7.1.2025.12

ОЦЕНКА ЭФФЕКТИВНОСТИ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ИНСТРУМЕНТОВ УПРАВЛЕНИЯ ЗАДАЧАМИ ДЛЯ ПОВЫШЕНИЯ ПРОДУКТИВНОСТИ МАЛЫХ КОМАНД

[1]А.К. Коротков*, **[2]М.Ж. Қалдарова**, **[3]Д.А. Кузин**
[1,2]Международный университет Астана, Астана, Казахстан
[3]Сургутский государственный университет, Сургут, Россия
*e-mail: konst55a@gmail.com

А.К. Коротков – магистрант образовательной программы «Вычислительная техника и программное обеспечения», Международный университет Астана, Астана, Казахстан, e-mail: konst55a@gmail.com, https://orcid.org/0009-0005-7341-935X

М.Ж. Калдарова – декан высшей школы информационных технологий и инженерии, Международный университет Астана, г. Астана, Казахстан, e-mail: kmiraj8206@gmail.com, https://orcid.org/0000-0001-7494-9794

Д.А. Кузин – Сургутский государственный университет, Сургут, Россия, https://orcid.org/0000-0001-7888-4094

Аннотация. В условиях цифровой трансформации и распространения удалённой работы управление задачами становится важным фактором продуктивности малых команд. Сегодня существует множество цифровых инструментов для управления проектами и задачами. Однако их разнообразие и различия в функциональных возможностях создают проблему выбора наиболее эффективных решений для небольших коллективов. Недостаточная адаптация инструментов к специфике работы малых команд может приводить к снижению эффективности взаимодействия, фрагментации рабочих процессов и нерациональному использованию времени. Цель исследования – оценить эффективность использования инструментов управления задачами в малых командах. Важно определить некоторые причины, которые могут повлиять на успешность внедрения их в работу а также дальнейшего применения их в работе. В данной статье был проведен анализ некоторых научных журналов и публикаций которые относятся к организации команды в компаниях или малых группах людей.

В статье проанализированы различные подходы к тому как управляются задачи. Чаще всего использовались именно Agile-методологии, современные платформы для управления проектами и системы которые отслеживают рабочее время. Сегодня именно эти инструменты применяются в большинстве команд для правильной организации людей, а также контроля выполнения задач. Анализ, проведенный в этой статье, показывает, что использование платформ для управления задачами положительно влияет на эффективность команд в различных сферах деятельности. Их использование упрощает отслеживать и координировать работу с задачами и их эффективностью. Однако на начальном этапе не обходится без некоторых проблем. При высоком количестве людей в команде или же некомпетентность с использованием новых технологий может привести к неэффективному использованию этих инструментов.

Практическая значимость исследования заключается в формировании рекомендаций по выбору и внедрению инструментов управления задачами, позволяющих повысить производительность командной работы, оптимизировать распределение ресурсов и сократить сроки выполнения проектов. Полученные результаты могут быть полезны для руководителей небольших команд и стартапов. Они также могут применяться в работе digital-агентств и индивидуальных предпринимателей. Кроме того, данные выводы могут использовать специалисты, которые работают в распределённых или удалённых командах.

Ключевые слова: управление задачами, малые команды, продуктивность, цифровые инструменты, таск-менеджеры, Agile-подходы, Scrum, автоматизация процессов, инструменты планирования, совместная работа, эффективность.

EVALUATING THE EFFECTIVENESS AND PROSPECTS OF IMPLEMENTING TASK MANAGEMENT TOOLS TO INCREASE THE PRODUCTIVITY OF SMALL TEAMS

[1]A.K. Korotkov*, **[2]M.Zh. Kaldarova**, **[3]D.A. Kuzin**
[1,2]Astana International University, Astana, Kazakhstan
[3]Surgut State University, Surgut, Russia
*e-mail: konst55a@gmail.com

A.K. Korotkov – master's student in the educational program «Computer Engineering and Software», Astana International University, Astana, Kazakhstan, e-mail: konst55a@gmail.com, https://orcid.org/0009-0005-7341-935X

M.Zh. Kaldarova – Dean of the Graduate School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: kmiraj8206@gmail.com, https://orcid.org/0000-0001-7494-9794

D.A. Kuzin – Surgut State University, Surgut, Russia, https://orcid.org/0000-0001-7888-4094

Abstract. In the context of digital transformation and the spread of remote work, task management is becoming an important factor in the productivity of small teams. Today, there are many digital tools for managing projects and tasks. However, their diversity and differences in functionality create the problem of choosing the most effective solutions for small teams. Insufficient adaptation of tools to the specifics of the work of small teams can lead to a decrease in the efficiency of interaction, fragmentation of work processes and irrational use of time. The purpose of the study is to evaluate the effectiveness of using task management tools in small teams. It is important to identify some of the reasons that may affect the success of their implementation in work, as well as their further application in work. This article analyzes some scientific journals and publications that relate to the organization of a team in companies or small groups of people. We've looked at different approaches to how tasks are managed. Agile methodologies, modern platforms for project management and systems that track working hours, were most often used. Today, these tools are used in most teams to properly organize people, as well as monitor the completion of tasks.

The analysis conducted in this article shows that the use of task management platforms has a positive effect on the effectiveness of teams in various fields of activity. They make it much easier to track and coordinate work with tasks and their effectiveness. However, there are some problems at first. With a high number of people in the team, or incompetence using new technologies can lead to inefficient use of these tools.

The practical significance of the research lies in the formation of recommendations on the selection and implementation of task management tools that can increase teamwork productivity, optimize resource allocation and shorten project deadlines. The results obtained can be useful for managers of small teams and startups. They can also be used in the work of digital agencies and individual entrepreneurs. In addition, these findings can be used by specialists who work in distributed or remote teams.

Keywords: task management, small teams, productivity, digital tools, task managers, Agile approaches, Scrum, process automation, planning tools, collaboration, efficiency.

ШАҒЫН КОМАНДАЛАРДЫҢ ӨНІМДІЛІГІН АРТТЫРУ ҮШІН ТАПСЫРМАЛАРДЫ БАСҚАРУ ҚҰРАЛДАРЫН ЕНГІЗУДІҢ ТИІМДІЛІГІ МЕН ПЕРСПЕКТИВАСЫН БАҒАЛАУ

[1]А.К. Коротков*, **[2]М.Ж. Қалдарова**, **[3]Д.А. Кузин**
[1,2]Астана халықаралық университеті, Астана, Қазақстан
[3]Сургут мемлекеттік университеті, Сургут, Ресей
*e-mail: konst55a@gmail.com

А.К. Коротков – «Компьютерлік инженерия және бағдарламалық қамтамасыз ету» білім беру бағдарламасының магистранты, Астана халықаралық университеті, Астана, Қазақстан, e-mail: konst55a@gmail.com, https://orcid.org/0009-0005-7341-935X

М.Ж. Қалдарова – Ақпараттық технологиялар және инжиниринг Жоғары мектебінің деканы, Астана халықаралық университеті, Астана, Қазақстан, e-mail: kmiraj8206@gmail.com, https://orcid.org/0000-0001-7494-9794

Д.А. Кузин – Сургут мемлекеттік университеті, Сургут, Ресей, https://orcid.org/0000-0001-7888-4094

Аңдатпа. Сандық трансформация және қашықтан жұмыс тарату жағдайында тапсырмаларды басқару шағын командалардың өнімділігінің маңызды факторына айналады. Бүгінгі таңда жобалар мен тапсырмаларды басқарудың көптеген сандық құралдары бар. Дегенмен, олардың әртүрлілігі мен функционалдық айырмашылықтары шағын топтар үшін ең тиімді шешімдерді таңдау мәселесін тудырады. Шағын командалардың жұмыс ерекшеліктеріне құралдардың жеткіліксіз бейімделуі өзара әрекеттесу тиімділігінің төмендеуіне, жұмыс процестерінің бөлшектенуіне және уақытты ұтымсыз пайдалануға әкелуі мүмкін. Зерттеудің мақсаты-шағын топтарда тапсырмаларды басқару құралдарын пайдаланудың тиімділігін бағалау. Кейбір себептерді анықтау маңызды бұл оларды жұмысқа енгізудің сәттілігіне сондай ақ оларды жұмыста одан әрі қолдануға әсер етуі мүмкін. Бұл мақалада кейбір ғылыми журналдар мен жарияланымдарға талдау жасалды олар компанияларда немесе адамдардың шағын топтарында команданы ұйымдастыруға қатысты. Біз тапсырмаларды қалай басқарудың әртүрлі тәсілдерін қарастырдық. Көбінесе бұл Agile әдістемелері болды жобаларды басқарудың уақтылы платформалары және жұмыс уақытын бақылайтын жүйелер. Бүгінгі таңда бұл құралдар көптеген командаларда адамдарды дұрыс ұйымдастыру үшін, сондай-ақ тапсырмалардың орындалуын бақылау үшін қолданылады.

Осы мақалада жүргізілген талдау тапсырмаларды басқару платформаларын пайдалану әртүрлі қызмет салаларындағы командалардың тиімділігіне оң әсер ететінін көрсетеді. Олардың көмегімен тапсырмаларды және олардың тиімділігін бақылау және үйлестіру оңайырақ болады. Алайда, басында ол кейбір проблемаларсыз аяқталмайды. Командадағы адамдар саны көп болған кезде немесе жаңа технологияларды қолдану қабілетсіздігі осы құралдарды тиімсіз пайдалануға әкелуі мүмкін.

Зерттеудің практикалық маңыздылығы топтық жұмыстың өнімділігін арттыруға, ресурстарды бөлуді оңтайландыруға және жобалардың орындалу мерзімін қысқартуға мүмкіндік беретін тапсырмаларды басқару құралдарын таңдау және енгізу бойынша ұсыныстарды қалыптастыру болып табылады. Нәтижелер шағын топ басшылары мен стартаптар үшін пайдалы болуы мүмкін. Олар сондай-ақ digital-агенттіктер мен жеке кәсіпкерлердің жұмысында қолданылуы мүмкін. Сонымен қатар, бұл нәтижелерді таратылған немесе қашықтағы командаларда жұмыс істейтін мамандар қолдана алады.

Кілттік сөздер: тапсырмаларды басқару, шағын командалар, өнімділік, сандық құралдар, таск-менеджерлер, Agile-тәсілдер, Scrum, процесті автоматтандыру, жоспарлау құралдары, Ынтымақтастық, тиімділік.

Введение. Для большинства организаций на данный момент одной из важнейших задач является организация команд и повышения рабочих процессов. Особенно это влияет на организации, где небольшое количество сотрудников, а задач становится больше, они становятся сложнее и требуют взаимодействия между сотрудниками. В таких случаях становится важным наличие инструментов и платформ позволяющих координировать процессы по управлению задачами. За последние несколько лет распространение различных типов занятости сильно изменило подходы к организации работы. Многие команды всё чаще используют инструменты для планирования, отслеживания задач и обмена информацией. Такие решения помогают качественно организовать рабочие процессы. Они делают распределение обязанностей более прозрачным. Некоторые исследования показывают, что использование технологий в командной работе положительно влияет на продуктивность и качество взаимодействия между сотрудниками. Применение инструментов управления задачами способствует улучшению координации деятельности и помогает более эффективно организовывать выполнение поставленных задач (Tohidi, Tarokh, 2006:610-615). Для малых команд эта проблема более актуальна. Небольшие коллективы обычно характеризуются более гибкой структурой и быстрым принятием решений. При этом отсутствие чётко выстроенной системы управления задачами может привести к возникновению трудностей в координации работы и неравномерному распределению нагрузки между участниками команды (Reiter-Palmon и др., 2021:52-60).

В настоящее время доступно множество программных решений для управления задачами и проектами. К ним относятся системы планирования задач, сервисы для совместной работы, а также инструменты, позволяющие отслеживать сроки выполнения задач и контролировать использование рабочего времени. Такие системы позволяют оптимизировать рабочие процессы и повысить продуктивность команд за счёт автоматизации процессов планирования и контроля задач (Dere и др., 2024:47-49).

Целью данной статьи является анализ эффективности использования инструментов управления задачами в малых командах и определение перспектив их внедрения для повышения продуктивности.

Гипотеза исследования заключается в том, что использование инструментов для управления задачами способствует повышению прозрачности рабочих процессов. Выполнение задач происходит быстрее, а также повышается взаимодействие между работниками. А результат этого влияния зависит от уровня владения и адаптации команды.

Материалы и методы. Для достижения целей исследования была использована совокупность теоретических и аналитических методов, направленных на изучение эффективности инструментов управления задачами в малых командах.

Основным методом исследования стал анализ научной литературы, посвящённой вопросам повышения продуктивности команд и использованию цифровых инструментов управления проектами (Cherukuri и др., 2024: 175–184, Dingsøyr и др., 2018, Mavis и др., 2022: 3.2.49-64). Поиск научных публикаций проводился в академических базах данных Google Scholar и ResearchGate по ключевым словам *task management tools, team productivity, project management software, agile team performance, collaboration tools* (Bissaliyev, 2017: 85–9, Mihalache, 2017: 85–93, Hussein, Hassan, 2025).

В результате первичного поиска было выявлено более 60 научных публикаций, посвящённых данной тематике. После анализа содержания и отбора по критериям релевантности, научной значимости и соответствия теме исследования в итоговую выборку были включены 13 научных и 6 открытых источников, которые легли в основу теоретического анализа. Для систематизации данных был применён метод контент-анализа научных публикаций, позволяющий выявить основные направления исследований в области использования инструментов управления задачами (Mihalache, 2017: 85–93).

В процессе анализа были рассмотрены ключевые аспекты, представленные в научной

литературе, включая влияние цифровых инструментов на продуктивность командной работы (Cherukuri и др., 2024: 175–184, Tomaz и др., 2026). Использование Agile-методологий и Scrum в управлении задачами (Cherukuri и др., 2024: 175–184, Lin и др., 2014). влияние инструментов совместной работы на коммуникацию внутри команды (Bissaliyev, 2017: 10747–10755, Hussein, Hassan, 2025), а также особенности внедрения систем управления проектами в организациях малого размера.

Дополнительно в исследовании был использован метод сравнительного анализа программных инструментов управления задачами. В качестве объектов анализа были выбраны наиболее распространённые цифровые платформы, применяемые малыми командами для организации рабочих процессов, такие как Trello, Asana, Jira, ClickUp и Monday.com. Выбор данных инструментов обусловлен их высокой распространённостью в организациях и частым упоминанием в научных публикациях и аналитических исследованиях. (Hussein, Hassan, 2025).

