ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ПРЕЗИДЕНТІНІҢ ЖАНЫНДАҒЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ

№2 (апрель-июнь)
2025 год

НАУКА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

Научный журнал НАН РК при Президенте РК

ҚР Президентінің жанындағы ҚР ҰҒА
«Интеллектуалды жүйелер ғылымы» ғылыми журналы

Scientific Journal of the NAS RK under the President of the RK
«Science of intelligent systems»

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПРЕЗИДЕНТІНІҢ ЖАНЫНДАҒЫ ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

№2 (апрель-июнь) 2025 год

«Интеллектуалды жүйелер ғылымы» ғылыми журнал

Научный журнал «Наука интеллектуальных систем»

Scientific Journal «Science of intelligent systems»

УЧРЕДИТЕЛЬ:
Национальная академия наук Республики Казахстан при Президенте Республики Казахстан
Издается с 2025 года
Выходит 4 раза в год, ежеквартально
Свидетельство о постановке на учет периодического печатного издания, информационного агентства и сетевого издания № KZ90VPY00113742, выданное Министерством культуры и информации от 03.03.2025 г.
Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28
Тел. канцелярии: +7 (727) 308 08 17
Тел. отв. редактора: +7 705 955 19 52
Сайт журнала: https://kazscience.kz

FOUNDER:
National Academy of Sciences of the Republic of Kazakhstan under the President of the Republic of Kazakhstan
Published since 2025 year.
Issued 4 times a year, quarterly
Certificate of registration of a periodical, news agency and online publication No. KZ90VPY00113742 issued by the Ministry of Culture and Information dated 03.03.2025.
Address of editorial offices: 050010, Almaty city, Shevchenko str., 28
Office phone number: +7 (727) 308 08 17
Tel. of the responsible editor: +7 705 988 19 52
Website: https://kazscience.kz

СОДЕРЖАНИЕ

CONTENT

Ахылбек Куришбаев,
академик,
Президент Национальной
академии наук при Президенте РК

ИИ управляет природными рисками

При Академии наук создана лаборатория пространственно-временного искусственного интеллекта

Глава государства Касым-Жомарт Токаев постоянно подчеркивает исключительную важность развития науки, укрепления международных научных связей и ставит задачу превратить Казахстан в страну высокотехнологичной экономики, основанной на современных знаниях и инновациях. Выполнение данного поручения на сегодняшний день является одним из главных приоритетов в деятельности Национальной академии наук при Президенте РК.

В настоящее время к числу принятых конкретных мер можно отнести создание в феврале 2025 года на базе Национальной академии наук Международного научного центра с объединенной лабораторией пространственно-временного искусственного интеллекта и устойчивого развития совместно с Чжэцзянским технологическим университетом при участии академиков Китайской академии наук и ведущих высокотехнологичных компаний КНР. Такой международный научный центр с современной лабораторией в Казахстане создан впервые, и объем инвестиций в данный проект составит 1 млрд юаней (около 70 млрд тенге).

Лаборатория данного центра представляет собой интегрированную платформу для обработки пространственно-временных данных, анализа и визуализации. Она включает в себя мощные серверы с высокопроизводительными процессорами, ускорительными картами для машинного обучения, высокоскоростные накопители для хранения больших объемов информации и специализированную систему отображения. Кроме того, лаборатория имеет мобильный комплекс SIGMA на базе трехосного тяжелого внедорожника, предназначенный для работы в экстремальных условиях и анализа пространственно-временных данных.

Основной задачей данного центра является создание научно-технической платформы для интегрированного мониторинга и прогнозирования природных явлений, управления ресурсами и содействия устойчивому развитию региона. В рамках данной задачи будут проведены научные исследования в области искусственного интеллекта, цифровых технологий, передовых инженерных решений и устойчивого развития, будут реализовываться инновационные проекты в области облачных вычислений в спутниковых сетях, интеллектуальных технологий предотвращения стихийных бедствий, интеллектуальной энергетики, сельского хозяйства, экологической защиты и логистики. При этом особое внимание будет уделено разработке решений для прогнозирования экологических рисков, устойчивого управления ресурсами и сохранения биоразнообразия через создание казахстанской интеллектуальной системы DeepBas на основе Deepseek.

Проект в перспективе нацелен на формирование научного хаба с охватом всех стран Центральной Азии, а в последующем – Ирана, Монголии и Афганистана. На этом этапе данная лаборатория будет способна решать широкий круг таких стратегических за-

дач в Центрально-Азиатском регионе, как моделирование и прогнозирование стихийных бедствий, включая наводнения, засухи, землетрясения, лесные пожары, разработка системы раннего предупреждения и превентивных мер, направленных на смягчение их последствий.

Кроме того, лаборатория будет заниматься разработкой интеллектуальных энергетических решений для оптимизации распределения энергии через «умные» сети, анализа потребления и прогнозирования спроса, что приводит к снижению энергопотребления и потерь. Наряду с этим она с использованием искусственного интеллекта будет решать проблемы оптимизации транспортных систем и городской инфраструктуры, управления дорожным движением в городах, оптимизации потоков, сокращения пробок и снижения выбросов, включая планирование маршрутов экстренных служб во время ЧС.

Важной составной частью деятельности центра и ее лаборатории станет развитие интеллектуального сельского хозяйства, использование дронов и спутниковых снимков для мониторинга здоровья урожая, состояния почвы, обнаружения вредителей и болезней, прогнозирование урожайности, оптимизация использования воды и удобрений, что напрямую способствует региональной продовольственной безопасности и устойчивости развития.

Также в их функционал входит решение вопросов сохранения биоразнообразия, создания системы экологического мониторинга и прогнозирования на базе искусственного интеллекта, геоинформационных систем и дистанционного зондирования для отслеживания состояния экосистем, формирования единого цифрового кадастра флоры и фауны региона, сопряженного с международными платформами. Немаловажной стороной их деятельности станет решение проблемы устойчивого развития сельских территорий путем разработки долгосрочных сценариев с учетом климатических изменений и роста ресурсной нагрузки.

Такая многосекторальная направленность центра и ее лаборатории создает уникальную возможность научным организациям региона сосредоточить свои усилия не только на решении общих задач, взаимно обогащая друг друга новыми научными знаниями и компетенциями, но и на подготовке научных кадров новой формации для каждой страны.

Официальное открытие центра планируется в рамках повестки предстоящего саммита «Китай – Центральная Азия», что подчеркивает его высокий политический статус и значимость для региональной интеграции.

(Казахстанская правда, № от 12.06.2025 г.)

UDC 004.85

Kumalakov B.*, Abdibek B., Mukhanov D.
Astana IT University, Astana, Kazakhstan
E-mail: b.kumalakov@gmail.com

ABOUT A FILE SORTING PROBLEM USING MACHINE LEARNING

Kumalakov B.A., PhD, ssociate professor at the School of Artificial Intelligence and Data Science, Astana IT University. E-mail: b.kumalakov@gmail.com, ORCID: https://orcid.org/0000-0003-1476-9542;
Abdibek B., Junior researcher. E-mail: ailpokabdibek@gmail.com, ORCID: https://orcid.org/0009-0006-7874-9371;
Mukhanov D., Junior researcher. E-mail: danilmukhanov21@gmail.com, ORCID: https://orcid.org/0009-0003-0753-6553.

File sorting is essential in a wide range of data management areas, including forensic sciences. In some cases, forensics specialists face situations when file extensions are absent or intentionally altered for some purposes. Nevertheless, such files might contain valuable information for the investigation at hand. This paper reports on an attempt to develop a deep learning system to sort files by categories using bit representation of file contents, unlike traditional file extension, header or metadata-based solutions. Training, validation and test datasets included 100 files of various document, media and audio formats. Overall, the system demonstrates accuracy rate that exceeds 95%, with highest inaccuracy when trying to classify files with similar contents (for instance, different video file types, etc.). Nonetheless, the solution serves a solid proof of the concept and a foundation for future research in this direction.

Keywords: machine learning, deep learning, file sorting.

Құмалақов Б.А.*, Әбдібек Б., Мұханов Д.
Astana IT University, Астана, Қазақстан
**E-mail: b.kumalakov@gmail.com*

МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНА ОТЫРЫП ФАЙЛДАРДЫ СҰРЫПТАУ ЕСЕБІ ТУРАЛЫ

Құмалақов Б.А., PhD, Жасанды интеллект және ерек туралы ғылым мектебінің қауымдастырылған профессоры, Astana IT University. E-mail: b.kumalakov@gmail.com, ORCID: https://orcid.org/0000-0003-1476-9542;
Абдибек Б., кіші ғылыми қызметкер. E-mail: ailpokabdibek@gmail.com, ORCID: https://orcid.org/0009-0006-7874-9371;
Муханов Д., кіші ғылыми қызметкер. E-mail: danilmukhanov21@gmail.com, ORCID: https://orcid.org/0009-0003-0753-6553.