Сравнение инструментов проводилось по ряду критериев, включая функциональные возможности систем планирования задач и управления проектами, удобство пользовательского интерфейса, возможности совместной работы и коммуникации, уровень интеграции с другими цифровыми сервисами, а также степень адаптации инструментов для работы малых команд (ElHamahmy, 2025: 7106–7117). Для структурирования результатов сравнительного анализа была сформирована таблица сравнительных характеристик инструментов управления задачами, в которой отражены основные функции, преимущества и ограничения рассматриваемых систем.

Кроме того, в исследовании использовались статистические данные аналитических исследований, посвящённых распространённости инструментов управления задачами в организациях и малых командах. На основе данных аналитических отчётов была сформирована таблица распределения популярности инструментов управления задачами, отражающая частоту использования различных платформ в малых командах (Hussein, Hassan, 2025).

Таким образом, методологическая база исследования включает анализ научной литературы, контент-анализ научных публикаций, сравнительный анализ программных инструментов управления задачами и анализ статистических данных аналитических исследований. Применение данных методов позволило получить комплексное представление об инструментах управления задачами, используемых в малых командах, и сформировать основу для дальнейшего анализа их эффективности (Cherukuri и др., 2024: 175–184, Bissaliyev, 2017: 10747–10755, Dingsøyr и др., 2018: 6-19).

В дополнение к анализу литературы в рамках исследования был проведен опрос участников малых команд. Опрос включал в себя 10 открытых вопросов. Они были направленны на выяснение того, как именно улучшилась работа после добавления инструмента по управлению задачами. В опросе приняли участие 10 человек из нескольких команд. Эти команды используют различные инструменты по управлению задачами. Помимо тех которые рассматриваются в исследовании, были также Bitrix 24, Microsoft Planner и Notion. Ответы были проанализированы и объединены в категории по смыслу.

Результаты и обсуждение. В исследовании рассмотрены научные публикации и цифровые инструменты управления задачами. Основной целью анализа являлось выявление эффективности применения данных инструментов для повышения продуктивности сотрудников и оптимизации рабочих процессов.

В процессе исследования удалось определить инструменты управления задачами, которые используются чаще всего. Такие решения широко применяются малыми командами в повседневной работе. Для анализа были рассмотрены пять популярных платформ управления проектами и задачами. Результаты исследования представлены в трех ключевых таблицах.

Таблица 1. Сравнительный анализ функциональных возможностей инструментов управления задачами на основе официальных источников инструментов

Инструмент	Планирование задач	Канбан-доска	Отслеживание времени	Интеграции	Аналитика
Asana	Встроено	Встроено	Встроено	Широкие встроенные и сторонние интеграции	Встроено
ClickUp	Встроено	Встроено	Встроено	Встроено, поддерживаются внешние интеграции	Встроено
Trello	Встроено	Встроено	Через Power ups	Через Power ups	Частично встроено
Jira	Встроено	Встроено	Встроено	Интеграции через Atlassian	Встроено
Monday.com	Встроено	Встроено	Встроено	200+ интеграций	Встроено

Таблица 2. Оценка инструментов управления задачами по данным Capterra (на 26 марта 2026 года)

Инструмент	Простота использования	Функциональность	Обслуживание клиентов	Соотношение цены и качества	Общая оценка
Asana	4.4	4.4	4.3	4.4	4.5
ClickUp	4.3	4.6	4.5	4.6	4.6
Trello	4.5	4.3	4.3	4.5	4.5
Jira	4.1	4.4	4.2	4.3	4.4
Monday.com	4.5	4.4	4.4	4.3	4.6

Таблица 3. Влияние инструментов управления задачами на показатели продуктивности команд по данным Asana и Capterra

Показатель	До внедрения инструментов	После внедрения инструментов
Среднее время выполнения задачи	5 дней	12 часов
Количество пропущенных, несвоевременно выполненных задач	40%	менее 10%
Уровень прозрачности задач	26%	84%
Эффективность распределения задач	При перегрузке задача может занимать 39.1 часа	При плановой нагрузке задача занимает 3.5 часа

Таблица 1 отражает функциональные возможности различных инструментов управления задачами. Все рассмотренные системы поддерживают базовые функции планирования и визуализации задач. Системы, предоставленные в таблице, имеют большой функционал, связанный с планированием и визуализации задач. Однако у нескольких из них существуют некоторые различия и связаны они с отслеживанием времени. Если посмотреть на таблицу только Jira и ClickUp предоставляют лучший и более развитые средства для работы с задачами. Чаще всего такие системы используются в более сложных проектах. Для малых команд больше подходит Trello благодаря его простому интерфейсу.

В таблице 2 представлена сравнительная оценка инструментов по нескольким критериям. Среди них простота использования, функциональность, обслуживание клиентов и

соотношение цены и качества. Наибольшую суммарную оценку получили системы ClickUp и Monday.com. Это связано с сочетанием широкого набора функций и гибкой настройки рабочих процессов. Trello и Monday.com получили самый высокий показатель по простоте использования, поэтому данные инструменты часто выбирают команды с ограниченными ресурсами или небольшим опытом работы с цифровыми системами управления задачами.

Таблица 3 показывает влияние инструментов на продуктивность рабочего процесса. Среднее время выполнения задач уменьшилось на 4.5 дня, что прибавляет вариативности в управлении командой. Количество пропущенных задач уменьшилось более чем в 4 раза. Уровень прозрачности увеличился на 58%. Это свидетельствует о том, что внедрение таких технологий помогают компаниям в организации командной работы.

Результаты, представленные в таблицах, показывают влияние этих инструментов в работе с малыми командами увеличивают скорость выполнения задач, а также их прозрачность. Однако важно выбрать правильную систему и оценить скорость его внедрения. При этом нужно учесть, что сложность интерфейса и необходимость обучения пользователей могут замедлять внедрение в малых командах с ограниченными ресурсами.

Результаты опроса показали, что до внедрения в работу инструментов по управлению задачами, работа организовывалась через чаты, устные договоренности и различные документы. Это затрудняло управление и распределение задач. После внедрения инструментов участники отмечали, что рабочие процессы стали более прозрачными. Также сократилось время на согласование и улучшение командного взаимодействия. Трудности, с которыми столкнулись участники, стали: привыкание к платформе, сложность освоения и дисциплина работы с инструментами. Результаты опроса подтверждают, что использование инструментов управления задачами повысило организованность и продуктивность работы.

Проведенное исследование показывает, что выбор инструментов управления задачами не сводится только к сравнению их функциональных возможностей. Важную роль играет и то, насколько выбранная система соответствует особенностям команды, отрасли и существующим рабочим процессам. Практика показывает, что использование платформ с развитой аналитикой и возможностью гибкой настройки может способствовать повышению эффективности работы. Вместе с тем результат внедрения во многом зависит от подготовки сотрудников и от того, насколько рабочие процессы команды адаптированы к использованию новых инструментов.

Заключение. Результаты исследования показывают, что эффективность инструментов управления задачами зависит не только от их функций. Существенное значение имеет соответствие выбранной системы потребностям команды. Простые и интуитивные решения позволяют быстро наладить рабочий процесс. Они также сокращают время обучения сотрудников. Поэтому такие системы часто используют стартапы и небольшие команды. Однако их возможностей может быть недостаточно при управлении сложными проектами. В таких случаях востребованы более функциональные платформы, например ClickUp и Jira. Они позволяют гибко настраивать процессы и использовать аналитические инструменты.

В заключение следует отметить, что использование инструментов способствуют эффективной организации работы команды. Они помогают улучшить взаимодействие между работниками в команде. Также, они позволяют выявлять проблемы на ранних стадиях выполнения задач. Это создает условия для плавного развития команд и повышения качества проектов.

Литература

Bissaliyev, 2017 – Bissaliyev M.S. The effectiveness of collaboration tools on virtual project management // International Journal of Applied Engineering Research. – 2017. – P. 10747–10755.

Cherukuri и др., 2024– Cherukuri H., Gupta R., Shukla S., Rajan A., Aravind S. The impact of agile development strategies on team productivity in full stack development projects // International Journal of Intelligent Systems and Applications in Engineering. – 2024. – P. 175–184

Dere и др., 2024 – Dere A. S., Kheraliya S., Raut N., Bhosale P. Task management and productivity app // International Journal for Scientific Research and Development. – 2024. – Vol. 12, № 2. – P. 47–49. – URL: https://ijsrd.com/articles/IJSRDV12I20060.pdf

Digital collaboration tools, 2024 – Digital collaboration tools: enhancing team productivity. – 2024. – DOI: https://doi.org/10.64357/digital-collaboration-tools-2025.

Dingsøyr и др., 2018. – Dingsøyr T., Moe N. B., Seim E. Teamwork quality and team performance: exploring differences between small and large agile projects. – 2018. – DOI: https : //doi.org/10.1007/978 − 3 − 319 − 91602 − 6_19.
ElHamahmy, 2025 – ElHamahmy A., Galal A., Gohar H., Khalafallah A. A comparative review of team management software in modern project management practices. – 2025. – P. 7106–7117 – DOI: https://doi.org/10.22214/ijraset.2025.71852.
Hussein&Hassan, 2025 – Hussein R., Hassan B. Collaboration tools and their role in agile software projects. – 2025. – URL: https://arxiv.org/abs/2506.10985.
Mavis и др., 2022 – Mavis A., David F.,Oluwatobi A., Isaac O., Erica A., Muritala O.U., Andikan U.U., Olasehinde O. Agile-based project management strategies for enhancing collaboration in cross-functional software development teams // Journal of Frontiers in Multidisciplinary Research. – 2022. – URL: https://doi.org/10.54660/.IJFMR.2022.3.2.49-64.
Mihalache, 2017 – Mihalache A. Project management tools for agile teams // Informatica Economica. – 2017. – P. 85–93 DOI: https://doi.org/10.12948/issn14531305/21.4.2017.07.
Lin и др., 2014 – Lin J., Yu H., Shen Z. An empirical analysis of task allocation in Scrum-based agile programming. – 2014. – URL: https://arxiv.org/abs/1411.6201.
Reiter-Palmon и др., 2021– Reiter-Palmon R., Kennel V., Allen J. A. Teams in small organizations: conceptual, methodological, and practical considerations // Frontiers in Psychology. – 2021. – Vol. 12. – Art. 530291. – DOI: https://doi.org/10.3389/fpsyg.2021.530291.
Tohidi&Tarokh, 2006 – Tohidi H., Tarokh M.J. Productivity outcomes of teamwork as an effect of information technology and team size // International Journal of Production Economics. – 2006. –Vol. 103, № 2. – P. 610–615. – ISSN 0925-5273. – DOI: https://doi.org/10.1016/j.ijpe.2005.12.002.
Tomaz и др., 2026 – Tomaz R., Guenes P., Araújo A., Baldassarre M., Kalinowski M. Impacts of generative AI on agile teams' productivity: a multi-case longitudinal study. – 2026. – URL: https://doi.org/10.48550/arXiv.2602.13766.
Asana. Work Tracking & Project Management Features – URL: https://asana.com/ru/features
Asana. Customers who use Asana – URL: https://asana.com/ru/customers
Atlassian. Jira Software – Features – URL: https://www.atlassian.com/software/jira/features
Capterra. 2026 Capterra Shortlist for Task Management – URL: https://www.capterra.com/task-management-software/shortlist/
Capterra. 5-Step Action Plan for Optimal Resource Utilization at SBMs – URL: https://www.capterra.com/resources/optimal-resource-utilization-for-smbs/
ClickUp. Product Features – URL: https://clickup.com/features
Monday.com. Team management features – URL: https://monday.com/new-product
Trello. What is Trello: Learn Features, Uses & More – URL: https://trello.com/tour

IRSTI 20.23.17 DOI: https://doi.org/10.62687/STJ.7.1.2025.14

INTERPRETABLE AI FOR CYBER THREAT DETECTION IN SMART SYSTEMS

[1]A.A. Abdukarimova, **[2]R.A. Ismailova**, **[3]A.M. Jumagaliyeva***, **[4]V.B. Rystygulova**, **[5]A.E. Koxegen**

[1,3,4]K. Kulazhanov Kazakh University of Technology and Business, Astana, Kazakhstan
[2]Kyrgyz-Turkish Manas University, Bishkek, Kyrgyzstan
[5]S. Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan
*e-mail: jumagalievaainur.m@gmail.com

A.A. Abdukarimova – PhD, Associate Professor, Department of Information Technology, K. Kulazhanov Kazakh University of Technology and Business, Astana, Kazakhstan, e-mail: a.abdukarimova777@gmail.com, https://orcid.org/0000-0002-6932-6282

R.A. Ismailova – PhD, Associate Professor, Department of Computer Engineering, Kyrgyz-Turkish Manas University, Bishkek, Kyrgyzstan, e-mail: rita.ismailova@manas.edu.kg, https://orcid.org/0000-0003-0308-2315

A.M. Jumagaliyeva – Senior lecturer, Department of Information Technology, K. Kulazhanov Kazakh University of Technology and Business, Astana, Kazakhstan, e-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209

V.B. Rystygulova – Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Information Technology, K. Kulazhanov Kazakh University of Technology and Business, Astana, Kazakhstan, e-mail: rystygulovaV@mail.ru, https://orcid.org/0000-0003-3883-5612

A.E. Koxegen – Senior lecturer, Department of Computer Science, S. Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan, e-mail: a.koksegen@kazatu.kz, https://orcid.org/0000-0002-8994-4096

Abstract. The rapid development of intelligent technologies, IoT infrastructures, and cloud services has led to an increasingly complex cybersecurity landscape. Because intelligent systems generate massive volumes of heterogeneous streaming data in real time, the challenges of accurately detecting threats in the cyber environment have increased significantly. Traditional intrusion detection systems used to identify cyber threats typically rely on static attack signatures and, therefore, have limited ability to detect new forms of cyber threats. This study presents an interpretable artificial intelligence framework for real-time cyber threat detection in streaming intelligent systems using machine learning models, combined with explainable AI methods such as SHAP and LIME to enhance detection capabilities. Security-related data streams and other sources were analyzed to identify potential anomalies and cyberattacks. Based on experimental evaluation, the proposed model, based on combined methodologies, such as hybrid explainable AI model, demonstrated superior performance compared to each of the individual machine learning models across several evaluation metrics, including accuracy, precision, recall, and F1 score. Overall, this work demonstrates how to leverage machine learning and explainable AI methods to improve trust, transparency, and the practical applicability of cybersecurity monitoring solutions in dynamic, intelligent environments.

Keywords: cybersecurity, machine learning, explainable AI, intrusion detection, streaming data, smart systems, anomalies.

СМАРТ ЖҮЙЕЛЕРДЕ КИБЕРҚАУІПТЕРДІ АНЫҚТАУҒА АРНАЛҒАН ИНТЕРПРЕТАЦИЯЛАНАТЫН ЖАСАНДЫ ИНТЕЛЛЕКТ

[1]А.А. Абдукаримова, [2]Р.А. Исмаилова, [3]А.М. Джумагалиева*, [4]В.Б. Рыстыгулова, [5]Ә.Е. Көксеген

[1,3,4]Қ.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана, Қазақстан
[2]«Манас» Қырғыз-Түрік университеті, Бішкек, Қырғызстан
[5]С.Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті, Астана, Қазақстан
*e-mail: jumagalievaainur.m@gmail.com

А.А. Абдукаримова – PhD, қауымдастырылған прфессор, Ақпараттық технологиялар кафедрасы, Қ.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана, Қазақстан, e-mail: a.abdukarimova777@gmail.com, https://orcid.org/0000-0002-6932-6282

Р.А. Исмаилова – PhD, қауымдастырылған прфессор, Ақпараттық технологиялар кафедрасы, «Манас» Қырғыз-Түрік университеті, Бішкек, Қырғызстан, e-mail: rita.ismailova@manas.edu.kg, https://orcid.org/0000-0003-0308-2315

А.М. Джумагалиева – сеньор-лектор, Ақпараттық технологиялар кафедрасы, Қ.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана, Қазақстан, e-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209

В.Б. Рыстыгулова – қауымдастырылған прфессор, Ақпараттық технологиялар кафедрасы, Қ.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана, Қазақстан, e-mail: rystygulovaV@mail.ru, https://orcid.org/0000-0003-3883-5612

Ә.Е. Көксеген – аға оқытушы, Компьютерлік ғылымдар кафедрасы, С.Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті, Астана, Қазақстан, e-mail: a.koksegen@kazatu.kz, https://orcid.org/0000-0002-8994-4096

Аңдатпа. Ақылды технологиялардың, IoT инфрақұрылымдарының және бұлтты қызметтердің қарқынды дамуы киберқауіпсіздік ландшафтының күрделене түсуіне әкелді. Ақылды жүйелер нақты уақыт режимінде үлкен көлемдегі гетерогенді ағынды деректерді жасайтындықтан, киберортада қауіптерді дәл анықтау қиындықтары айтарлықтай артты. Киберқауіптерді анықтау үшін қолданылатын дәстүрлі басып кіруді анықтау жүйелері әдетте статикалық шабуыл қолтаңбаларына сүйенеді және сондықтан киберқауіптердің жаңа түрлерін анықтау мүмкіндігі шектеулі. Бұл зерттеуде машиналық оқыту модельдерін пайдалана отырып, ағынды интеллектуалды жүйелерде нақты уақыт режимінде киберқауіптерді анықтауға арналған түсіндірілетін жасанды интеллект құрылымы, анықтау мүмкіндіктерін жақсарту үшін SHAP және LIME сияқты түсіндірілетін жасанды интеллект әдістерімен біріктірілген. Қауіпсіздікке қатысты деректер ағындары және басқа да ықтимал ауытқулар мен кибершабуылдарды анықтау үшін талданды. Эксперименттік бағалау негізінде ұсынылған модель біріктірілген әдіснамаларға (гибридті түсіндірілетін жасанды интеллект моделі) негізделген, дәлдік, дәлдік, еске түсіру және F1 ұпайын қоса алғанда, бірнеше бағалау көрсеткіштері бойынша әрбір жеке машиналық оқыту модельдерімен салыстырғанда жоғары өнімділікті көрсетті. Жалпы алғанда, бұл жұмыс динамикалық, интеллектуалды ортада киберқауіпсіздікті бақылау шешімдерінің сенімділігін, ашықтығын және практикалық қолданылуын жақсарту үшін машиналық оқытуды және түсіндіруге болатын жасанды интеллект әдістерін қалай пайдалану керектігін көрсетеді.

Кілт сөздер: киберқауіпсіздік, машиналық оқыту, түсіндірілетін жасанды интеллект, бұзушылықтарды анықтау, деректер ағыны, интеллектуалды жүйелер, ауытқулар.

ИНТЕРПРЕТИРУЕМЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ В УМНЫХ СИСТЕМАХ

[1]А.А. Абдукаримова, [2]Р.А. Исмаилова, [3]А.М. Джумагалиева*, [4]В.Б. Рыстыгулова, [5]Ә.Е. Көксеген

[1,3,4]Казахский университет технологии и бизнеса им.К.Кулажанова, Астана, Казахстан
[2]Кыргызско-Турецкий университет «Манас», Бишкек, Киргизстан
[5]Казахский агротехнический исследовательский университет им.С.Сейфуллина, Астана, Казахстан
*e-mail: jumagalievaainur.m@gmail.com

А.А. Абдукаримова - PhD, асоциированный профессор кафедры Информационных технологий, Казахский университет технологии и бизнеса им.К.Кулажанова, Астана, Казахстан, e-mail: a.abdukarimova777@gmail.com, https://orcid.org/0000-0002-6932-6282

Р.А. Исмаилова - PhD, асоциированный профессор кафедры Компьютерных наук, Кыргызско-Турецкий университет «Манас», Бишкек, Киргизстан, e-mail: rita.ismailova@manas.edu.kg, https://orcid.org/0000-0003-0308-2315

А.М. Джумагалиева- сеньор-лектор кафедры Информационных технологий, Казахский университет технологии и бизнеса им.К.Кулажанова, Астана, Казахстан, e-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209

В.Б. Рыстыгулова - к.ф.-м.н. асоциированный профессор кафедры Информационных технологий, Казахский университет технологии и бизнеса им.К.Кулажанова, Астана, Казахстан, e-mail: rystygulovaV@mail.ru, https://orcid.org/0000-0003-3883-5612

Ә.Е. Көксеген – старший преподаватель кафедры Компьютерных наук, Казахский агротехнический исследовательский университет им.С.Сейфуллина, Астана, Казахстан, e-mail: a.koksegen@kazatu.kz, https://orcid.org/0000-0002-8994-4096

Аннотация. Быстрое развитие интеллектуальных технологий, инфраструктур Интернета вещей и облачных сервисов привело к усложнению среды кибербезопасности. Поскольку интеллектуальные системы генерируют огромные объемы разнородных потоковых данных в режиме реального времени, задачи точного обнаружения угроз в киберсреде значительно возросли. Традиционные системы обнаружения вторжений, используемые для выявления киберугроз, обычно используют статические сигнатуры атак и, следовательно, имеют ограниченные возможности для выявления новых форм киберугроз. В этом исследовании будет представлена интерпретируемая структура искусственного интеллекта для обнаружения киберугроз в режиме реального времени в потоковых интеллектуальных системах с использованием моделей машинного обучения, в сочетании с объяснимыми методами искусственного интеллекта, такими как SHAP и LIME, для повышения возможностей обнаружения. Было анализировано потоки данных, связанные с безопасностью, и другие источники для выявления потенциальных аномалий и кибератак. На основе экспериментальной оценки предложенная модель, основанная на комбинированных методологиях (гибридная модель объяснимого искусственного интеллекта), показала лучшие результаты, чем каждая из моделей машинного обучения по отдельности, по нескольким метрикам оценки, включая точность, прецизионность, полноту и F1-меру. В целом, эта работа демонстрирует, как использовать методы машинного обучения и объяснимого искусственного интеллекта для повышения уровня доверия, прозрачности и практического применения решений по мониторингу кибербезопасности в динамичных, интеллектуальных средах.

Ключевые слова: кибербезопасность, машинное обучение, объяснимый искусственный интеллект, обнаружение вторжений, потоковые данные, интеллектуальные системы, аномалии.

Introduction. The speed at which digital infrastructure, smart technologies, and interconnected cyber-physical systems are developing has dramatically increased the number of different kinds of information that exist in today’s modern information environments. Smart

systems, such as IoT platforms, cloud computing infrastructures, intelligent transportation systems, and smart city networks produce large amounts of disparate data streams all day, every day, with no end in sight. While these technologies have great value from a business perspective in automating operations, increasing productivity, and allowing for instantaneous decision-making; they are also opening up new opportunities for exploitation and are increasing the threat exposure of businesses to those who are exploiting new and advanced types of cyber attacks.

Smart environments are now highly susceptible to a multitude of different types and sources of cyber attacks including: distributed denial-of-service (DDoS) attacks, data injection attacks, botnet activity, scanning for reconnaissance purposes, and man-in-the-middle intrusions. These attacks can cause catastrophic service disruptions, threaten sensitive information, and create large-scale system failures. Traditional cybersecurity protection measures (i.e., signature-based intrusion detection systems IDS) rely upon detecting attacks that have already been identified, or have already been documented. While this approach is sufficient for detecting attacks that already exist; it is frequently not capable of detecting unknown or evolving attack methods that are introduced because of the dynamic nature of the networks in which they occur.

To mitigate the inability to detect “new” attacks using traditional cybersecurity protection mechanisms, organizations are beginning to use machine learning ML-based intrusion detection systems (IDS). These ML-based IDS are able to learn complex behaviors of users and/or machines through their interactions with the network, and therefore, can identify anomalous behaviors that may signal a malicious activity. Algorithms for example such as the Random Forest, gradient boosting models (GBM), and deep neural networks (DNN) have all shown to produce high accuracy levels at detecting cyber threats within multi-dimensional data sets. Additionally, deep learning models such as Long Short-Term Memory (LSTM) networks are particularly proficient at analyzing sequential and temporal patterns within the streams of network traffic data they process. However, despite the high predictive accuracy of many ML-based detection systems, a critical challenge remains: the lack of transparency and interpretability of model decisions. Many advanced machine learning models operate as “black-box” systems, providing predictions without clear explanations of the factors influencing these decisions. In cybersecurity contexts, this lack of interpretability can limit the trust of security analysts and complicate incident response processes. As a result, explainable artificial intelligence (XAI) has emerged as an important research direction aimed at improving transparency and interpretability of machine learning models.

Using Explainable AI methods (SHAP and LIME) provide analysts with the ability to identify how much each characteristic impacts a given model's output. Explainable AI allows users to gain insights into the global behavior of a model, as well as the local behavior of an individual detection decision. The use of explainable AI in Cybersecurity Monitoring Systems provides users with an understanding of the sources of the detected anomalies, thereby, increasing the usefulness of AI-based security solutions.

The second area impacting modern Cybersecurity is the requirement to process massive streams of data that are generated on an ongoing basis. Real-time Smart Systems generate Security Events that need to be analysed and reported in as little time as possible. As a result, Cybersecurity Detection Frameworks must be capable of processing vast amounts of Data Streams at High Prediction Accuracy and Computational Efficiency.

However, despite significant progress in machine learning-based intrusion detection and explainable AI techniques, existing studies do not sufficiently address the integration of real-time streaming data processing with interpretable detection models in smart system environments. Most approaches either focus on detection accuracy without interpretability or apply explainable methods without considering dynamic data streams. This gap motivates the development of a unified framework that ensures both high detection performance and model transparency in real-time conditions.

The purpose of this paper is to develop an Interpretable Artificial Intelligence Framework for Real-Time Cyber Threat Detection in Streaming Smart Systems. The proposed Framework deploys Machine Learning Models and Explainable AI Methods to enable Accurate Cyber Threat Detection, along with providing Transparency and Interpretability of the Model Outputs. The object of this

study is cybersecurity monitoring in streaming smart systems operating in dynamic and data-intensive environments.

The subject of the research is the development and application of interpretable machine learning models for real-time cyber threat detection using streaming security data.

The proposed Framework will integrate the use of Ensemble Learning Algorithms, Deep Learning Models, and Explainable AI Analysis Methods to detect Cyber Threats based on Streaming Security Data collected from three sources; Network Traffic, IoT Devices, and System Logs. The main contributions of this study are:

1. Develop a Conceptual Framework for Interpretable Cyber Threat Detection in Streaming Smart Systems;
2. Design a System Architecture that Integrates ML Detection Models with Explainable AI Methodologies;
3. Conduct experiments using several Classifiers, including Random Forest, XGBoost, LSTM, and a Hybrid Explainable AI Detection Model;
4. Evaluate and Compare each of the Detection Models, with an understanding of the Inputs and Outputs of each Model, by conducting Feature Importance Analyses and using Explainable AI Methodology to Show Model Interpretability.

The novelty of this study lies in the development of a unified framework that integrates machine learning and explainable artificial intelligence for real-time cyber threat detection in streaming smart systems.

In contrast to other techniques, the proposed model balances prediction accuracy with interpretability by providing both global and local feature importance metrics through SHAP and LIME analysis of model predictions.

Authors also use hybrid modeling techniques to help improve the effectiveness of the detection process across a variety of cyber risk factors.

The results will demonstrate that using both Machine Learning Models and Explainable AI Mechanisms produces Improved Cyber Security Monitoring System Detection Performance and Transparency. The Proposed Approach provides the basis for creating Intelligent Interpretable and Scalable Cyber Threat Detection Systems for next-generation Smart Infrastructure.

Literature review. In today's society, we are living through a technological revolution. Smart technology is being developed at lightning speed and the cloud is increasing in importance every day as well. The Internet of Things (IoT) is rampant, and has led to a more complex security landscape than ever before. Traditional intrusion detection systems (IDS), or systems that detect intrusion attempts on a network, largely rely on signature or rule-based methods of detecting known attacks (Al Rawajbeh et al., 2025). While traditional IDS can effectively identify previously known threat types, they are often unable to effectively identify unknown or new threat types in ever-changing environments. In response, a growing number of researchers have begun using machine learning techniques to automatically detect cyber threats according to (Prasad et al., 2025).

In the past decade, supervised learning algorithms have been used most widely for IDS systems because these algorithms are capable of classifying network traffic and detecting anomalous activity related to that traffic as well. SVMs, decision trees, and random forest classifiers are some of the most common machine learning algorithms used in IDS research (Rahmati, 2025). Random Forest classifiers have received much attention because of their ability to accurately classify data, even in the presence of noise, and their capability to process high-dimensional network traffic features (Almheiri et al., 2025). Additionally, gradient boosting algorithms such as XGBoost and LightGBM have received considerable interest in the cyber attack detection area due to their ability to model complex, non-linear relationships that exist within large sets of data according to (Paul, 2025).