Файлдарды сұрыптау деректерді басқарудың көптеген салаларында, соның ішінде цифрлық криминалистикада кеңінен пайдаланады. Кейбір жағдайларда цифрлық криминалист кейбір мақсаттар үшін файл кеңейтімдері жоқ немесе әдейі өзгертілген жағдайларға тап болады. Дегенмен, мұндай файлдарда тергеу үшін құнды ақпарат болуы мүмкін. Бұл мақалада дәстүрлі файл кеңейтімі, тақырып немесе метадеректер негізінде жұмыс істейтін шешімдерден өзгеше, файл мазмұнының биттік көрінісін пайдаланып файлдарды санаттар бойынша сұрыптау үшін терең оқыту жүйесін әзірлеу әрекеті туралы хабарлайды. Тренинг, валидация және сынақ деректер жинақтары әртүрлі құжат, медиа және аудио форматтағы 100 файлды қамтыды. Жалпы алғанда, жүйе файлдарды 95% дәлдікпен анықтайды, бірақ мазмұны ұқсас файлдарды (мысалы, әртүрлі бейнефайл түрлері және т.б.) анықтағанда қате жіберуі мүмкін. Дегенмен, шешім тұжырымдаманың берік дәлелі және осы бағыттағы болашақ зерттеулер үшін негіз болады.

Түйін сөздер: машиналық оқыту, терең оқыту, файлдарды сұрыптау.

Кумалаков Б.*, Абдибек Б., Муханов Д.
Astana IT University, Астана, Казахстан
**E-mail: b.kumalakov@gmail.com*

ОБ ОДНОЙ ЗАДАЧЕ СОРТИРОВКИ ФАЙЛОВ С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ

Кумалаков Б.А., PhD, ассоциированный профессор Школы искусственного интеллекта и Науки о данных Astana IT University. E-mail: b.kumalakov@gmail.com, ORCID: https://orcid.org/0000-0003-1476-9542;
Абдибек Б., младший научный сотрудник. E-mail: ailpokabdibek@gmail.com, ORCID: https://orcid.org/0009-0006-7874-9371;
Муханов Д., младший научный сотрудник. E-mail: danilmukhanov21@gmail.com, ORCID: https://orcid.org/0009-0003-0753-6553.

Сортировка файлов играет важную роль в широком спектре областей управления данными, включая цифровую криминалистику. В некоторых случаях специалисты по цифровой криминалистике сталкиваются с ситуациями, когда расширения файлов отсутствуют или намеренно изменены для каких-либо целей. Тем не менее, такие файлы могут содержать ценную информацию для проводимого расследования. В данной статье представлена попытка разработки системы глубокого обучения для сортировки файлов по категориям с использованием битового представления их содержимого, в отличие от традиционных решений, основанных на расширении файлов, заголовках или метаданных. Обучающие, валидационные и тестовые наборы данных включали 100 файлов различных форматов документов, медиа- и аудиофайлов. В целом система демонстрирует точность, превышающую 95%, с наибольшей погрешностью при классификации файлов со схожим содержимым (например, разных типов видеофайлов и т. д.). Тем не менее, решение служит убедительным подтверждением концепции и основой для будущих разработок в этом направлении.

Ключевые слова: машинное обучение, глубокое обучение, сортировка файлов.

INTRODUCTION

File sorting is essential in a wide range of data management areas [1, 2], including forensic sciences. Of a special interest are cases when experts must deal with damaged files, such as files recovered from damaged memory partitions or – in fact - purposely altered for any reason. Hence, traditional file classification techniques, such as file extension- or header-based approaches, become invalid and use of deep learning systems to examine file fragments - in its binary representation - becomes promising enhancement.

Over past years numerous industrially applicable open-source systems made their way to the market. Namely TrID, DROID, Siegfried, Magika, FiFTy, File Fragment Classification and the "Binary Classification of CSV Files" project gained visibility.

Magika is a software product developed by Google, based on deep neural networks, that classifies over 100 file types with over 99% accuracy [3]. The solution provides fast processing regardless of file size and is available through both a Python command-line interface and an API. Advantages include high classification accuracy, support for a wide range of file types, and ease of integration via the API. However, using Magika requires significant computing resources, and customizing the tool for specific tasks can be complex. FiFTy is a tool that uses neural networks to classify file fragments and supports various scenarios and block sizes, including 512 and 4096 bytes [4]. It supports 75 file types, including archives, documents, media formats, and executable files. FiFTy's advantages include its ability to handle corrupted data and the ability to train on new data. Its disadvantages include the need for pre-training and model training. FiFTy is particularly effective when tailored to specific tasks.

The File Fragment Classification project implements support vector matching (SVM) and k-nearest neighbour (KNN) to classify 13 file types [5, 6, 7, 8]. The solution demonstrates high accuracy on real-world data, making it useful for digital forensics. Advantages also include high accuracy on a limited set of file types

and relatively low computational requirements. However, the project is limited in the number of file types it supports and is less effective when working with fragmented or corrupted data. This solution is suitable for working with small datasets, especially in the presence of partial corruption.

Binary Classification of CSV Files uses various machine learning models for binary classification of CSV files [9], which can be adapted to classify other file types by modifying the dataset and tailoring an algorithm. Key advantages include high accuracy in specific tasks and flexibility in model selection. Limitations include the need to adapt to other file types and a narrow focus on binary classification. This solution can be useful for automating data sorting based on its structural characteristics.

At this stage we can generalise that machine learning enabled tools either rely on availability of an external dependence (such as Goodle database or a library of signatures) or have extremely limited number of file types it can handle. This fact serves as a basis to develop a bespoke solution for forensic file sorting needs this research pursues.

Remainder of this paper reports on a file sorting application which utilises traditional classification technique with an optional deep learning component and its test results. The machine learning based component is a three-layer network trained to recognize 19 (nineteen) file extensions. The system demonstrated 95% classification efficiency with a training time of 6.5 minutes using a graphics processing unit and 30 minutes with central processing unit only. The traditional file classification algorithms include “extensions”, “header” and “signatures” based sorting.

MATERIALS AND METHODS

The workflow is to unpack files stored in a digital archive into target folders according to their type and use. Specifically, category folders are: “media” (with graphics, video, audio and animation sub-folders), “configuration files”, “documents”, “no match” and “others”. Some files are intentionally saved with false extensions (or without one) and some are with stripped metadata.

Schematically algorithm is presented in figure 1. When launched, the program reads the archive and extracts files one by one. If a file is an archive itself, it recursively processes it and carries on till the root archive files remain. In other cases, it tries to classify the file using its “extension”, “header” and/or “signature” in the named order. After that the same file is classified using machine learning and one of three scenarios happen. First, if both methods produce the same outcome, the file is saved into corresponding folder (such as media, document, etc.). Second, if both methods fail to identify file type, it is saved into the “others” folder. Third, if two steps classify the file differently or one of them fails to do so, it is saved to the “no match” folder. Such a naïve approach is designed not to distract the evaluator from machine learning component efficiency and keep experiment setting as simple as possible.

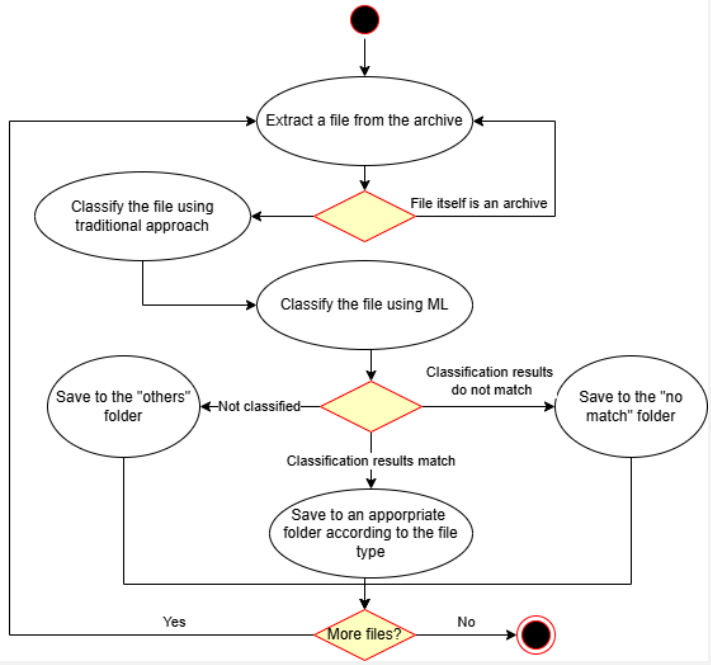

Figure 1 – Schematic representation of the sorting algorithms

Experiment dataset consists of 100 files with the following extensions: doc, docx, html, pdf, pptx, txt, xls, xlsx, xml, gif, jpeg, jpg, png, mov, mp4, audioaac, mp3, and opus. They were proportionally divided into three sets: training (64%), validation (16%), and testing (20%).

For each file, the first 2048 bytes were extracted, of which the first 256 bytes were removed. The remaining 1792 bytes were used as features added to the "content" column. To run the model, binary data was converted into strings. To balance the data, 100 files of each type were randomly selected to avoid imbalance and inaccuracies in the classification of underrepresented file types.

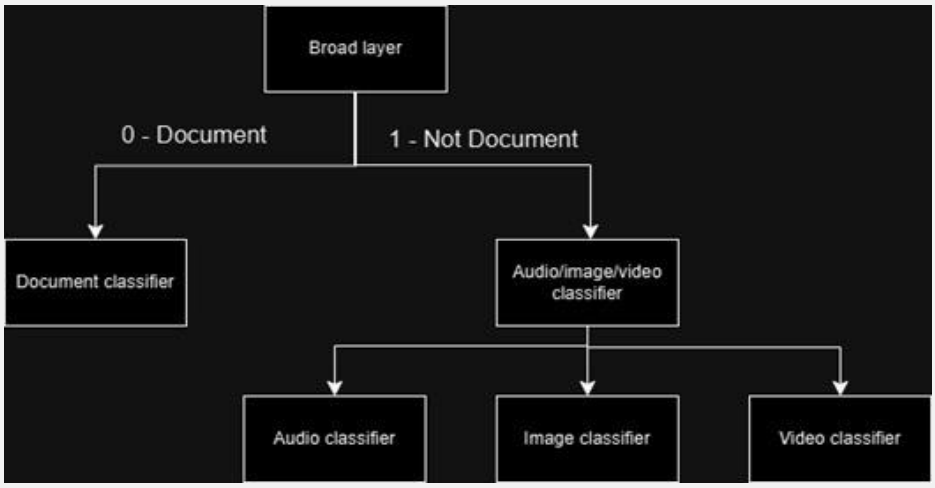

Figure 2 – Deep learning structure

Figure 2 visualises the hierarchical structure of the deep learning system. Every rectangle represents a classifier layer. Various algorithms were investigated, including random forest, support vector machines, XGBoost, and neural networks. The neural network was trained using various hidden layer configurations (convolutional, pooling, and dense) and the number of neurons (from 32 to 256 in each layer). Additionally, the XGBoost classifier was trained on n-gram vectors. Early stopping, dropout, and layer normalization were used to reduce overfitting.

Evaluation metrics included precision and recall, where:

- Precision: the proportion of relevant instances among those retrieved.
- Recall: the proportion of relevant instances that were retrieved.

These metrics were saved in the classification report (see figure 3). The performance was evaluated by file type: precision was analysed for each type to identify anomalies.

```
Audio model classification report:
{'.aac': 0, '.mp3': 1, '.opus': 2, '.wav': 3}
              precision    recall  f1-score   support

           0       1.00      1.00      1.00        21
           1       1.00      0.95      0.97        19
           2       1.00      1.00      1.00        25
           3       0.94      1.00      0.97        15

    accuracy                           0.99        80
   macro avg       0.98      0.99      0.99        80
weighted avg       0.99      0.99      0.99        80
```

Figure 3 – Classification report structure for a single classifier

Forward propagation on the first layer is defined as follows:

$$z^{(l)} = W^{(l)}a^{(l-1)} + b^{l}$$

$$a^{(l)} = f(z^{(l)})$$

where $W^{(l)}$– layer weights matrix, $b^{(l)}$ – displacement vector, $a^{(l-1)}$ – output of the previous layer.

Backward propagation is used to calculate gradients and update weights. Gradients are defined using the chain rule:

$$\frac{\partial L}{\partial W^{(l)}} = \delta^{(l)} \cdot a^{(l-1)}$$

The loss function, in turn, determines the difference between the network predictions and the true values:

$$L = -\frac{1}{m}\sum_{i=1}^{m}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)]$$

where m is the number of examples, y_i is the true label, $\hat{y}_i$ is the predicted probability.

$$\delta^{(l)} = \frac{\partial L}{\partial z^{(l)}} \cdot f'(z^{(l)})$$

where $\delta^{(l)}$ — error gradient at the level l.

In turn, the weight update is implemented using the gradient descent method.:

$$W^{(l)} := W^{(l)} - \eta\frac{\partial L}{\partial W^{(l)}}$$

where η is the learning speed.

To implement the algorithm, a convolutional neural network is used, which uses 768 bytes of the input file, totalling 1024 bytes of the input file for processing. The file extension is ignored when reading at the code logic level. The word length of 768 was chosen because a significant proportion of text files (.txt) and animations (.gif) are small, and using longer words would capture part of the file footer.

RESULTS AND DISCUSSION

Deep learning system performance results are presented in figures 4 and 5.

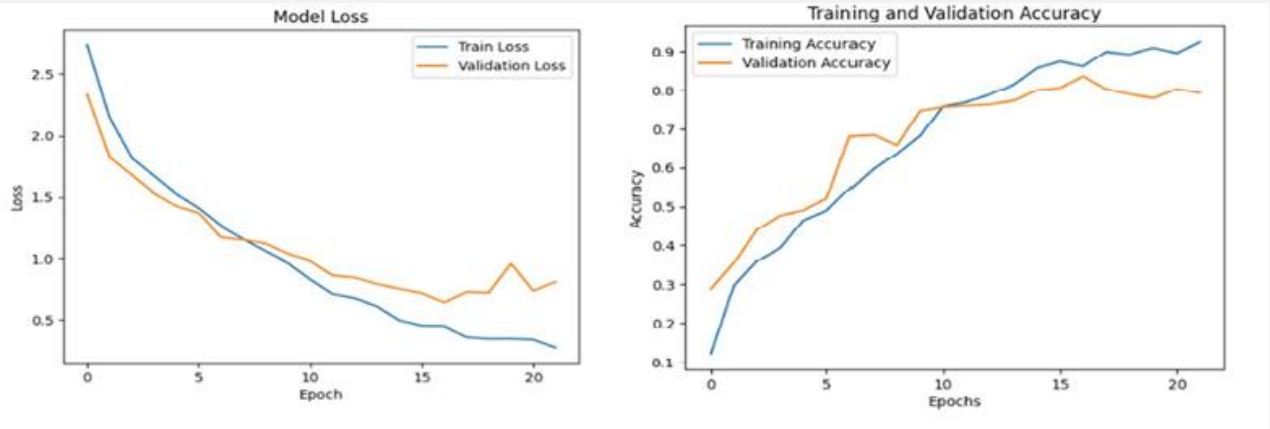

Figure 4 – Model training and validation accuracy

File recognition quality for general categories exceeds 95%. However, test results also indicate that the neural network has difficulty recognizing files with similar content (e.g., png, jpeg, and jpg; as well as audio

files (mp4 and mov). This might be fixed by dynamically increasing the number of input bytes fed to the model for certain file types.

```
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 249ms/step - accuracy: 0.6041 - loss: 1.6449
Test accuracy for .aac: 0.6299999952316284
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 256ms/step - accuracy: 0.9046 - loss: 0.4458
Test accuracy for .doc: 0.9100000262260437
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 257ms/step - accuracy: 0.9786 - loss: 0.0629
Test accuracy for .docx: 0.9700000286102295
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 253ms/step - accuracy: 0.1579 - loss: 3.9718
Test accuracy for .gif: 0.15000000596046448
4/4 ━━━━━━━━━━━━━━━━━━━━ 2s 404ms/step - accuracy: 0.9109 - loss: 0.2106
Test accuracy for .html: 0.9100000262260437
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 249ms/step - accuracy: 0.0554 - loss: 6.0902
Test accuracy for .jpeg: 0.05000000074505806
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 253ms/step - accuracy: 0.5771 - loss: 2.7527
Test accuracy for .jpg: 0.5600000023841858
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 256ms/step - accuracy: 0.1873 - loss: 4.7060
Test accuracy for .mov: 0.20000000298023224
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 263ms/step - accuracy: 0.4122 - loss: 2.2803
Test accuracy for .mp3: 0.38999998569488525
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 247ms/step - accuracy: 1.0000 - loss: 0.0010
Test accuracy for .mp4: 1.0
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 256ms/step - accuracy: 0.9724 - loss: 0.1014
Test accuracy for .opus: 0.9700000286102295
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 253ms/step - accuracy: 0.6190 - loss: 2.1101
Test accuracy for .pdf: 0.6100000143051147
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 262ms/step - accuracy: 0.1359 - loss: 2.6067
Test accuracy for .png: 0.1599999964237213
4/4 ━━━━━━━━━━━━━━━━━━━━ 2s 408ms/step - accuracy: 0.8341 - loss: 0.7577
Test accuracy for .pptx: 0.8299999833106995
4/4 ━━━━━━━━━━━━━━━━━━━━ 2s 346ms/step - accuracy: 0.9816 - loss: 0.2243
Test accuracy for .txt: 0.9800000190734863
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 259ms/step - accuracy: 0.8892 - loss: 0.4034
Test accuracy for .wav: 0.8999999761581421
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 256ms/step - accuracy: 0.9653 - loss: 0.1291
Test accuracy for .xls: 0.9599999785423279
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 255ms/step - accuracy: 0.9352 - loss: 0.3015
Test accuracy for .xlsx: 0.949999988079071
4/4 ━━━━━━━━━━━━━━━━━━━━ 1s 260ms/step - accuracy: 0.9630 - loss: 0.0753
Test accuracy for .xml: 0.9700000286102295
```

Figure 6 – Classification accuracy by file extension

The training was also run using central processing unit only and a graphical processing unit enabled (GPU) modes. When using GPU training took on average 6.5 minutes, while in a CPU only mode it took 30 minutes to reach the same result.

CONCLUSION

Paper presented a hybrid file classification and sorting application that combines traditional algorithms and machine learning techniques to effectively address data management issues for forensics needs. The proposed multi-level classification involves n-gram tokenization, and convolutional neural networks, and achieved classification accuracy exceeding 95% for provided file types, despite the challenges associated with similarity. The use of GPU acceleration significantly reduced training time, making the method scalable and suitable for working with large volumes of data. However, limitations related to the recognition of rare or corrupted file types remain, requiring further research. Future work will focus on improving the model's adaptability, expanding its capabilities to work with more complex datasets, and integrating new technologies to improve accuracy and performance.

Author contributions

Kumalakov B. – principal investigator, manuscript author, solution design, model tuning, assessment design.