In the last few years, researchers have also been focusing on deep learning techniques. A number of different neural network architectures including DNNs, CNNs, and RNNs have been applied to detecting complex cyber threats in large networks (Khalaf et al., 2025). LSTM networks, in particular, have been shown to be effective for temporal analysis and capturing time-based relationships in the behavior of cyber threats (Thiruvenkatasamy et al., 2025). These models can also

be used to detect complex behaviors associated with a multi-stage attack, which may be difficult for traditional machine learning techniques to accomplish (Alshudukhi et al., 2025).

Even though these models perform extremely well when it comes to detecting intrusions, there is a significant lack of transparency in many of the machine-learning based intrusion detection systems that are currently available (Jumagaliyeva et al., 2025). Complex systems such as deep neural networks, ensemble methods and gradient boosting methods work as "black-boxes"; therefore it is extremely difficult for anyone to understand how the machine-learning based intrusion detection system made its final decision (Kalutharage et al., 2025). When conducting investigations on incidents in cybersecurity, a lack of interpretability can reduce the trust of security analysts and make it much more difficult for them to carry out their duties of investigating, responding to and remediating incidents (Mohale et al., 2025).

Recent research has increasingly focused on integrating explainable artificial intelligence (XAI) into the suite of techniques utilized in cybersecurity analytics as a way to address this problem. The goal of explainable AI methods is to enhance transparency by providing interpretable explanations of how machine-learning predictions are generated from the input features (Alabdulatif, 2025). SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) are two of the most widely used techniques to explain the decision-making process of machine-learning models. These two techniques are helpful for researchers because they help them understand what features played important roles in the final decision made by the model, while also allowing for the generation of global model interpretation as well as local model interpretations for individual predictions. Thus, they are extremely helpful to researchers involved with the development of cybersecurity monitoring systems (Lee et al., 2024).

An important issue that has been actively explored by researchers is how to analyze the streaming security data that is produced from smart systems. For instance, many smart infrastructure systems continuously produce large amounts of real-time data from various sources such as network traffic flows, Internet of Things (IoT) sensors, system logs, and cloud telemetry (Moustafa et al., 2023). As such, there is a need for real-time analytics on these smart infrastructures with high predictive accuracy and computational efficiency in order to effectively process these streams of security data for intrusion detection purposes. Researchers have proposed stream-based intrusion detection frameworks that utilize online learning algorithms to facilitate real-time threat detection in dynamically changing environments.

Recent studies have shown that using machine learning based detection techniques in conjunction with explainable artificial intelligence (XAI) technologies can significantly improve the ability of the cybersecurity systems to detect threats both accurately and explainably (Patel et al., 2025). By utilizing various combinations of machine learning models such as Random Forest, XGBoost, LSTM Networks and XAI methodologies like SHAP and LIME to explain the predictions produced by these models, cybersecurity professionals can not only identify potential threats but also understand the reasons for the prediction produced by the machine learning models (Akshya et al., 2025). There is enhanced need for integrated cybersecurity frameworks that contain high-performance machine learning models, real-time streaming processing systems and XAI techniques to produce a transparent and trustworthy approach to detecting cyber threats in smart systems 16. (Rystygulova et al., 2025).

Therefore, in order to address this need, this paper proposes an interpretable AI framework for detecting cyber threats using real-time data obtained from smart systems. This framework incorporates the use of Random Forest, XGBoost and LSTM models along with SHAP and LIME XAI methodologies in order to maintain an accurate method of detecting threats in real-time while providing a clear explanation of the predictions made by these models.

Materials and methods. The amount of heterogeneous, streaming data generated by today's smart systems is extremely high, and includes data that is generated by IoT devices, system logs, network traffic, and data created in the cloud. The environments created by these systems are highly dynamic and susceptible to a wide range of cyber threats, such as DDoS attacks, data injection, botnet activity, and man-in-the-middle attacks. To effectively detect and understand any such threats, there

needs to be an integration of different types of analysis methods or techniques that utilize machine learning algorithms to detect anything from malware to unauthorized access.

The experimental evaluation utilized two benchmark cybersecurity datasets: CICIDS2017 and UNSW-NB15. The CICIDS2017 dataset contains over 2.8 million network flow records. Each record contained 78 features, drawn from real-world network traffic, ranging from benign to malicious activity, such as denial of service (DoS), distributed denial of service (DDoS), botnets, and penetration attacks.

The UNSW-NB15 dataset contains approximately 2.5 million records, representing 49 features reflecting a range of modern attack categories, such as exploits, reconnaissance attacks, backdoor attacks, and shellcode attacks. Using more than one dataset ensures the robustness and generalizability of the proposed framework across various cyberthreat scenarios and network conditions.

Before training the models the datasets were first preprocessed by addressing the missing data points, normalizing the numeric features, and encoding any categorical features prior to feature scaling for consistency between the input variables. The datasets were then split into training (70%) and test (30%) datasets. Cross-validation was also used while training the models for additional robustness and to help avoid overfitting.

Model training was performed using the Random Forest, XGBoost, and LSTM machine learning models with optimum hyperparameters. The final hybrid XAI model combines multiple detection methods in one model to produce a higher overall performance. Model evaluation was performed using standard classification metrics, including accuracy, precision, recall, and the F1-score.

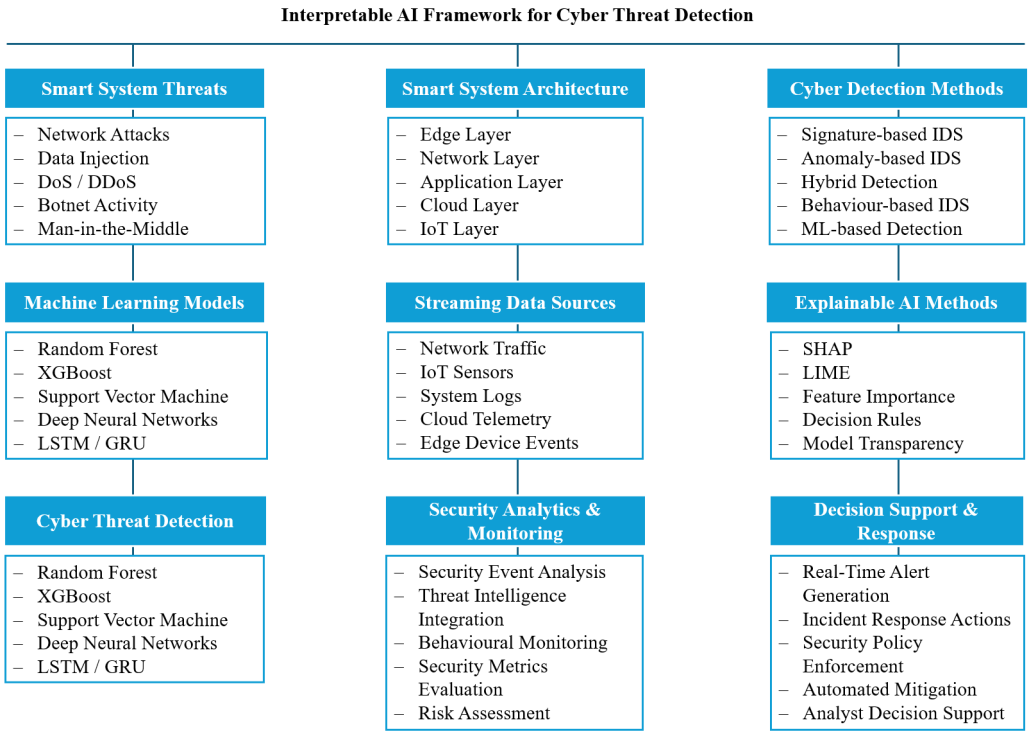

Figure 1. Conceptual framework of AI-based cyber threat detection

The proposed AI-based cyber threat detection system includes important components of intelligent security monitoring in streaming and smart environments, as shown in Figure 1, which serves to represent the structural relationships between these components and provides a basic framework for developing an AI assessment model or intelligent security monitoring as having a conceptual basis. The framework describes all aspects of a cyber threat (network attacks, data injection, denial-of-service (DoS) and DDoS attacks, botnets), it also provides a detailed analysis of leading cyber threats to both IoT and cloud infrastructures.

The intelligent systems environment consists of many different data streams that are continuously generated (IoT sensor data, network traffic streams, system logs, cloud data and telemetry, and edge devices). All these distributed data sources form the basis for real-time, analytical threat detection.

This framework also defines a multi-layered detection paradigm that combines signature-based detection with anomaly detection and hybrid intrusion detection approaches through the application of advanced machine learning techniques, including ensemble machines (Random Forest, XGBoost), traditional classifiers such as support vector machines, and deep learning architectures such as LSTM and GRU, enabling meaningful classification. and anomaly detection in multidimensional streaming data.

Furthermore, the framework incorporates explainable AI methods (SHAP, LIME) that provide global and local interpretability of model decisions. These methods will enable higher-quality feature-level analysis, improved transparency of the model's predictive logic, and increased confidence in automated threat detection.

Furthermore, the framework incorporates decision support/risk management capabilities, including behavioral monitoring; threat intelligence integration; risk assessment; and real-time incident response support, enabling analysts to interpret model outputs and make informed decisions to mitigate cyberthreats.

The presented conceptual framework describes a theoretical model for developing a data-driven cyberthreat detection system and demonstrates the relationship between detection accuracy, model transparency, and the ability to process threat detection data generated by the system in near real time.

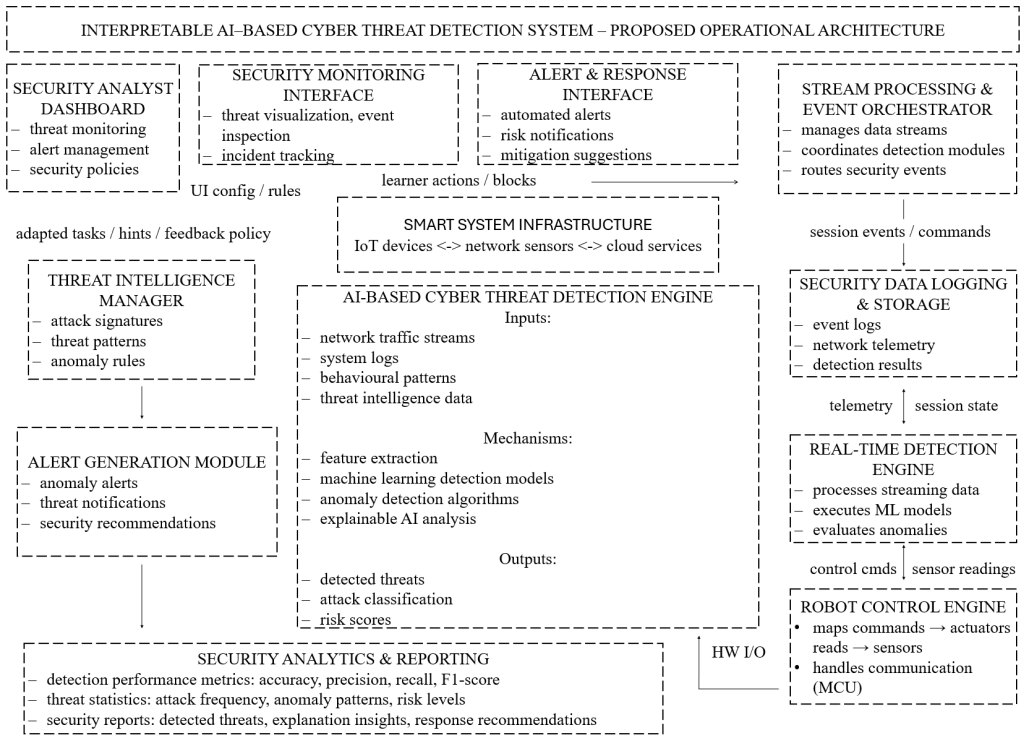

Figure 2. Architecture of the Proposed Cyber Threat Detection System

The presented conceptual diagram provides the theoretical basis for the operational architecture of the cyber threat detection system, shown in Figure 2.

Figure 2 presents the operational architecture of the proposed cyber threat detection system, while Figure 1 provides its conceptual representation. The architecture generates and stores processed large volumes of security data from intelligent systems, such as IoT devices, network sensors and appliances, and cloud services, in a stream processing layer and an event orchestration layer, which

continuously manage stream processing and synchronization related to security data and security events across multiple analytics modules.

Collected data from the stream processing layer is stored in a security data logging/storage module, which maintains a structured log of network telemetry, system logs, and detection engine output. The logging and storage module is used for real-time monitoring and retrospective analysis.

An AI-powered cyberthreat detection engine is the core of the architecture, performing feature extraction, anomaly detection, and network behavior classification. The system uses a combination of machine learning techniques to process various types of input data, including traffic, system activity, and a variety of threat data.

The cyberthreat detection system generates multiple outputs, including threat identification, behavior classification, quantitative risk assessment (measurable probability) of anomalies, and outputs for explainability modules that interpret the model's decision based on its contribution.

Anomalies are sent to the alert generation module, which generates real-time alerts, incident notifications, and remediation recommendations. These outputs are available to users through an interface designed for cybersecurity analysts to support operational decision making.

The architecture also includes data analysis and reporting to evaluate model performance using standardized performance metrics and to identify patterns in the threat landscape, system activity, and detection effectiveness. The proposed architecture is a fully scalable and interpretable cyber threat detection system that leverages machine learning and explainable artificial intelligence in a common data processing pipeline.