Abdibek B. – data preparation, machine learning model implementation and training, programming, building graphs.

Mukhanov D. – programming, performing tests, building graphs.

Information about financing

This study was carried out with the financial support of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan under Agreement No. 388/PTF-24-26 dated October 1, 2024, under the scientific research project IRN BR24992852 "Development of intelligent models and methods of the Smart City digital ecosystem for sustainable development of the city and improving the quality of life of citizens".

REFERENCES

1. Johnson L.,Williams R. Automation in Data Processing. Journal of Information Systems, 2019. (in English).
2. Smith J. Big Data Management: Strategies and Technologies. International Journal of Data Analysis, 2020. (in English).
3. Google. Magika: Detect File Content Types with Deep Learning. GitHub repository, 2021. URL: https://github.com/google/magika (in English).
4. Mittal G., Korus, P., Memon, N. FiFTy: Large-Scale File Fragment Type Identification Using Convolutional Neural Networks. IEEE Transactions on Information Forensics and Security, 2021, vol. 16, pp. 28-41, DOI: 10.1109/TIFS.2020.3026581. (in English).
5. Cayli M. File Fragment Classification with Machine Learning. GitHub repository, 2017. URL: https://github.com/mervecayli/File_Fragment_Classification (in English).
6. Anil S. Binary Classification of CSV Files using Machine Learning and Deep Learning Models. GitHub repository, 2019. URL: https://github.com/Smitha-anil/Binary_classification (in English).
7. Krasov A.V., Shterenberg S. I., Fakhrutdinov R. M., Ryzhakov D. V., Pestov I. E. Analysis of the information security of an enterprise based on the collection of user data from open resources and monitoring of information resources using machine learning. T-Comm-Telecommunications and Transport, 2018, 12(10), pp. 36-40. DOI: 10.24411/2072-8735-2018-10154. (in Russ.).
8. Matveev A. O., Bystrov A.V., Babaev,V. I., Povarov N. I. Development of software tools to improve the operation of the code auto-completion mechanism using machine learning algorithms in an integrated development environment for the Python language. Bulletin of Novosibirsk State University. Series: Information Technology, 2020, 18(2), pp. 62-75. DOI: 10.25205/1818-7900-2020-18-2-62-75. (in Russ.)
9. Selezneva Ya. M., & Zenkin A.M. Models and methods for ensuring cybersecurity of digital economy systems based on machine learning. In The Almanac of scientific papers of young scientists of ITMO University, 2022, pp. 371-374. URL: https://www.elibrary.ru/item.asp?id=49550578. Accessed: 15.01.2025. (in Russ.)
10. Zhang H., Liang H., Ni T., Huang L., Yang J. (2021). Research on multi-object sorting system based on deep learning. Sensors, 2021, 21(18), 6238. https://doi.org/10.3390/s21186238 (in English).

МРНТИ 28.23.15
УДК 004.056.5

С. Адилжанова, А. Ануарбек*
Казахский национальный университет имени аль – Фараби, 71, проспект аль-Фараби, 050040, Алматы, Казахстан
*E-mail: aidosik165@gmail.com

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В ОБЛАЧНЫХ СРЕДАХ

Адилжанова Салтанат Альмуханбетовна, PhD, и.о. доцента кафедры «Кибербезопасность и криптология» факультета «Информационных технологий». E-mail:asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X
Ануарбек Айдос Маратұлы, магистрант 1 курса; E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Управление информационными рисками является ключевым элементом обеспечения безопасности современных организаций, особенно в условиях роста киберугроз и широкого внедрения облачных технологий. В настоящей работе рассматривается актуальная проблема повышения эффективности управления информационными рисками за счет интеграции организационных и технических подходов, а также автоматизации процессов их оценки и анализа. Значимость исследования обусловлена увеличением сложности и разнообразия современных киберугроз, требующих новых решений для их эффективного предотвращения. Для решения поставленной задачи использованы методологии OCTAVE и NIST SP 800-30, позволяющие комплексно подходить к управлению информационными рисками, сочетая организационные и технические аспекты. В рамках исследования проведена автоматизация процесса оценки рисков с помощью разработанных автором Python-скриптов, предназначенных для выявления сетевых уязвимостей и анализа конфигураций облачных систем. Результаты работы демонстрируют преимущества комбинированного подхода к управлению рисками и подтверждают эффективность автоматизации для повышения оперативности и точности анализа. Установлено, что модель Shared Responsibility Model требует уточнения границ ответственности сторон в облачных средах. Также подтверждается перспектива применения технологий искусственного интеллекта и машинного обучения для повышения точности прогнозирования угроз информационной безопасности. Использование этих технологий позволяет анализировать большие объемы данных и оперативно выявлять потенциальные угрозы, что значительно усиливает возможности прогнозирования и реагирования на инциденты. Полученные результаты имеют практическую значимость и могут быть использованы организациями при разработке и совершенствовании политики информационной безопасности, а также служат основой для дальнейших исследований по интеграции передовых технологий в системы управления рисками.

Ключевые слова: информационная безопасность, управление рисками, облачные технологии, политика безопасности, искусственный интеллект, машинное обучение, автоматизация аудита и оценки рисков.

С. Адилжанова, А. Ануарбек*
Әл-Фараби атындағы Қазақ ұлттық университеті, 71, әл-Фараби даңғылы, Алматы 050040, Қазақстан
*E-mail: aidosik165@gmail.com

БҰЛТТЫҚ ЖҮЙЕЛЕРДЕ АҚПАРАТТЫҚ ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫ АВТОМАТТАНДЫРУ

Адилжанова Салтанат Альмуханбетовна, PhD, "Ақпараттық технологиялар" факультетінің "киберқауіпсіздік және криптология" кафедрасының доцентінің м. а. E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X
Ануарбек Айдос Маратұлы – 1 курс магистранты. E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Ақпараттық тәуекелдерді басқару қазіргі заманғы ұйымдардың қауіпсіздігін қамтамасыз етудің негізгі элементі болып табылады, әсіресе киберқауіптердің өсуі және бұлтты технологияларды кеңінен енгізу жағдайында. Бұл жұмыста ұйымдастырушылық және техникалық тәсілдерді интеграциялау, сондай-ақ тәуекелдерді бағалау және талдау процестерін автоматтандыру арқылы ақпараттық тәуекелдерді басқарудың тиімділігін арттырудың өзекті мәселесі қарастырылады. Зерттеудің маңыздылығы заманауи киберқауіптердің күрделілігі мен әртүрлілігінің артуына байланысты, оларды тиімді болдырмау үшін жаңа шешімдерді қажет етеді. Мәселені шешу үшін ақпараттық тәуекелдерді басқаруға жан-жақты тәсіл ұсынатын, ұйымдастырушылық және техникалық аспектілерді біріктіретін OCTAVE және NIST SP 800-30 әдістемелері қолданылды. Зерттеу барысында желілік осалдықтарды анықтау және бұлттық жүйелер конфигурацияларын талдау үшін автор әзірлеген Python-скрипттер арқылы тәуекелдерді бағалау процесі автоматтандырылды. Жұмыс нәтижелері тәуекелдерді басқарудағы біріктірілген тәсілдің артықшылықтарын көрсетеді және талдаудың жеделдігі мен дәлдігін арттыруда автоматтандырудың тиімділігін растайды. Shared Responsibility Model моделі бұлттық ортада тараптардың жауапкершілік шекараларын нақтылауды қажет ететіндігі анықталды. Сонымен қатар, ақпараттық қауіпсіздік қатерлерін болжау дәлдігін арттыру үшін жасанды интеллект пен машиналық оқыту технологияларын қолданудың перспективасы расталды. Бұл технологияларды пайдалану үлкен көлемдегі деректерді талдауға және ықтимал қауіптерді жедел анықтауға мүмкіндік береді, бұл оқиғаларды болжау және оларға жауап беру мүмкіндіктерін айтарлықтай күшейтеді. Алынған нәтижелер практикалық мәнге ие және ұйымдар ақпараттық қауіпсіздік саясатын әзірлеу және жетілдіру кезінде қолдана алады, сондай-ақ озық технологияларды тәуекелдерді басқару жүйелеріне интеграциялау саласындағы одан әрі зерттеулерге негіз болып қызмет етеді.

Түйін сөздер: ақпараттық қауіпсіздік, тәуекелдерді басқару, бұлттық технологиялар, қауіпсіздік саясаты, жасанды интеллект, машиналық оқыту, аудит пен тәуекелдерді бағалауды автоматтандыру.

S. Adilzhanova, A. Anuarbek*
Al-Farabi Kazakh National University, 71, Al-Farabi Avenue, Almaty 050040, Kazakhstan
*E-mail: aidosik165@gmail.com

AUTOMATION OF INFORMATION RISK MANAGEMENT IN CLOUD ENVIRONMENTS

Adilzhanova Saltanat, PhD; Acting Associate Professor of the Department of Cybersecurity and Cryptology at the Faculty of Information Technology. E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X;
Anuarbek Aidos, 1 year master's student; E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Information risk management is a key element in ensuring the security of modern organizations, especially in the context of increasing cyber threats and the widespread adoption of cloud technologies. This paper addresses the urgent problem of improving the effectiveness of information risk management through the integration of organizational and technical approaches, as well as the automation of risk assessment and analysis processes. The significance of the study is due to the increasing complexity and diversity of modern cyber threats, which require new solutions for their effective prevention. To address this problem, the OCTAVE and NIST SP 800-30 methodologies were employed, allowing for a comprehensive approach to information risk management by combining organizational and technical aspects. Within the study, the risk assessment process was automated using Python scripts developed by the author, designed to identify network vulnerabilities and analyze cloud system configurations. The results demonstrate the advantages of a combined approach to risk management and confirm the effectiveness of automation in improving the efficiency and accuracy of analysis. It was established that the Shared Responsibility Model requires clarification of the parties' responsibilities in cloud environments. The study also confirms the potential of using artificial intelligence and machine learning technologies to enhance the accuracy of forecasting information security threats. These technologies enable the analysis of large volumes of data and the rapid identification of potential threats, significantly enhancing the ability to predict and respond to incidents. The obtained results have practical significance and can be utilized by organizations in the development and improvement of information security policies, as well as serving as a basis for further research on integrating advanced technologies into risk management systems.

Keywords: Information security, risk management, cloud technologies, security policy, artificial intelligence, machine learning, automation of audit and risk assessment.

ВВЕДЕНИЕ.

Современные организации сталкиваются с растущей сложностью информационной инфраструктуры и увеличением числа киберугроз, что делает управление информационными рисками важнейшим элементом обеспечения безопасности [1], [2]. Особое значение этот вопрос приобретает при внедрении облачных технологий и использовании Интернета вещей (IoT), где ресурсы распределены, а управление сторонними сервисами требует новых подходов к оценке и минимизации рисков [3], [4].

Анализ литературы показывает, что эффективное управление информационными рисками требует сочетания организационных и технических подходов. Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) акцентирует внимание на организационных приоритетах и систематической оценке уязвимостей и активов [5]. В свою очередь, модель NIST SP 800-30 ориентирована на идентификацию угроз, анализ уровня риска и рекомендации по его смягчению [6]. Совмещение этих подходов обеспечивает комплексное управление рисками, особенно в облачных средах, где важна модель разделенной ответственности (Shared Responsibility Model) [7], [8].

Для повышения эффективности процессов оценки и анализа рисков активно применяются инструменты автоматизации. Python-скрипты позволяют проводить аудит сетевых уязвимостей, анализ конфигураций облачных систем и обработку больших данных о

событиях безопасности [9], [10], [11]. Дополнительно методы искусственного интеллекта и машинного обучения обеспечивают прогнозирование потенциальных угроз и выявление аномалий, что повышает оперативность реагирования на инциденты [12], [13], [14].

Современные международные стандарты и фреймворки, такие как ISO/IEC 27005, COBIT и NIST Cybersecurity Framework предоставляют рекомендации по управлению рисками и интеграции этих процессов в корпоративное управление и соответствие нормативным требованиям [15], [16], [17]. В сочетании с автоматизацией и AI/ML технологии, они создают возможности для более точного и быстрого анализа угроз и принятия решений [18], [19].

Таким образом, актуальность работы обусловлена необходимостью интеграции организационных и технических подходов к управлению информационными рисками, автоматизации оценки и анализа, а также использования современных технологий прогнозирования угроз.

Цель статьи – провести обзор существующих методологий и инструментов управления информационными рисками с акцентом на их автоматизацию и применение в облачных средах.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ.

Процессы оценки и управления рисками, интегрирующиеся в существующую ИТ-инфраструктуру организации, являются важным аспектом аудита информационной безопасности [3]. Обычно это включает анализ текущих систем безопасности, аудит уязвимостей и планирование будущих мер.

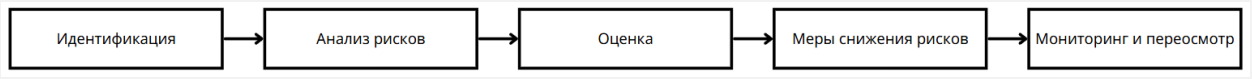

Рис. 1. Процесс управления рисками.

На рисунке 1 представлена блок-схема, иллюстрирующая процесс управления рисками в информационной безопасности. Этот процесс включает несколько ключевых шагов: идентификацию рисков, анализ угроз, разработку плана действий и мониторинг состояния безопасности.

Для крупных организаций с большим количеством информационных систем процесс оценки рисков может быть частично автоматизирован [5]. Например, с помощью скриптов на Python можно проводить аудит сетевых уязвимостей и проверку конфигураций систем.

```python
import matplotlib.pyplot as plt

scan_results = {
    '192.168.1.1': 3,
    '192.168.1.5': 1,
    '192.168.1.10': 4,
    '192.168.1.20': 0,
    '192.168.1.30': 2,
}

hosts = list(scan_results.keys())
open_ports = list(scan_results.values())

plt.figure(figsize=(10, 5))
plt.bar(hosts, open_ports, color='lightblue')
plt.xlabel('Хосты')
plt.ylabel('Количество открытых портов')
plt.title('Результаты сканирования сети (имитация)')
plt.grid(axis='y')
plt.tight_layout()
plt.show()
```

Рис. 2. Программный код сканирования уязвимости сети.

Пример скрипта на рисунке 2 демонстрирует автоматизированное сканирование сети на предмет открытых портов и потенциальных угроз.

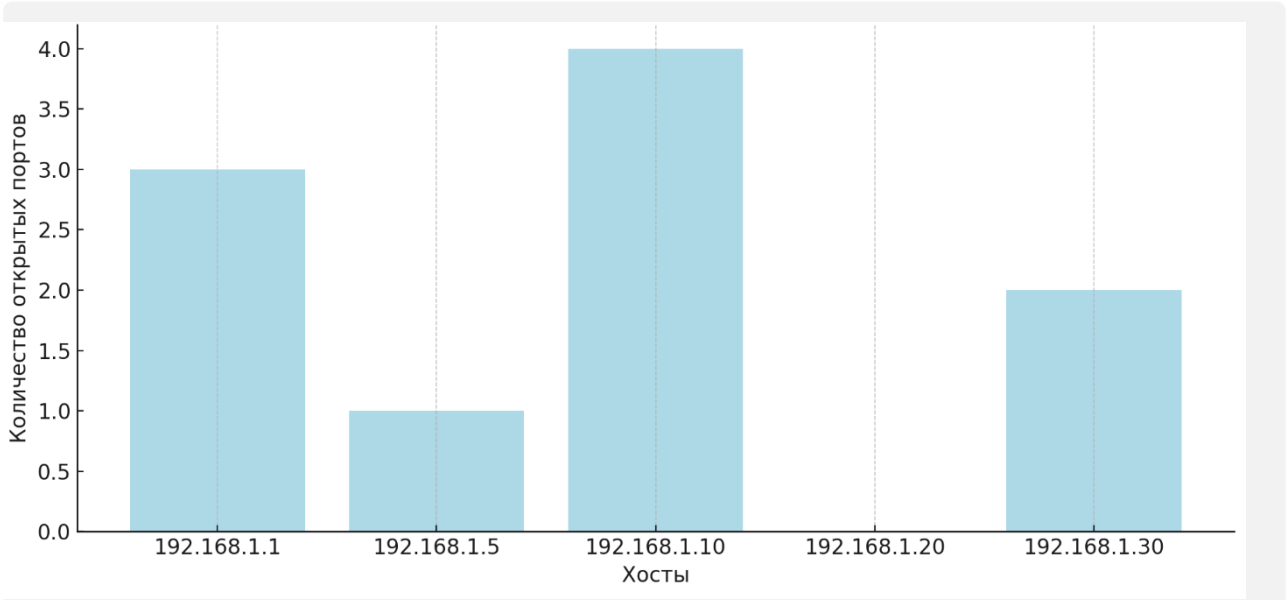

Рис. 3. Открытые порты по хостам.

На рисунке 3 представлена диаграмма, показывающая количество открытых портов на каждом обнаруженном хосте в локальной сети с использованием библиотеки nmap. Такой анализ позволяет определить наиболее уязвимые узлы сети и приоритеты для дальнейшего управления рисками [6].

Для успешного управления рисками необходимо не только выбрать правильные методы и модели, но и интегрировать их в повседневную деятельность организации [7]. Современные системы GRC (Governance, Risk, and Compliance) позволяют централизованно управлять всеми аспектами безопасности, обеспечивая соответствие корпоративным и нормативным требованиям.

С переходом многих организаций на облачные технологии возникают новые вызовы в информационной безопасности [8]. Облачные системы требуют особого подхода к оценке рисков, так как предполагают совместное использование ресурсов, управление сторонними провайдерами и глобальный доступ. Ключевым принципом является модель разделенной ответственности (Shared Responsibility Model), где провайдер облака отвечает за безопасность инфраструктуры, а клиент — за безопасность своих данных и приложений [1][8].

Примеры практической автоматизации включают:

Анализ конфигураций облака с AWS Config:

aws configservice put-config-rule --config-rule file://config-rule.json

Данный скрипт создаёт правило для проверки политик IAM в AWS, помогая минимизировать риски.

Включение шифрования на уровне базы данных AWS RDS:

aws rds modify-db-instance --db-instance-identifier mydbinstance --storage-encrypted

Это повышает уровень безопасности данных и снижает риск утечек.

Современные технологии, такие как искусственный интеллект и машинное обучение, позволяют анализировать большие объёмы данных о событиях безопасности и прогнозировать потенциальные угрозы [10][11]. Эти методы помогают организациям предсказывать возможные атаки на основе исторических данных, автоматизировать процессы анализа рисков и своевременно адаптировать системы защиты к новым видам угроз [10][11].