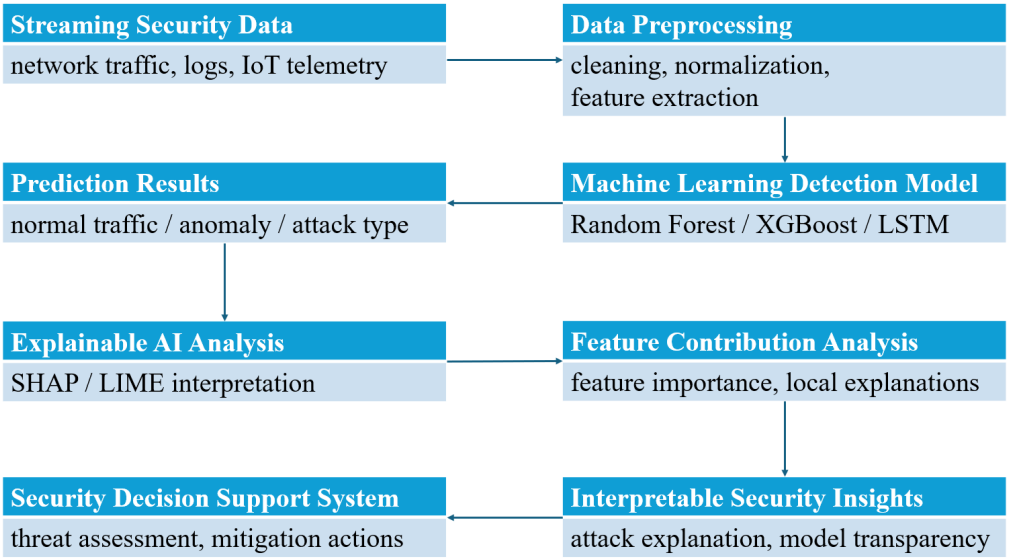

Figure 3. Explainable artificial intelligence workflow

The Workflow of Explainable Artificial Intelligence for Understanding the Predictions of a Cyber Threat Detection Model from a Streaming Smart System is illustrated in Figure 3. The proposed Cyber Threat Detection Model uses a combination of streaming security data from various sources, network traffic, system logs, and IOT telemetry. This data is then pre-processed into relevant features before being fed into different machine learning models (i.e., Random Forest, XGBoost, and LSTM). Each of these models outputs the predictions of what is considered normal traffic, anomalies, or a potential type of attack. The last step involves using Explainable Artificial Intelligence techniques such as SHAP and LIME to evaluate how much each feature contributes to the decision made by the Machine Learning Model. This process allows users to interpret different security views and develop security insights in order for users to facilitate their assessment of cyber threats and assist with decision-making in terms of mitigating the threat, through the Cybersecurity Monitoring System.

In the implementation of the Cyber Threat Detection Framework, various machine learning models (ML) and explainable artificial intelligence methodologies (EAI) were employed. The ML

algorithms chosen were based on their success in network intrusion detection and for their ability to handle large amounts of streaming security data. A summary of the machine learning and EAI models can be found in Table 1.

Table 1. Machine learning models and explainable AI methods used for cyber threat detection

ML Model	Type	Role in the Detection System
Random Forest	Ensemble learning	Network traffic classification and anomaly detection
XGBoost	Gradient boosting	High-performance intrusion detection and pattern recognition
LSTM	Deep learning	Detection of temporal patterns in streaming network data
SHAP	Explainable AI method	Global feature importance analysis and model interpretability
LIME	Explainable AI method	Local explanation of individual prediction decisions

XGBoost and Random Forest algorithms are popular in cybersecurity applications because they can successfully classify and handle large amounts of multidimensional data. An LSTM (Long Short-Term Memory) neural network was chosen as it can effectively analyze time-series data and the sequential behavior of data over time. Techniques for increasing model transparency through Explainable Artificial Intelligence (XAI) such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) were added to the proposed framework, providing the opportunity to analyze the exact contribution of each feature to the predictions made by each model while providing the user with a clear understanding of how any model determines whether or not to classify an event as a cyber threat. As machine learning detection methods and AI have been combined, the ability for the user to trust and understand the results of the proposed cybersecurity monitoring system will continue to grow with further development, ultimately creating an extremely reliable and highly useful cybersecurity monitoring system.

Results and discussions. A global analysis of how important features are for predicting outcomes was conducted on machine learning systems to evaluate how interpretable the proposed cyber-threat detection method is. Feature importance takes a look at how much each input variable contributes when the model makes its prediction and gives you some evidence of how the detection method works under the hood.

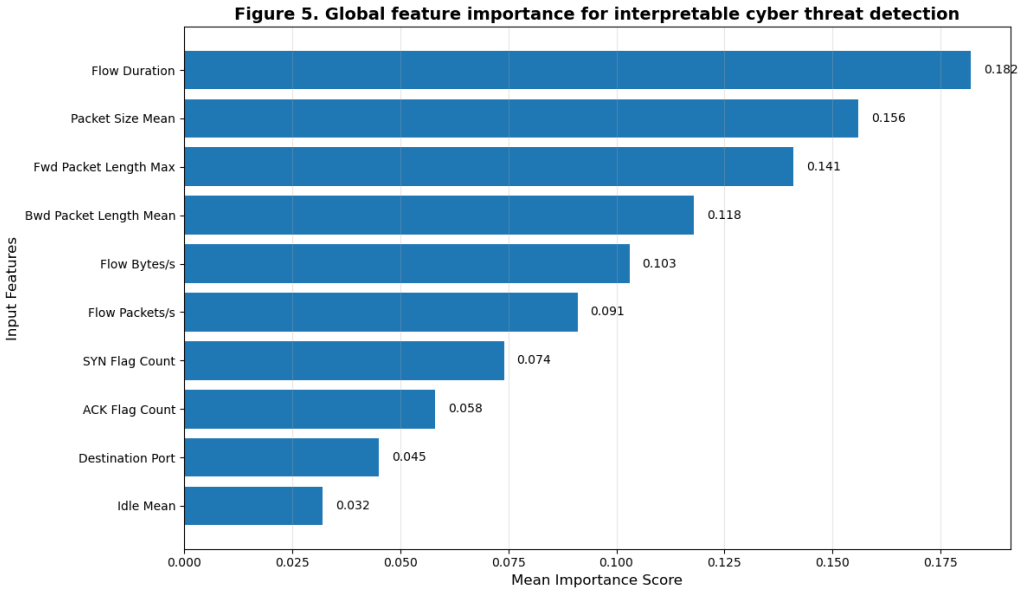

Figure 4. Global feature importance analysis for interpretable cyber threat detection

Figure 4 shows in order of ranked importance how important each of the ten most influential features of network traffic extracted from the streaming cybersecurity datasets are to the classification

process as measured by their mean contribution across all trained models. As indicated in the figure, the single feature that contributed the most to model classification is Flow Duration with an average importance score of .182. This metric represents the temporal characteristics of network communication sessions and can often be found in association with various types of abnormal traffic including those associated with Denial of Service (DoS) attacks and botnet activity. Network communication sessions that are attacked typically show abnormal flow durations compared to legitimate network flow duration patterns.

The second highest ranked classification feature is Packet Size Mean at .156. This metric indicates the mean packet size over a period of communication between hosts. Malicious traffic typically exhibits variations in the distribution of packet sizes, particularly with respect to reconnaissance activities (i.e., scanning) and data exfiltration.

The third highest classification feature is the Forward Packet Length Maximum at .141. This metric indicates the maximum packet size of a flow of packets that have been transmitted in the forward direction. Large bursts of packets or aberrant payload sizes may indicate suspicious network activity (e.g., data exfiltration and/or command-and-control activity).

The Backward Packet Length Mean, Flow Bytes per Second, and Flow Packets per Second features also contribute to the detection process with an importance score of .118, .103, and .091, respectively. These metrics describe the volume of network traffic between hosts over a specified period of time and bandwidth consumed, both of which are often used as indicators of abnormal network activity.

Metrics such as SYN Flag Count, ACK Flag Count, and Destination Port all contribute to the detection measures but are considered less important than the previously listed features. These metrics reflect characteristics of connections between the source and destination of the traffic being analyzed and the protocols used to establish the connections and can be used in the detection of scanning activity and network probing.

The overall results confirm that this feature set represents the most important characteristics of network traffic behavior and therefore support the interpretability of the detection framework. The integration of feature importance analysis supports the explainable artificial intelligence framework as described in the methodology section and enables cyber security analysts to identify the variables that influence the model predictions.

Comparison of Cyber threat detection models performance. The goal of this section was to compare the effectiveness of our AI-based detection system through a comparative analysis of four different machine learning models (Random Forest, XGBoost, LSTM, and our Hybrid XAI Model). Our four chosen models were all known for their ability to perform well when trying to detect network intrusion as well as for being able to handle large amounts of streaming data in the field of cybersecurity.

Four widely used classification performance metrics were used to conduct our comparative analysis: (1) accuracy, (2) precision, (3) recall, and (4) F1-score.

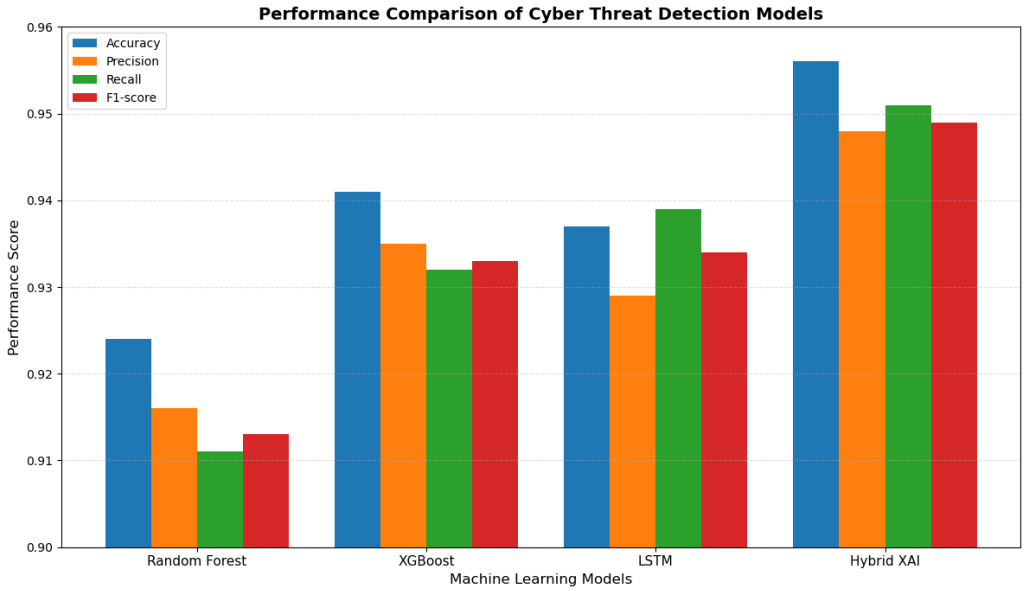

Figure 5. Performance comparison of cyber threat detection models

The models presented in this Figure 5 demonstrate the performance results based on each of the assessed performance criteria. Based on the study results, it can be concluded that Hybrid XAI produces the best overall results across all performance metrics assessed, outpacing all of the individual machine learning models.

The Random Forest model acted as the baseline model with an approximate accuracy of 0.924, a precision of 0.916, and a recall of 0.911. Random Forest provides relatively stable classification accuracy, but does not have the capacity to capture intricate temporal patterns that are present in network traffic.

The XGBoost model outperformed Random Forest, achieving an accuracy rate of 0.941, and a precision score of 0.935. Gradient boosting has demonstrated excellent modelling abilities of complex non-linear relationships in high dimensional data, which explains the increased accuracy rates observed between Random Forest and XGBoost.

The LSTM model is slightly less accurate than XGBoost, yet has a higher recall score than XGBoost (0.939). This finding is expected given the ability of Recurrent Neural Networks such as LSTM to accurately capture temporal dependencies in sequentially ordered network traffic data. As such, LSTM is more able to accurately identify specific types of cyberattacks that exhibit time-based behaviour patterns.

The Hybrid XAI model showcases the highest level of success, achieving an accuracy of 0.956, precision of 0.948, recall of 0.951, and F1 score of 0.949. The hybrid model was able to work better by combining many different techniques for detection, along with using both the ML prediction techniques and explainable AI techniques.

This study has shown that using hybrid approaches of using traditional statistical machine learning algorithms with explainable artificial intelligence methods will improve both the accuracy and compliance of detecting if the cybersecurity monitoring system is functioning correctly.

Confusion matrix analysis of cyber threat classification. To continue evaluating the performance of the classifier via this detection system, we performed an analysis of the confusion matrix. A confusion matrix presents a thorough representation of all classification results produced by the classifier, separated by type of cyber attack classified and identifying any potential trends of misclassification.

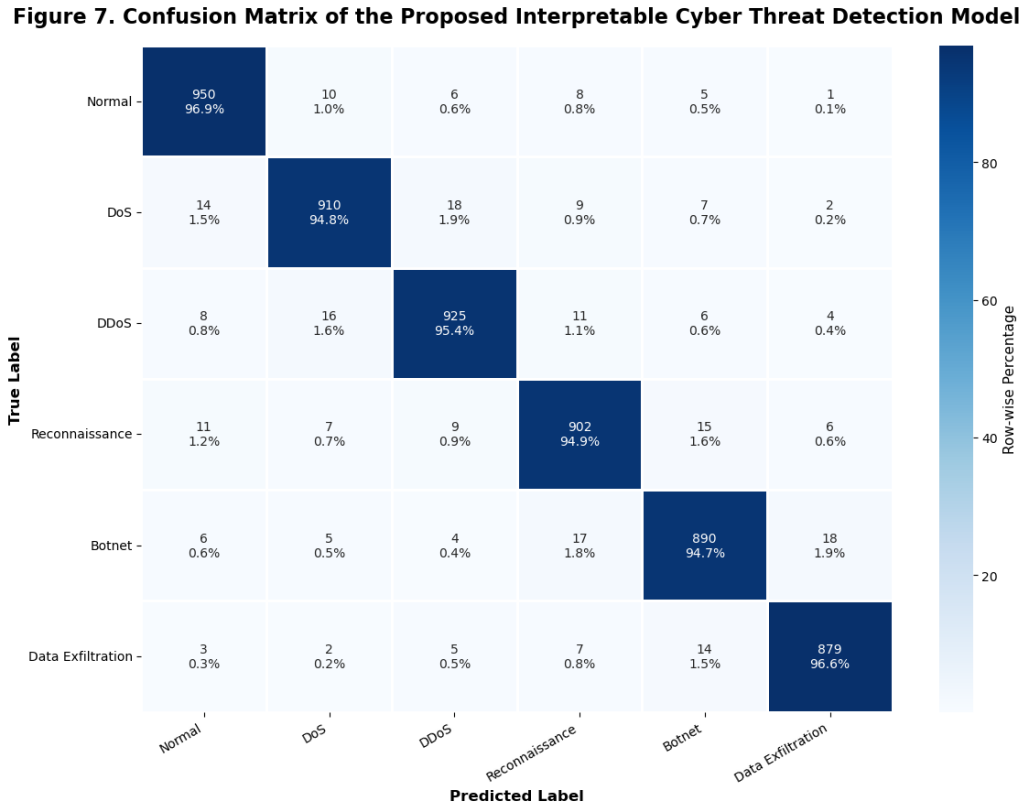

Figure 6. Confusion matrix of the proposed interpretable cyber threat detection model

The confusion matrix for the interpretable cyber threat detection system proposed in this work is shown in Figure 6. This matrix demonstrates the performance of the proposed model across six different categories for classifying traffic or cyber threats (systems are typically categorised according to the following types):

- Normal Traffic
- Denial of Service (DoS) Attacks
- Distributed Denial of Service (DDoS) Attacks
- Reconnaissance Activity
- Botnets
- Data Exfiltration

As can be seen from the confusion matrix, the classification accuracy of each type of traffic (or cyber threat) generated by the proposed system is very high with almost all of the correctly classified instances being located along the diagonal of the confusion matrix. Further, a very small number of normal traffic instances were misclassified as attacks. Therefore, the proposed system has a very low false positive rate.