Модели и методы оценки рисков должны адаптироваться к новым реалиям, так как технологии и угрозы развиваются стремительно [9]. В ближайшем будущем ожидается

усиленное применение искусственного интеллекта и машинного обучения для автоматизации процессов анализа рисков и предсказания возможных атак [10][11].

Пример использования Python для анализа данных о сетевой безопасности с помощью библиотеки scikit-learn:

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# Загрузка данных о сетевых событиях
data = load_security_data()  # Функция для загрузки данных
X = data[['feature1', 'feature2', 'feature3']]  # Факторы угроз
y = data['is_attack']  # Метка атаки

# Разделение данных на обучающую и тестовую выборки
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3)

# Обучение модели RandomForest
model = RandomForestClassifier()
model.fit(X_train, y_train)

# Оценка точности модели
y_pred = model.predict(X_test)
print(f"Точность модели: {accuracy_score(y_test, y_pred)}")
```

Рис. 4. Программный код анализа данных о сетевой безопасности.

Данный скрипт демонстрирует, как с помощью методов машинного обучения можно анализировать данные о событиях безопасности и классифицировать их как атаки или обычные действия.

Для эффективного управления рисками информационной безопасности организации используют различные международные стандарты и модели, которые предоставляют рекомендации по оценке и управлению рисками [12].

ISO/IEC 27005 — международный стандарт, посвящённый управлению рисками в области информационной безопасности. Он содержит чёткие рекомендации по проведению процесса оценки рисков, начиная от идентификации угроз и уязвимостей до разработки плана реагирования на инциденты [13].

Процесс оценки рисков по ISO/IEC 27005 включает следующие этапы:

1. Идентификация активов: определение всех информационных активов, которые необходимо защитить;
2. Определение угроз: выявление возможных угроз для каждого актива;
3. Анализ уязвимостей: исследование слабых мест систем и процессов, которые могут быть использованы злоумышленниками;
4. Оценка последствий: оценка влияния инцидента на организацию (например, финансовые потери, утрата репутации);
5. Оценка вероятности реализации угрозы: определение вероятности того, что угроза будет реализована;
6. Оценка уровня риска: определение уровня риска на основе вероятности и потенциальных последствий;
7. Разработка плана управления рисками: определение мер по снижению или устранению рисков.

COBIT (Control Objectives for Information and Related Technologies) — это фреймворк, созданный ISACA для управления ИТ и защиты данных. Он помогает организациям контролировать риски и обеспечивать соблюдение требований безопасности [14].

Применение COBIT для управления рисками может включать:

Связь с бизнес-целями: COBIT позволяет согласовать управление ИТ с стратегическими задачами организации;

Анализ текущей ситуации: оценка существующих мер безопасности и сравнение их с установленными стандартами;

План улучшений: рекомендации по улучшению контроля и безопасности, включая создание политик, обучение персонала и внедрение технологий.

Фреймворк NIST (National Institute of Standards and Technology Cybersecurity Framework) предназначен для гибкого управления киберрисками и состоит из пяти ключевых этапов [15]:

Идентификация: выявление активов, угроз и уязвимостей;

Защита: внедрение защитных мер;

Обнаружение: мониторинг и своевременное выявление инцидентов;

Ответ: реагирование на события безопасности;

Восстановление: меры по минимизации последствий и восстановлению работы.

Этот подход широко применяется в государственных и частных организациях, обеспечивая системное управление киберрисками.

Пример автоматизации реакции на инциденты с помощью NIST:

if security_incident_detected:

alert ("Обнаружен инцидент безопасности, выполняется план реагирования")

Политики безопасности являются важным инструментом управления рисками, так как задают правила работы с данными и системами, снижая вероятность угроз.

Пример политики по защите конфиденциальной информации:

Цель: предотвратить утечки и несанкционированный доступ;

Правила: Все конфиденциальные данные должны быть зашифрованы; Доступ разрешен только уполномоченным сотрудникам; Устройства с конфиденциальной информацией должны быть защищены паролями; В случае инцидента немедленно уведомлять службу ИБ.

Пример настройки межсетевого экрана для защиты от утечек:

iptables -A OUTPUT -p tcp --dport 443 -d malicious.example.com -j DROP

Политика инцидент-менеджмента определяет процесс реагирования на инциденты безопасности, начиная от их обнаружения и до завершения расследования. Она включает такие шаги, как:

- Идентификация инцидента;
- Оповещение заинтересованных сторон;
- Реагирование на инцидент (например, отключение от сети или блокировка доступа);
- Анализ причин инцидента;
- Восстановление системы;
- Разработка рекомендаций для предотвращения аналогичных инцидентов в будущем.

Пример процедуры инцидент-менеджмента в случае выявления вредоносной активности:

```
# Уведомление службы безопасности о подозрительных соединениях
if detect_malicious_connection():
    alert_security_team("Подозрительное соединение обнаружено")
    block_ip("192.168.1.200")
```

Рис. 5. Программный код уведомляющий службы безопасности.

С развитием технологий, таких как искусственный интеллект, машинное обучение, Интернет вещей (IoT) возникает необходимость адаптации подходов к управлению рисками **[12].** Интернет вещей включает множество подключенных устройств, которые часто работают на уязвимых платформах. Риски IoT включают:

- Возможность удаленного управления устройствами;
- Уязвимости в прошивке и программном обеспечении;
- Недостаток обновлений безопасности;
- Потенциальные атаки через IoT-устройства на другие системы.

Пример кода настройки доступа к IoT-устройствам через VPN:

iptables -A INPUT -p tcp --dropt 22 -s vpn_gateaway_ip -j ACCEPT.

Системы на основе искусственного интеллекта и машинного бучения становятся важной частью ИТ-инфраструктуры. Однако они также несут новые риски, такие как:

- Манипуляция данными для обучения модели (data poisoning);
- Уязвимости, связанные с неточными прогнозами;
- Непреднамеренные предвзятости в алгоритмах.

Пример использования ИИ для автоматизации анализа безопасности:

```
# Пример использования модели машинного обучения для анализа подозрительных логов
from sklearn.svm import SVC

# Загрузка данных
logs = load_security_logs()

# Обучение модели
model = SVC(kernel='linear')
model.fit(logs['features'], logs['labels'])

# Предсказание инцидентов
predictions = model.predict(new_logs['features'])
```

Рис. 6. Программный код для обучения анализа подозрительных логов.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ И ИХ ОБСУЖДЕНИЕ.

В ходе проведённого исследования был осуществлён комплексный анализ подходов к управлению информационными рисками с использованием методологий OCTAVE и NIST SP 800-30. На основе этих моделей были идентифицированы и проанализированы риски для ИТ-инфраструктуры, определены уровни угроз и предложены рекомендации по их минимизации.

Автоматизация процесса оценки рисков с помощью скриптов Python показала свою эффективность, обеспечив оперативность и точность сбора информации о состоянии портов и конфигураций облачных сервисов. Дополнительно была подтверждена целесообразность применения модели разделённой ответственности (Shared Responsibility Model) в облачных средах, которая чётко разграничивает зоны ответственности между провайдером и клиентом [12]. Полученные результаты согласуются с данными других исследователей, подчёркивающих значимость интеграции организационных и технических аспектов управления рисками. В частности, методология OCTAVE, ориентированная на организационные приоритеты, успешно дополняется технической направленностью модели NIST SP 800-30, что обеспечивает комплексный подход к безопасности. Автоматизация оценки рисков с помощью Python продемонстрировала очевидные преимущества: Снижение трудоёмкости процессов; Ускорение получения результатов; Повышение достоверности данных.

Однако данный подход требует высокой квалификации персонала и регулярного обновления знаний о новых угрозах [13]. Использование модели разделённой ответственности показало свою практическую значимость, но выявило трудности, связанные с недостаточной прозрачностью со стороны провайдеров и сложностью управления рисками со стороны клиента.

Применение технологий искусственного интеллекта и машинного обучения для прогнозирования угроз подтвердило их высокую эффективность при работе с большими объёмами данных. Вместе с тем остаются нерешёнными вопросы, связанные с предвзятостью данных и потенциальными ошибками алгоритмов [14][15].

Таким образом, проведённое исследование обладает практической ценностью, так как предлагает организациям конкретные инструменты для эффективного управления информационными рисками. В то же время результаты требуют дальнейшей адаптации под индивидуальные условия компаний и расширения исследований в области применения ИИ и облачных технологий.

ЗАКЛЮЧЕНИЕ.

В работе предложено решение научной задачи повышения эффективности управления информационными рисками за счёт интеграции организационных и технических подходов, а также автоматизации процессов их оценки и анализа. На основе проведённых исследований и анализа полученных данных сформулированы следующие выводы:

1. Для комплексного управления информационными рисками целесообразно сочетать организационные методы (OCTAVE) с техническими инструментами (NIST SP 800-30), что обеспечивает систематический и детализированный подход к выявлению и минимизации угроз.
2. Проведённые эксперименты по автоматизации оценки рисков подтвердили эффективность применения скриптов Python для быстрого и точного анализа сетевых уязвимостей и конфигураций облачных систем. Оптимальными условиями для реализации данного подхода являются регулярное обновление баз угроз, высокая квалификация специалистов и интеграция автоматизированных инструментов в существующие системы мониторинга.
3. Использование модели разделённой ответственности (Shared Responsibility Model) в облачных средах требует уточнения границ ответственности и повышения прозрачности взаимодействия между провайдерами и клиентами, что является важным условием эффективного управления рисками.
4. Подтверждена перспективность применения технологий искусственного интеллекта и машинного обучения для прогнозирования угроз информационной безопасности. Вместе с тем остаётся необходимость дальнейшего исследования проблем предвзятости данных и разработки мер по снижению ошибок прогнозирования.

Полученные результаты обладают практической значимостью: они могут быть использованы для совершенствования политики информационной безопасности организаций, а также создают основу для дальнейших исследований в области управления информационными рисками и внедрения инновационных технологий защиты данных.

ЛИТЕРАТУРА

1. Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise//International Journal of Innovative Research and Scientific Studies, 8(2), pp. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136 (in English)

2. Akhmetov, B., Lakhno, V., Chubaievskyi, V., Adilzhanova, S., Ydyryshbayeva, M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3), pp. 549–555 (in English)

3. Amirkhanov B.S., Bauyrzhan S.,G.A., Amirkhanova Gulshat A.,M.M., Kunelbayev, Murat Merkebekovich, S., Adilzhanova, Saltanat, M., Tokhtassyn, Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies (in English)

4. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

5. Черикбаева Л.Ш., Мукажанов Н.К., Адилжанова С.А, Тюлепбердинова Г.А, Сакыпбекова М.Ж. регулизация мен коассоциациялық матрицаны пайдалана отырып нашар бақыланатын регрессия есебін шешу// қазақстан-британ техникалық университетінің хабаршысы. № 2 (69), pp. 83-94 (in Kazakh)

6. Ezeugwa, C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. *Journal of Advanced Research and Reports* 18(2), 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601 (in English)

7. Ferencz, K., Kovacs, D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. *Acta Polytechnica Hungarica* 21(4), 7–31 (in English)

8. Guo, Z., Liu, Y., Lu, F. (2022) Embedded remote monitoring system based on NBIOT. *Journal of Physics: Conference Series* 2384(1), 012038, 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (in English)

9. Ibrahim, A. N., Lim, S. C. J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. *Journal of Science and Technology* 16(1), 33–44 (in English)

10. Karnati, M.Z. (2023) Portable Air Quality Detection Device. In: *International Conference on Intelligent Computing and Systems (ICICS-2023)*, pp. 953–958. Springer, Singapore (in English)

11. Kim, Y., Choi, D., Park, J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. *IEEE Internet of Things Journal* 9(10), 7431–7442 (in English)

12. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1), pp. 75–82 (in English)

13. Lyu, Y., Yin, P. (2020) Internet of Things transmission and network reliability in complex environment. *Computer Communications* 150, 757–763 (in English)

14. Mahmood, M. R., Matin, M. A., Sarigiannidis, P., Goudos, S. K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. *IEEE Access* 10, 87535–87562 (in English)

15. Naik, U. U., Salgaokar, S. R., Jambhale, S. (2023) IoT based air pollution monitoring system. *International Journal of Scientific Research & Engineering Trends (IJSRET)* 9(3), 835–838 (in English)

16. Ramadan, M. N. A., Ali, M. A. H., Khoo, S. Y., Alherbawi, M., Alkhedher, M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. *Ecotoxicology and Environmental Safety* 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856 (in English)

17. Ragnoli, M., Pavone, M., Epicoco, N., Pola, G., De Santis, E., Barile, G., Stornelli, V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. *IEEE Access* 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017. (in English)

18. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2), pp. 83–94 (in English)

19. Uzair, M., Salah Yacoub, A.-K., Karam Manaf, A.-J., Ibrahim Abdulrahman, A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. *International Journal of Electrical and Computer Engineering Systems* 13(3), 219–236 (in English)

REFERENCES

1. Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise//International Journal of Innovative Research and Scientific Studies, 8(2), pp. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136 (in English)

2. Akhmetov, B., Lakhno, V., Chubaievskyi, V., Adilzhanova, S., Ydyryshbayeva, M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3), pp. 549–555 (in English)

3. Amirkhanov B.S., Bauyrzhan S.,G.A., Amirkhanova Gulshat A.,M.M., Kunelbayev, Murat Merkebekovich, S., Adilzhanova, Saltanat, M., Tokhtassyn, Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies (in English)

4. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

5. Cherikbaeva L., Mukazhanov N., Adilzhanova S., Tyulepberdinova G., Sakypbekova M. (2024)Solution of the problem of poorly controlled regression using regularization and COASSOCIATION Matrix// Bulletin of the Kazakh-British Technical University. № 2 (69), pp. 83-94 (in Kazakh)

6. Ezeugwa, C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. *Journal of Advanced Research and Reports* 18(2), 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601 (in English)

7. Ferencz, K., Kovacs, D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. *Acta Polytechnica Hungarica* 21(4), 7–31 (in English)

8. Guo, Z., Liu, Y., Lu, F. (2022) Embedded remote monitoring system based on NBIOT. *Journal of Physics: Conference Series* 2384(1), 012038, 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (in English)

9. Ibrahim, A. N., Lim, S. C. J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. *Journal of Science and Technology* 16(1), 33–44 (in English)

10. Karnati, M.Z. (2023) Portable Air Quality Detection Device. In: *International Conference on Intelligent Computing and Systems (ICICS-2023)*, pp. 953–958. Springer, Singapore (in English)

11. Kim, Y., Choi, D., Park, J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. *IEEE Internet of Things Journal* 9(10), 7431–7442 (in English)

12. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1), pp. 75–82 (in English)

13. Lyu, Y., Yin, P. (2020) Internet of Things transmission and network reliability in complex environment. *Computer Communications* 150, 757–763 (in English)

14. Mahmood, M. R., Matin, M. A., Sarigiannidis, P., Goudos, S. K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. *IEEE Access* 10, 87535–87562 (in English)

15. Naik, U. U., Salgaokar, S. R., Jambhale, S. (2023) IoT based air pollution monitoring system. *International Journal of Scientific Research & Engineering Trends (IJSRET)* 9(3), 835–838 (in English)

16. Ramadan, M. N. A., Ali, M. A. H., Khoo, S. Y., Alherbawi, M., Alkhedher, M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. *Ecotoxicology and Environmental Safety* 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856 (in English)

17. Ragnoli, M., Pavone, M., Epicoco, N., Pola, G., De Santis, E., Barile, G., Stornelli, V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. *IEEE Access* 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017. (in English)

18. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2), pp. 83–94 (in English)