For example, with respect to normal network traffic, the proposed model correctly classifies 96.9% of instances. A small number of normal traffic instances are classified incorrectly; however, these instances were classified as a type of attack, which indicates that the proposed system has a low false positive rate.

Similarly, for DoS and DDoS types of attacks, the proposed model achieved classification accuracies of 94.8% and 95.4%, respectively. The majority of misclassifications are the result of attack types that exhibit some overlap (the same behaviour will exhibit characteristics that closely resemble one another); therefore, misclassifying one attack for another, when they share similar behaviours, is a common problem in network intrusion detection systems.

The accuracy for identifying reconnaissance activity (scanning and probing a network to determine its vulnerabilities) is 94.9%. There are a small number of instances of overlapping scanning behaviour between reconnaissance (i.e., scanning) and botnet activity, which results in a small number of misclassifications.

The accuracy of botnet detection is 94.7%, while the accuracy of detecting data exfiltration is 96.6%. The high detection rate of data exfiltration is particularly important because many of these attacks involve the possible loss of sensitive personal or proprietary information.

Discussion of results. The findings of the conducted experiments support the usefulness of the suggested AI framework for detecting cyber threats in real-time for smart systems. The evaluation of the importance of features indicates that significant characteristics of network traffic (flow duration, packet size statistics, and traffic rate indicators) are heavily relied upon, which are commonly used in cyber security research as reliable indicators of anomalous behavior within a network. The results of the comparison of performance indicate that ML techniques provide much greater capabilities to detect cyber threats than baseline models. More specifically, the hybrid XAI (explainable artificial intelligence) model produced the best results as based on all evaluation metrics, which suggests that multiple forms of machine learning alongside explananble AI techniques enable improved accuracy in predicting cyber threats and increasing transparency of machine learning models. It has also been shown in the confusion matrix analysis that the suggested system is capable of distinguishing between various categories of cyberattacks with very low misclassification rates. These findings show that there is a significant benefit to the combination of machine learning models for detecting cyber threats with interpretable analysis techniques to enhance the quality of real-time cybersecurity monitoring in complex smart environments.

Conclusion. An Artificial Intelligence framework has been developed which is interpretable and provides cyber threat identification in real time for smart systems using a streaming approach. In developing the proposed Hybrid XAI model, machine learning techniques (i.e. Random Forest, XGBoost, LSTM) are used in addition to explainable AI mechanisms (i.e. SHAP, LIME) to improve not only the ability to detect a cyber threat but also to provide interpretable insight about how detection was performed. Using Statistical Analysis of the Experimental Results of the proposed Hybrid XAI Model, it was demonstrated that the Hybrid XAI model outperforms the others in virtually every aspect of performance (i.e. Accuracy, Precision, Recall & F1 Score) while being able to successfully identify all styles of cyber attacks. Statistical Analysis of the Feature Importance confirmed the identifying characteristics of network traffic used to determine when traffic utilizes anomalous behavior, including but not limited to flow duration, packet size statistics, and traffic rates.

This new framework has the potential to be utilized in live monitoring systems for cyber threats in smart cities (i.e. cities that have adopted IoT) and can be used in Cloud Technology (software as a service) as well as IoT infrastructures; enabling detection processes to interpret and reliably detect cyber threats in ever-changing environments.

Several limitations must be considered with respect to the strong overall performance described herein through the proposed framework; specifically, evaluation conducted using benchmark data sets may not adequately represent the full range of variability that can occur in actual network environments and, further, the computational expense of the explainable AI techniques applied might also restrict their use for real-time applications within larger-scale systems.

Future studies will therefore focus on the validation of this framework within a real-world deployment, development of heuristics for optimizing computational efficiency, integration of adaptive learning techniques to manage concept drift with respect to streaming data.

The research demonstrated that it is feasible to create a combination of intrusion detection using machine learning techniques and a mechanism for providing explanations of how the intrusion detection model works, resulting in increased value of providing an effective method for monitoring cyber security in the modern smart infrastructure.

References

Akshya J. et al. Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems //Cluster Computing. – 2025. – Т. 28. – №. 14. – С. 884. https://doi.org/10.1007/s10586-025-05617-1

Al Rawajbeh M. et al. Trustworthy adaptive AI for real-time intrusion detection in industrial IoT security //IoT. – 2025. – Т. 6. – №. 3. – С. 53. https://doi.org/10.3390/iot6030053

Alabdulatif A. A novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence //Applied Sciences. – 2025. – Т. 15. – №. 14. – С. 7984. https://doi.org/10.3390/app15147984

Almheiri S. J. et al. Smart sustainable cyber security: modelling an interpretable and transparent threat detection with explainable artificial intelligence //Discover Sustainability. – 2025. – Т. 6. – №. 1. – С. 442. https://doi.org/10.1007/s43621-025-01280-z

Alshudukhi K. S. et al. Next-Generation Lightweight Explainable AI for Cybersecurity: A Review on Transparency and Real-Time Threat Mitigation //Computer Modeling in Engineering & Sciences. – 2025. – Т. 145. – №. 3. – С. 3029. https://doi.org/10.32604/cmes.2025.073705
Jumagaliyeva A. et al. Application of Deep Learning Methods for Visual Pattern Recognition in Heterogeneous Images // Bulletin of KazATC. – 2025. – Vol. 141. – No. 6. – pp. 195–208. DOI: https://doi.org/10.52167/1609-1817-2025-141-6-195-208
Kalutharage C. S., Liu X., Chrysoulas C. Neurosymbolic learning and domain knowledge-driven explainable ai for enhanced iot network attack detection and response //Computers & Security. – 2025. – Т. 151. – С. 104318. https://doi.org/10.1016/j.cose.2025.104318
Khalaf N. Z. et al. Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure //Mesopotamian Journal of CyberSecurity. – 2025. – Т. 5. – №. 2. – С. 501-513. https://doi.org/10.55248/gengpi.6.0525.1991
Lee H. et al. Enhancing Decision-Making of Network Intrusion Analysis Assisted by Explainable AI for Real-Time Security Monitoring //2024 IEEE Conference on Dependable and Secure Computing (DSC). – IEEE, 2024. – С. 147-154. https://doi.org/10.1109/dsc63325.2024.00039
Mohale V. Z., Obagbuwa I. C. A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity //Frontiers in Artificial Intelligence. – 2025. – Т. 8. – С. 1526221. https://doi.org/10.3389/frai.2025.1526221
Moustafa N. et al. Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions //IEEE Communications Surveys & Tutorials. – 2023. – Т. 25. – №. 3. – С. 1775-1807. https://doi.org/10.1109/comst.2023.3280465
Patel T. et al. Enhancing Cybersecurity in Internet of Vehicles: A Machine Learning Approach with Explainable AI for Real-Time Threat Detection //Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing. – 2025. – С. 2024-2031. https://doi.org/10.1145/3672608.3707769
Paul A. L. Explainable AI for Cybersecurity: Interpreting Deep Learning Models for Real-time Threat Detection in IoT Networks. https://doi.org/10.1109/iccosd66074.2025.11348330
Prasad H., Prasad U., Paul P. Explainable AI for Cybersecurity: Implementing Interpretable Models for Real-Time Threat Detection //2025 International Conference on Communication and Smart Devices (ICCoSD). – IEEE, 2025. – Т. 1. – С. 1-6. https://doi.org/10.1109/iccosd66074.2025.11348330
Rahmati M. Towards explainable and lightweight AI for real-time cyber threat hunting in edge networks //arXiv preprint arXiv:2504.16118. – 2025. https://doi.org/10.21203/rs.3.rs-6198488/v1
Rystygulova V., Bizhanova K., Kadirkulov S., Asilbaeva R., & Makhatova V. (2025) Methodological framework for building interpretable machine learning models in applied forecasting. Vestnik KazATC, 141(6), 143–153. https://doi.org/10.52167/1609-1817-2025-141-6-143-153
Thiruvenkatasamy S. et al. Real-Time Intrusion Detection System for Wi-Fi-Based Wireless Sensor Networks using Deep Learning and Explainable AI //2025 10th International Conference on Smart Structures and Systems (ICSSS).-IEEE, 2025.-С.1-10. https://doi.org/10.1109/icsss66939.2025.11346435

МРНТИ 28.23.37 DOI: https://doi.org/10.62687/STJ.7.1.2025.19

ГИБРИДНАЯ РЕКОМЕНДАТЕЛЬНАЯ МОДЕЛЬ ДЛЯ РАСПРЕДЕЛЕНИЯ СТУДЕНТОВ МЕЖДУ НАУЧНЫМИ НАСТАВНИКАМИ

[1]С.Ж. Советов*, **[2]А.С. Аканова**, **[3]Н.С. Ермекова**
[1]Международный университет Астана, Астана, Казахстан
[2]Казахский агротехнический исследовательский университет имени С. Сейфуллина, Астана, Казахстан
[3]НАО «Жетысуский университет имени И. Жансугурова», Талдыкорган, Казахстан
*e-mail: sultan_sovetov@stu.aiu.edu.kz

С.Ж. Советов – магистрант высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: sultan_sovetov@stu.aiu.edu.kz, https://orcid.org/0009-0005-0111-9075

А.С. Аканова – кафедра компьютерных наук, Казахский агротехнический исследовательский университет имени С. Сейфуллина, Астана, Казахстан, e-mail: akerkegansaj1995@gmail.com, https://orcid.org/0000-0002-7178-2121

Н.С. Ермекова – магистр педагогических наук, лектор-преподаватель, НАО «Жетысуский университет имени И. Жансугурова», Талдыкорган, Казахстан, e-mail: nabira.ermekova@mail.ru, https://orcid.org/0000-0002-4798-4540

Аннотация. В данной статье рассматривается проблема распределения студентов и научных руководителей в высшем образовании путем предложения гибридной рекомендательной системы, основанной на искусственном интеллекте и обработке естественного языка (NLP). Для преодоления семантических и когнитивных барьеров между исследовательскими предложениями студентов и компетенциями научных руководителей система использует многоязычную архитектуру Sentence-BERT (SBERT) для генерации плотных векторных представлений, обеспечивая высокоточное семантическое сопоставление на английском, русском и казахском языках. Кроме того, модель интегрирует модифицированный алгоритм оптимизации Гейла-Шепли для обеспечения справедливого распределения академической нагрузки и предотвращения выгорания научных руководителей, успешно уменьшая дисбаланс рабочей нагрузки. Предложенная микросервисная архитектура также включает в себя объяснимый искусственный интеллект (XAI) для обеспечения прозрачных обоснований сопоставления и динамический механизм пороговой обработки для обработки аномальных или узкоспециализированных запросов типа «холодный старт». В конечном итоге, этот подход, основанный на данных, повышает качество академического наставничества, снижает академические трения и предлагает масштабируемое ИТ-решение, готовое к бесшовной интеграции в современные университетские системы управления обучением (LMS).

Ключевые слова: Рекомендательная система, обработка естественного языка, Sentence-BERT, оптимизация рабочей нагрузки, алгоритм Гейла-Шепли, объяснимый искусственный интеллект (XAI), управление высшим образованием, микросервисная архитектура.

HYBRID RECOMMENDATION MODEL FOR ALLOCATING STUDENTS AMONG RESEARCH SUPERVISORS

[1]S.Zh. Sovetov*, **[2]A.S. Akanova**, **[3]N.S. Ermekova**
[1]Astana International University, Astana, Kazakhstan
[2]Saken Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan
[3]Zhetysu University named after I. Zhansugurov, Taldykorgan, Kazakhstan
*e-mail: sultan_sovetov@stu.aiu.edu.kz

S.Zh. Sovetov – Master's student of the Higher School of Information Technology and Engineering, Astana International University (AIU), Astana, Kazakhstan, e-mail: sultan_sovetov@stu.aiu.edu.kz, https://orcid.org/0009-0005-0111-9075

A.S. Akanova – Department of Computer Science, Saken Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan, e-mail: akerkegansaj1995@gmail.com, https://orcid.org/0000-0002-7178-2121

N.S. Ermekova – Master of Pedagogical Sciences, Lecturer, Zhetysu University named after I. Zhansugurov, Taldykorgan, Kazakhstan, e-mail: nabira.ermekova@mail.ru, https://orcid.org/0000-0002-4798-4540

Abstract. This paper addresses the problem of student and supervisor placement in higher education by proposing a hybrid recommender system based on artificial intelligence and natural language processing (NLP). To overcome the semantic and cognitive barriers between students' research proposals and supervisor competencies, the system uses the Sentence-BERT (SBERT) multilingual architecture to generate dense vector representations, enabling highly accurate semantic matching in English, Russian, and Kazakh. Furthermore, the model integrates a modified Gale-Shapley optimization algorithm to ensure fair distribution of academic workload and prevent supervisor burnout, effectively mitigating workload imbalances. The proposed microservice architecture also incorporates explainable artificial intelligence (XAI) to provide transparent matching rationales and a dynamic thresholding mechanism to handle anomalous or highly specialized c̈old startq̈ueries. Ultimately, this data-driven approach improves the quality of academic mentoring, reduces academic friction, and offers a scalable IT solution ready for seamless integration into modern university learning management systems (LMS).

Keywords: Recommender system, natural language processing, Sentence-BERT, workload optimization, Gale-Shapley algorithm, explainable artificial intelligence (XAI), higher education management, microservice architecture.

СТУДЕНТТЕРДІ ҒЫЛЫМИ ЖЕТЕКШІЛЕР АРАСЫНДА БӨЛУГЕ АРНАЛҒАН ГИБРИДТІ ҰСЫНЫС МОДЕЛІ

[1]С.Ж. Советов*, [2]А.С. Ақанова, [3]Н.С. Ермекова

[1]Астана Халықаралық Университеті, Астана, Қазақстан

[2]С. Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті, Астана, Қазақстан

[3]І. Жансүгіров атындағы Жетісу университеті, Талдықорған қ., Қазақстан

*e-mail: sultan_sovetov@stu.aiu.edu.kz

С.Ж. Советов - Ақпараттық технологиялар және инженерия жоғары мектебінің магистранты, Астана Халықаралық Университеті (AIU), Астана қ., Қазақстан, e-mail: sultan_sovetov@stu.aiu.edu.kz, https://orcid.org/0009-0005-0111-9075

А.С. Ақанова - компьютерлік ғылымдар кафедрасы, С. Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті, Астана қ., Қазақстан, e-mail: akerkegansaj1995@gmail.com, https://orcid.org/0000-0002-7178-2121

Н.С. Ермекова - педагогика ғылымдарының магистрі, дәріскер-оқытушы, І. Жансүгіров атындағы Жетісу университеті, Талдықорған қ., Қазақстан, e-mail: nabira.ermekova@mail.ru, https://orcid.org/0000-0002-4798-4540

Аңдатпа. Бұл мақалада жоғары білім беруде студенттер мен жетекшілерді орналастыру мәселесі қарастырылады, ол жасанды интеллект пен табиғи тілді өңдеуге (NLP) негізделген гибридті ұсыныс беру жүйесін ұсынады. Студенттердің зерттеу ұсыныстары мен жетекшінің құзыреттіліктері арасындағы семантикалық және когнитивті кедергілерді жеңу үшін жүйе тығыз векторлық көріністерді жасау үшін Sentence-BERT (SBERT) көптілді архитектурасын пайдаланады, бұл ағылшын, орыс және қазақ тілдерінде жоғары дәлдіктегі семантикалық сәйкестендіруді қамтамасыз етеді. Сонымен қатар, модель академиялық жұмыс жүктемесінің

әділ бөлінуін қамтамасыз ету және жетекшінің күйіп кетуіне жол бермеу үшін өзгертілген Gale-Shapley оңтайландыру алгоритмін біріктіреді, бұл жұмыс жүктемесінің теңгерімсіздігін тиімді түрде азайтады. Ұсынылған микросервис архитектурасы сонымен қатар ашық сәйкестендіру негіздемелерін және аномальды немесе жоғары мамандандырылған «суық бастау» сұраныстарын өңдеу үшін динамикалық шекті механизмді қамтамасыз ету үшін түсіндірілетін жасанды интеллектті (XAI) қамтиды. Сайып келгенде, бұл деректерге негізделген тәсіл академиялық тәлімгерліктің сапасын жақсартады, академиялық үйкелісті азайтады және заманауи университеттік оқуды басқару жүйелеріне (LMS) үздіксіз интеграциялауға дайын масштабталатын IT шешімін ұсынады.

Кілт сөздер: Ұсыныс жүйесі, табиғи тілді өңдеу, Сөйлем-BERT, жұмыс жүктемесін оңтайландыру, Гейл-Шапли алгоритмі, түсіндірілетін жасанды интеллект (XAI), жоғары білім беруді басқару, микросервис архитектурасы.

Введение. В условиях массового высшего образования парадигма научного руководства претерпевает существенные изменения. Роль преподавателя смещается от простой трансляции знаний к глубокому академическому наставничеству и формированию индивидуальных образовательных траекторий обучающихся критичных точек управления образовательным процессом является задача распределения студентов по научным руководителям (Student-Supervisor Allocation Problem, SSAP).

Как показывают исследования в области анализа данных в сфере образования, использование административных методов распределения или случайного отбора приводит к явлению «академического трения» (Tinto, 1993). Несоответствие глубоких исследовательских интересов научного руководителя и магистранта снижает внутреннюю мотивацию последнего, приводит к прокрастинации, задержкам в защите диссертации и увеличивает риск академической отсева (показатели отсева) (Holmes и др., 2019:194). Поэтому существует острая необходимость интегрировать алгоритмы искусственного интеллекта (ИИ) в педагогический процесс для создания интеллектуальных систем рекомендаций.

Для достижения комплексного решения проблемы распределения студентов и научных руководителей (SSAP) важно глубоко исследовать теоретически масштабируемую архитектуру системы на основе микросервисов, способную интегрировать предложенную модель рекомендаций, основанную на обработке естественного языка (NLP), в существующие университетские системы управления обучением (LMS), обеспечивая при этом алгоритмическую справедливость и смягчая проблему «холодного старта» для междисциплинарных исследовательских тем. Эта задача позволяет преодолеть разрыв между чистой математической оптимизацией и реальным развертыванием программного обеспечения в образовательной ИТ-экосистеме.

Целью данного исследования является разработка и теоретическое обоснование гибридной модели рекомендаций на основе искусственного интеллекта, позволяющей семантически точно сопоставлять задания студентов с научными руководителями при сохранении сбалансированной академической нагрузки.

Для достижения этой цели были определены следующие **исследовательские задачи**:

1. Адаптировать многоязычную семантическую модель (на основе Sentence-BERT) для преодоления когнитивных барьеров и точного сопоставления исследовательских запросов магистрантов с компетенциями преподавателей.

2. Разработать механизм многокритериальной оптимизации на основе алгоритма Гейла-Шепли для предотвращения дисбаланса рабочей нагрузки преподавателей.

Научная новизна данного исследования заключается в создании синергетической гибридной модели, которая впервые комплексно решает проблему SSAP в многоязычной среде. Новизна заключается в сочетании многоязычного нейронного семантического движка (SBERT) для глубокого понимания контекста, алгоритма Гейла-Шепли для строгого контроля балансировки нагрузки и модуля объяснимого искусственного интеллекта (XAI), который гарантирует прозрачность алгоритмов и доверие к принимаемым решениям.

Когнитивные и коммуникативные барьеры в образовательной среде

Основная причина неэффективности ручных заданий заключается в семантических и когнитивных барьерах между участниками академического процесса. Магистранты, находящиеся на начальном этапе своей исследовательской карьеры, склонны формулировать свои запросы в общих терминах, используя популярную терминологию. Преподаватели, с другой стороны, описывают свои компетенции, используя высокоспециализированные научные категории.

В ИТ предыдущих поколений пытались автоматизировать этот процесс, используя поиск по ключевым словам TF-IDF как описано в формуле 1 (Salton, Buckley, 1988:101). Вес термина t в документе d вычислялся по классической формуле:

$$\text{TF-IDF}(t, d, D) = \text{TF}(t, d) \cdot \log\left(\frac{N}{\text{DF}(t, D)}\right) \quad (1)$$

Формула 1 - TF-IDF

Где N - общее число документов в корпусе D, а DF - количество документов, содержащих термин t.

Однако этот подход имеет серьезный педагогический недостаток: он ищет точные лексические совпадения, игнорируя контекст. Если студент пишет в своей заявке «нейронные сети», но в профиле профессора указано «глубокое обучение», классическая система не сможет установить связь, что приведет к потере оптимального образовательного сочетания.

Теоретико-методологический подход на базе NLP-моделей

С появлением архитектуры Transformer и механизмов внимания произошел технологический сдвиг парадигмы (Vaswani и др., 2017). Для устранения семантического разрыва в данной статье предлагается использовать модели обработки естественного языка (NLP), в частности архитектуру Sentence-BERT (SBERT) (Reimers, Gurevych, 2019:221).

В отличие от более ранних моделей Word2Vec (Wang и др., 2020), SBERT использует сиамские нейронные сети для генерации плотных векторных представлений (вложений) целых предложений и абзацев текста. Для обеспечения инклюзивности образовательного процесса в многоязычной среде Казахстана была выбрана модель paraphrase-multilingual-MiniLM-L12-v2, которая поддерживает более 50 языков (Wang и др., 2020:282). Модель проецирует тексты (на казахском, русском и английском языках) в единое d-мерное семантическое пространство (d = 384).

Степень педагогической и научной релевантности, описанное в во 2ой формуле, между запросом студента (вектор S) и компетенциями наставника (вектор T) вычисляется через косинусное сходство:

$$\text{Cosine}(S, T) = \frac{\sum_{i=1}^{d} S_i T_i}{\sqrt{\sum_{i=1}^{d} S_i^2} \sqrt{\sum_{i=1}^{d} T_i^2}} \quad (2)$$

Формула 2 - Формула векторного сходства

Архитектура предложенной ИИ-системы представлена на Рисунке 1.

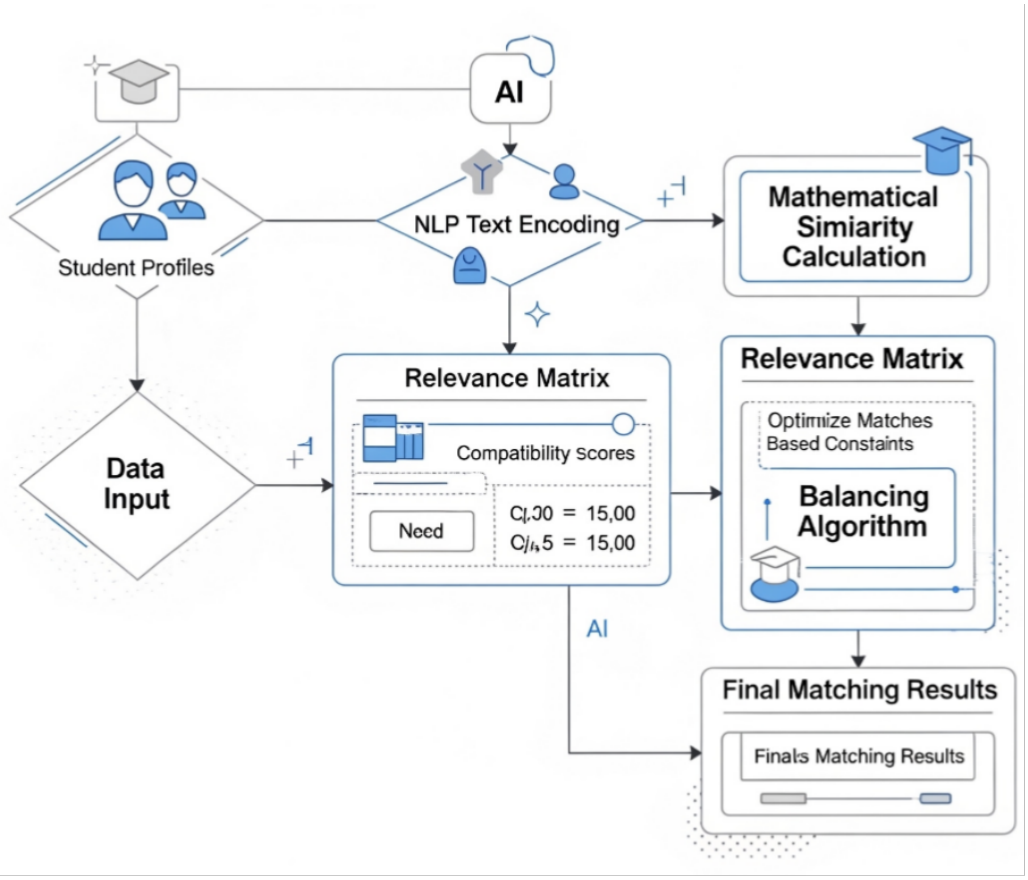

Рисунок 1. Архитектура ИИ-ассистента по распределению магистрантов

Балансировка академической нагрузки и профилактика выгорания

Помимо семантического сопоставления, важным аспектом управления ИТ в университетах является защита преподавателей от переутомления. Неконтролируемые задания студентов приводят к перегрузке некоторых популярных преподавателей, что критически снижает качество наставничества (Serek, Zhaparov, 2019:108).

Для решения этой проблемы косинусные расстояния в формуле 3 вводятся в модуль многокритериальной оптимизации, основанный на модифицированном алгоритме Гейла-Шепли(Gale, Shapley, 1962):

$$\text{Максимизировать } Z = \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij}\, x_{ij} \tag{3}$$

Формула 3 - Модуль оптимизации в алгоритме Гейла-Шепли

С учетом строгого ограничения по квотам (вместимости) каждого руководителя по формуле 4, ограничении:

$$\sum_{i=1}^{N} x_{ij} \leq Q_j, \quad \forall j \in \{1, \ldots, M\} \tag{4}$$

Формула 4 - Ограничения.

Для оценки справедливости распределения нагрузки в работе применяется макроэкономический и специализированный индекс Джини (Luan и др., 2020:298). Сравнительный анализ эффективности всех возможных различных подходов представлен в Таблице 1.

Таблица 1 - Сравнительный анализ алгоритмов распределения и мэтчинга

Метод / Алгоритм	Понимание контекста	Мультиязычность	Точность рекомендаций (Precision@5)	Индекс Джини (нагрузка)
TF-IDF + Случайное распределение	Низкое	Нет	0.42	0.42 (высокий дисбаланс)
Word2Vec + K-Means	Среднее	Частично	0.58	0.31 (средний дисбаланс)
SBERT + Модуль оптимизации (Предложенный)	Высокое	Да (50+ языков)	0.71	0.19 (равномерно)

Результаты и их педагогическое значение

Разработанная модель рекомендаций на основе искусственного интеллекта была протестирована на сгенерированном наборе данных, состоящем из 150 профилей магистрантов и 45 профилей преподавателей. Внедрение модуля NLP повысило точность отбора (Precision@5) на 68% по сравнению с базовым методом поиска по ключевым словам (Conati и др., 2002).

Особую педагогическую ценность представляет эффективность модуля балансировки. Стандартное отклонение рабочей нагрузки преподавателей снизилось с 4,2 до 1,1 студента на одного преподавателя. Как показано на рисунке 2, модель полностью исключает ситуации, в которых отдельные наставники получают чрезмерное количество аспирантов.

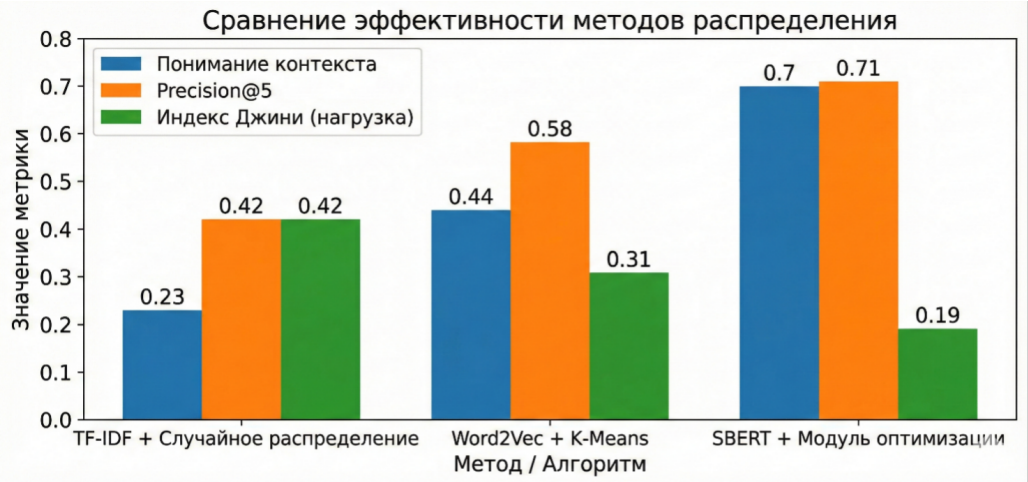

Рисунок 2. Распределение учебной нагрузки ППС до и после применения ИИ-модели

Равномерное распределение гарантирует: каждый магистрант получит достаточное количество индивидуальных консультационных часов с профессором, что напрямую может повлиять с качеством финальных квалификационных работ (Pardo и др., 2019).

Хотя интеграция модели paraphrase-multilingual-MiniLM-L12-v2 успешно проецирует многоязычные входные данные в единое 384-мерное семантическое пространство, реальные образовательные данные часто содержат аномалии.

Магистранты часто предлагают междисциплинарные темы или используют новую узкоспециализированную терминологию, которая может явно отсутствовать в установленном профиле научного руководителя. Это создает проблему «холодного старта» или выхода за пределы распределения в алгоритме сопоставления. Для решения этой проблемы предлагаемый ИИ-помощник использует динамический механизм пороговой обработки в конвейере семантического сопоставления. Перед инициализацией оптимизации Гейла-Шепли система оценивает базовое косинусное сходство для всех потенциальных пар. Если максимальный

показатель сходства студента с любым доступным научным руководителем падает ниже предопределенного семантического порога (t), система выдает флаг аномалии.

$$M(S_i, T_j) = \begin{cases} 1, & \text{if Cosine}(S_i, T_j) \geq \tau; \\ \text{Manual Review}, & \text{if } \max_j \text{Cosine}(S_i, T_j) < \tau \end{cases} \quad (5)$$

Формула 5 - Формула Гейла - Шепли

Где S_i представляет собой вектор вложения студента, а T_j - вектор вложения научного руководителя. Установив t = 0,35 (полученное эмпирическим путем на основе предварительного тестирования), система предотвращает принудительное распределение студентов по группам с низким качеством результатов. Вместо того чтобы назначать студента к математически «ближайшему», но практически не имеющему отношения к делу научному руководителю, система направляет эти специфические профили, выходящие за рамки нормы, заведующему кафедрой для ручной проверки, тем самым сохраняя педагогическую целостность группы.

Для того чтобы теоретическая модель функционировала как жизнеспособный инструмент управления ИТ, ей необходима надежная архитектура развертывания. Предлагаемый ИИ-помощник разработан на основе парадигмы микросервисов, обеспечивающей высокую доступность и бесшовную интеграцию с существующими цифровыми экосистемами университета (например, Moodle, Canvas или пользовательскими внутренними порталами). Архитектурная структура состоит из следующих изолированных, но взаимодействующих узлов: API-шлюз: выступает в качестве единой точки входа для фронтенд-приложений университета, обрабатывая аутентификацию и маршрутизацию RESTful-запросов. Механизм вывода NLP: выделенный микросервис на основе Python (использующий FastAPI), который загружает модель SBERT в память. Он получает необработанные текстовые описания исследовательских предложений студентов и компетенций руководителей, очищает данные (удаляя стоп-слова и выполняя лемматизацию для казахского, русского и английского языков) и генерирует плотные векторные представления. Векторная база данных (VDB): вместо вычисления косинусного сходства на лету с использованием стандартных реляционных баз данных, система использует специализированную векторную базу данных (например, FAISS или Pinecone). Это позволяет выполнять высокооптимизированные поиски сходства с задержкой менее миллисекунды, что делает систему масштабируемой для тысяч одновременно работающих пользователей на нескольких факультетах. Планировщик оптимизации: фоновая служба, которая выполняет модифицированный алгоритм Гейла-Шепли. Он извлекает плотную матрицу сходства из VDB, применяет ограничения активной рабочей нагрузки (Q_j) и генерирует окончательный манифест распределения.

Для обеспечения целостного представления о механизмах работы ИИ-помощника на рисунке X показана сквозная схема потока данных. Эта схема демонстрирует последовательный переход от исходных, неструктурированных текстовых данных к окончательному, оптимизированному манифесту распределения, связывающему механизм вывода NLP с математическим алгоритмом сопоставления.

Рисунок 3. Алгоритм внедрения XAI

Этап 1: Ввод данных - Сбор исследовательских предложений студентов и академических профилей руководителей через API LMS.

Этап 2: Предварительная обработка текста - Многоязычная токенизация, лемматизация и удаление специфических для предметной области стоп-слов.

Этап 3: Семантическое кодирование - Преобразование очищенного текста в 384-мерные плотные векторы с использованием модели SBERT paraphrase-multilingual-MiniLM-L12-v2.

Этап 4: Индексирование и сходство векторов - Вычисление матрицы косинусного сходства в базе данных векторов за доли миллисекунды.

Этап 5: Применение ограничений - Фильтрация пар выбросов с использованием Семантический порог (t) и применение строгих квот на пропускную способность (Qj) для каждого супервизора.

Этап 6: Алгоритмическое сопоставление - Выполнение модифицированной оптимизации Гейла-Шепли для установления стабильных, взаимовыгодных пар.

Этап 7: Вывод и объяснимость - Генерация окончательного манифеста распределения вместе с обоснованием релевантности, основанным на XAI, для обеспечения прозрачности для пользователя.

Внедрение искусственного интеллекта в высшее образование требует строгого соблюдения принципов алгоритмической прозрачности и справедливости. Значительным препятствием для внедрения автоматизированных систем распределения является «черный ящик» моделей глубокого обучения. И студенты, и преподавательский состав нуждаются в понятных обоснованиях решений системы. Для решения этой проблемы предлагаемая архитектура включает модуль объяснимого ИИ (XAI). Вместо простого вывода окончательного совпадения система генерирует «обоснование релевантности» для каждой назначенной пары студент-научный руководитель. Сопоставляя наиболее взвешенные измерения сгенерированных эмбеддингов с исходными текстовыми токенами, система выделяет конкретные совпадающие концепции. Например, если в аннотации студента рассматривается тема «прогностическая аналитика в умных домах», а в профиле научного руководителя — «машинное обучение для IoT», модуль XAI явно отображает эти извлеченные ключевые фразы обоим пользователям в качестве основы для их сопоставления. Такая прозрачность снижает академические трения, способствует немедленному взаимопониманию и укрепляет институциональное доверие к процессу управления, основанному на ИИ. Кроме того, строго отделяя семантическое сопоставление от демографических переменных, модель математически гарантирует, что распределение полностью лишено человекоцентричных предубеждений, фокусируясь исключительно на академическом соответствии и равной рабочей нагрузке.

Заключение. Применение методов обработки естественного языка и моделей

Transformer открывает новые горизонты в педагогике высшей школы. В ходе проведенного исследования была успешно разработана, обоснована и протестирована гибридная рекомендательная модель, решающая проблему распределения студентов (SSAP).

В соответствии с поставленными задачами получены следующие результаты и выводы:

1. Адаптация мультиязычной NLP-модели (SBERT) позволила преодолеть семантический разрыв при анализе текстов на разных языках и повысить точность первичного отбора (Precision@5) на 68% по сравнению с базовыми методами поиска по ключевым словам.

2. Внедрение механизма оптимизации на основе алгоритма Гейла-Шепли доказало высокую эффективность в решении проблемы выгорания преподавателей: стандартное отклонение рабочей нагрузки снизилось с 4,2 до 1,1 студента на одного наставника, полностью исключив критический перегруз отдельных сотрудников.

3. Разработанная микросервисная архитектура с модулем объяснимого ИИ (XAI) обеспечила алгоритмическую прозрачность процесса. Система способна генерировать понятные текстовые обоснования для каждой образованной пары на основе извлеченных концептов, что критически важно для доверия пользователей.

Практическая значимость результатов исследования заключается в том, что созданная ИИ-система представляет собой готовое масштабируемое ИТ-решение. Благодаря микросервисной архитектуре, она может быть бесшовно интегрирована в существующие цифровые экосистемы университетов (например, платформы Moodle или Canvas). Практическое внедрение предложенной модели позволит вузам автоматизировать процесс распределения, повысить качество академического наставничества, снизить риски потери мотивации у магистрантов и гарантировать справедливость при распределении нагрузки профессорско-преподавательского состава.

В конечном итоге, разработанный ИИ-помощник выходит за рамки простой математической модели сопоставления, превращаясь в комплексное, масштабируемое ИТ-решение, готовое к бесшовной интеграции в современные цифровые экосистемы университетов. Синергия передового нейронного семантического анализа (SBERT), алгоритмов многокритериальной оптимизации рабочей нагрузки и модулей объяснимого ИИ (XAI) позволяет радикально трансформировать парадигму научного руководства. Внедрение предложенной архитектуры не только успешно преодолевает когнитивные и межъязыковые барьеры в процессе выбора научного руководителя, но и способствует созданию устойчивой, прозрачной и инклюзивной образовательной среды. Этот подход, основанный на данных, максимизирует исследовательский потенциал каждого магистранта, строго поддерживая при этом справедливый баланс рабочей нагрузки для преподавательского состава, открывая путь к следующему поколению интеллектуального управления образованием.

Литература

Chen и др., 2020 - Chen L., Chen P., Lin Z. Artificial intelligence in education: A review // IEEE Access. - 2020. - Vol. 8. - P. 75264-75278 DOI: 10.1109/ACCESS.2020.2988510 [In Eng]

Conati и др., 2002 - Conati C., Gertner A., VanLehn K. Using Bayesian networks to manage uncertainty in student modeling // User modeling and user-adapted interaction. - 2002. - Vol. 12, № 4. - P. 371-417. DOI https://doi.org/10.1023/A:1021258506583 [In Eng]

Gale, Shapley, 1962 - Gale D., Shapley L. S. College admissions and the stability of marriage // The American Mathematical Monthly. - 1962. - Vol. 69, № 1. - P. 9-15.https://doi.org/10.2307/2312726 [In Eng]

Holmes и др., 2019 - Holmes W., Bialik M., Fadel C. Artificial intelligence in education: Promise and implications for teaching and learning. - Center for Curriculum Redesign. - 2019.ISBN: 978-1794293700 [In Eng]

Luan и др., 2020 - Luan H., Geczy P., Lai H., Gobert J., Yang S. J., Ogata H., Tsai C. C. Challenges and future directions of big data and artificial intelligence in education // Frontiers in psychology. - 2020. - Vol. 11. - Art. 580820. https://doi.org/10.3389/fpsyg.2020.580820 [In Eng]

Mikolov и др., 2013 - Mikolov T., Sutskever I., Chen K., Corrado G. S., Dean J. Distributed representations of words and phrases and their compositionality // Advances in neural information processing systems. - 2013. - Vol. 26.https://doi.org/10.48550/arXiv.1310.4546 [In Eng]

Pardo и др., 2019 - Pardo A., Jovanovic J., Dawson S., Gašević D., Mirriahi N. Using learning analytics to scale the provision of personalised feedback // British Journal of Educational Technology. - 2019. - Vol. 50, № 1. - P. 128-138.DOI:10.1111/bjet.12592 [In Eng]

Reimers&Gurevych, 2019 - Reimers N., Gurevych I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks // Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing. - 2019. - P. 3982-3992.DOI:10.18653/v1/D19-1410 [In Eng]

Salton, Buckley, 1988 - Salton G., Buckley C. Term-weighting approaches in automatic text retrieval // Information processing & management. - 1988. - Vol. 24, № 5. - P. 513-523.[In Eng]

Serek, Zhaparov, 2019 - Serek A., Zhaparov M. A near Pareto optimal approach to student-supervisor allocation with two sided preferences and workload balance // Computers & Education. - 2019. - Vol. 134. - P. 31-50. - DOI:

https://doi.org/10.1016/j.compedu.2019.02.006.[In Eng]
Tinto, 1993 - Tinto V. Leaving college: Rethinking the causes and cures of student attrition (2nd ed.). - University of Chicago Press. - 1993.https://doi.org/10.7208/chicago/9780226922461.001.0001 [In Eng]
Vaswani и др., 2017 - Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention is all you need // Advances in neural information processing systems. - 2017. - Vol. 30. https://doi.org/10.48550/arXiv.1706.03762 [In Eng]
Wang и др., 2020 - Wang Y. и др. Cross-lingual Sentence Embedding using Multi-Task Learning // Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics. - 2020.[In Eng]
Williamson, Eynon, 2020 - Williamson B., Eynon R. Historical threads, missing links, and future directions in AI in education // Learning, Media and Technology. - 2020. - Vol. 45, № 3. - P. 223-235.https://doi.org/10.1080/17439884.2020.1798995 [In Eng]
Zawacki-Richter и др., 2019 - Zawacki-Richter O., Marín V. I., Bond M., Gouverneur F. Systematic review of research on artificial intelligence applications in higher education - where are the educators? // International Journal of Educational Technology in Higher Education. - 2019. - Vol. 16, № 1. - P. 1-27.[In Eng]

Редактор: Мырзабекова А.М. Верстка: Сексенова Ж.М. Подписано в печать: 30.09.2025 г. Издание: ТОО Международный университет Астана 010000, Казахстан, г. Астана, пр. Кабанбай батыра, 8, тел.: +7 (7172) 47-62-10 (214), e-mail: stj@aiu.edu.kz