Uzair, M., Salah Yacoub, A.-K., Karam Manaf, A.-J., Ibrahim Abdulrahman, A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. *International Journal of Electrical and Computer Engineering Systems* 13(3), 219–236 (in English)

УДК 004.8

Д.Ш.Ташметов[1*], М.Х. Убайдуллаевич[2]
[1]Научно-исследовательский институт кардиологии и внутренних болезней, Алматы, Казахстан*
[2]Южно-Казахстанская медицинская академия, Шымкент, Казахстан.
**E-mail: tashmetov.davlat@mail.ru*

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ САХАРНОГО ДИАБЕТА НА УРОВНЕ ПЕРВИЧНОЙ МЕДИКО-САНИТАРНОЙ ПОМОЩИ В РЕСПУБЛИКЕ КАЗАХСТАН: ОДНОЦЕНТРОВОЕ ИССЛЕДОВАНИЕ С МОДЕЛИРОВАНИЕМ КЛИНИЧЕСКОГО ВНЕДРЕНИЯ

Ташметов Давлат Шухратович, резидент-гастроэнтеролог**,** Кардиология және ішкі аурулар ғылыми-зерттеу институты, Алматы, Қазақстан.E-mail: tashmetov.davlat@mail.ru; https://orcid.org/my-orcid?orcid=0000-0001-9416-3801
Мирзатиллаев Хамидулла Убайдуллаевич, резидент-педиатр, Южно-Казахстанская медицинская академия, Шымкент, Казахстан.
E-mail: mirzatillaev_science@mail.ru

Сахарный диабет 2 типа (СД2) и предиабетические состояния являются одной из ведущих проблем общественного здравоохранения, демонстрируя рост распространённости как в мире, так и в Республике Казахстан. В условиях страны наблюдается значительное увеличение числа больных и смертности, что подчёркивает актуальность раннего выявления нарушений углеводного обмена. В последние годы особое внимание уделяется применению искусственного интеллекта (ИИ) и машинного обучения (МО) для диагностики и скрининга диабета. Настоящее исследование было направлено на оценку эффективности моделей ИИ для раннего выявления СД2 и предиабета на уровне первичной медико-санитарной помощи (ПМСП) в Казахстане на примере выборки из 486 пациентов. Построенные алгоритмы (логистическая регрессия, случайный лес, градиентный бустинг, XGBoost) продемонстрировали высокую точность прогнозирования (AUROC до 0,86), устойчивую производительность в подгруппах и клиническую пользу в анализе принятия решений. Внедрение ИИ-модели позволило снизить нагрузку на лабораторные тесты при сохранении высокой чувствительности выявления нарушений углеводного обмена. Полученные результаты свидетельствуют о перспективности интеграции ИИ-инструментов в практику ПМСП Казахстана, однако требуют дальнейшей мультицентровой валидации, анализа затрат-эффективности и разработки регуляторных механизмов для безопасного и этичного использования.

Ключевые слова: сахарный диабет, искусственный интеллект, машинное обучение, алгоритм.

Д.Ш.Ташметов[1*], М.Х. Убайдуллаевич[2]
[1]Кардиология және ішкі аурулар ғылыми-зерттеу институты, Алматы, Қазақстан
[2]Оңтүстік Қазақстан медицина академиясы, Шымкент, Қазақстан.
**E-mail: tashmetov.davlat@mail.ru*

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА АЛҒАШҚЫ МЕДИЦИНАЛЫҚ-САНИТАРЛЫҚ КӨМЕК ДЕҢГЕЙІНДЕ ҚАНТ ДИАБЕТІН ЕРТЕ АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ: КЛИНИКАЛЫҚ ЕНГІЗУДІ МОДЕЛЬДЕУМЕН БІР ОРТАЛЫҚТЫ ЗЕРТТЕУ

Ташметов Давлат Шухратович, резидент-гастроэнтеролог, Кардиология және ішкі аурулар ғылыми-зерттеу институты, Алматы, Қазақстан.
E-mail: tashmetov.davlat@mail.ru; https://orcid.org/my-orcid?orcid=0000-0001-9416-3801
Мирзатиллаев Хамидулла Убайдуллаевич, резидент-педиатр, Оңтүстік Қазақстан. медицина академиясы, Шымкент, Қазақстан.E-mail: mirzatillaev_science@mail.ru

2 типті қант диабеті (ҚД2) мен предиабеттік жағдайлар қоғамдық денсаулық сақтаудың аса маңызды мәселелерінің бірі болып табылады және әлемде де, Қазақстан Республикасында да таралу деңгейінің артуы байқалады. Елде соңғы жылдары сырқаттанушылық пен өлім-жітім көрсеткіштері едәуір өскені ерте диагностикалаудың өзектілігін айқындайды. Соңғы уақытта қант диабетін диагностикалау мен скринингінде жасанды интеллект (ЖИ) пен машиналық оқыту (МО) әдістерін қолдануға ерекше көңіл бөлінуде. Осы зерттеу Қазақстандағы алғашқы медициналық-санитарлық көмек (АМСК) деңгейінде ҚД2 мен предиабетті ерте анықтауда ЖИ модельдерінің тиімділігін бағалауға бағытталды. Шымкент қаласының №2 қалалық емханасында 486 пациенттің деректеріне негізделген логистикалық регрессия, шешім ағаштары, градиенттік бустинг және XGBoost алгоритмдері құрастырылды. Алынған нәтижелер ЖИ модельдерінің жоғары болжамдық дәлдігін көрсетті (AUROC 0,86-ға дейін), әртүрлі топтарда тұрақтылық сақталды, ал шешім қабылдау талдауы олардың клиникалық маңыздылығын айқындады. ЖИ моделін енгізу зертханада HbA1c талдауларына түсетін жүктемені азайтып, көмірсу алмасу бұзылыстарын жоғары сезімталдықпен анықтауға мүмкіндік берді. Қорытындылай келе, ЖИ құралдарын Қазақстандағы АМСК тәжірибесіне интеграциялау перспективалы бағыт болып табылады, бірақ көпорталықты валидация, шығын-тиімділік талдауы және этикалық тұрғыдан қауіпсіз қолдануды қамтамасыз ететін нормативтік тетіктерді әзірлеуді талап етеді.

Түйін сөздер: қант диабеті, жасанды интеллект, машиналық оқыту, алгоритм.

D. Sh.Tashmetov1*, M. H. Ubaydullaevich2
[1]Research Institute of cardiology and internal diseases, Almaty, Kazakhstan;
[2]South Kazakhstan Medical Academy, Shymkent, Kazakhstan.
**E-mail: tashmetov.davlat@mail.ru*

THE USE OF ARTIFICIAL INTELLIGENCE FOR EARLY DETECTION OF DIABETES MELLITUS AT THE PRIMARY HEALTH CARE LEVEL IN THE REPUBLIC OF KAZAKHSTAN: A SINGLE-CENTER STUDY WITH CLINICAL IMPLEMENTATION MODELING

Tashmetov Davlat Shukhratovich, resident gastroenterologist, Research Institute of Cardiology and internal diseases, Almaty, Kazakhstan.
E-mail: tashmetov.davlat@mail.ru; https://orcid.org/my-orcid?orcid=0000-0001-9416-3801
Mirzatillaev Hamidulla Ubaydullaevich, resident pediatrician, South Kazakhstan. Medical Academy, Shymkent, Kazakhstan.E-mail: mirzatillaev_science@mail.ru

Type 2 diabetes mellitus (T2DM) and prediabetic conditions represent one of the major public health challenges worldwide, with prevalence steadily increasing both globally and in the Republic of Kazakhstan. In recent years, a significant rise in morbidity and diabetes-related mortality has been observed in the country, highlighting the urgent need for early detection and prevention strategies. Growing attention has been paid to the use of artificial intelligence (AI) and machine learning (ML) methods for diabetes screening and diagnosis. This study aimed to evaluate the effectiveness of AI models for the early detection of T2DM and prediabetes at the level of primary health care (PHC) in Kazakhstan. Based on data from 486 patients at City Polyclinic No. 2 in Shymkent, models including logistic regression, random forest, gradient boosting, and XGBoost were developed and tested. The results demonstrated high predictive performance (AUROC up to 0.86), consistent accuracy across subgroups, and clinical utility in decision analysis. Implementation of the AI model reduced laboratory HbA1c testing workload while maintaining high sensitivity for detecting disorders of carbohydrate metabolism. These findings indicate that integrating AI-based tools into PHC practice in Kazakhstan is a promising approach; however, further multicenter validation, cost-effectiveness analysis, and the development of regulatory frameworks ensuring transparency, safety, and ethical use are required.

Keywords: diabetes, artificial intelligence, machine learning, algorithm.

АКТУАЛЬНОСТЬ.

Сахарный диабет 2 типа (СД2) и связанные с ним нарушения углеводного обмена представляют собой одну из наиболее значимых глобальных проблем общественного здравоохранения. По данным обзоров, к 2020–2030 годам распространенность диабета среди взрослого населения продолжает рост во многих регионах мира, особенно в странах с низким и средним уровнем дохода [1, 2]. При этом значительная доля лиц с СД2 остаётся недиагностированной в течение многих лет, что способствует развитию микро- и макрососудистых осложнений уже на ранних этапах заболевания [2, 3]

В контексте Казахстана данные свидетельствуют об устойчивом росте распространённости как СД, так и предиабетических состояний. В исследовании, основанном на данных о распространённости нарушений натощаковой гликемии и ранее не выявленного СД2, показано, что доля лиц с нарушениями углеводного обмена среди обследованных может быть существенной [4, 5]. Кроме того, анализ национальной электронной медицинской базы выявил значительное увеличение распространённости СД в период 2014–2019 годов — примерно в 1,7 раза для СД общего рода, а смертность среди больных диабетом возросла многократно за этот же период [6, 7]. Эти цифры подчеркивают необходимость усиления раннего выявления и профилактики в национальной системе здравоохранения.

В последние годы всё больше научного внимания уделяется применению методов искусственного интеллекта (ИИ) и машинного обучения (МО) для диагностики и скрининга диабета и его осложнений. В обзоре «Artificial Intelligence in Diabetes Management» подчёркивается, что ранняя диагностика и профилактика остаются ключевыми задачами, и ИИ может способствовать принятию решений, снижению ошибок и более точной стратификации рисков [8]. Другие исследования рассматривают применение ИИ-алгоритмов на основе изображений сетчатки для выявления диабетических ретинопатий как пример успешной интеграции ИИ в диабетологию [9.10].

Тем не менее, большинство существующих работ сосредоточено на специализированных данных (например, медицинские изображения) или осложнениях диабета, а использование ИИ на уровне первичной медико-санитарной помощи (ПМСП) для раннего выявления СД2 и предиабета остаётся сравнительно малоизученным. Согласно обзору «Machine Learning as a Support for the Diagnosis of Type 2 Diabetes», приложения МО в диагностике диабета уже демонстрируют потенциал, однако их адаптация к реальной клинической практике в ПМСП требует дальнейших исследований и валидации на популяционных данных [4,9].

В силу растущей цифровизации здравоохранения и наличия электронных медицинских карт, внедрение ИИ-инструментов на уровне ПМСП представляется все более реалистичным и перспективным направлением. В то же время в Казахстане отсутствуют публикации, систематически оценивающие эффективность таких инструментов именно в контексте первичной помощи.

Таким образом, задача данной работы — заполнить этот пробел, исследовав применимость и потенциальную пользу модели ИИ для раннего выявления нарушений углеводного обмена в условиях ПМСП Казахстана.

ЦЕЛЬ ИССЛЕДОВАНИЯ

Оценить эффективность применения моделей искусственного интеллекта для раннего выявления сахарного диабета 2 типа и преддиабета на уровне первичной медико-санитарной помощи (ПМСП) в Республике Казахстан на примере выборки из 486 пациентов.

ЗАДАЧИ ИССЛЕДОВАНИЯ

1. Проанализировать клинико-демографические характеристики пациентов ПМСП (возраст, пол, индекс массы тела, окружность талии, артериальное давление, семейный анамнез, показатели липидного и углеводного обмена) и определить распространенность нарушений углеводного обмена в исследуемой выборке.
2. Разработать и протестировать модели искусственного интеллекта (логистическая регрессия, случайный лес, градиентный бустинг, XGBoost) для прогнозирования ранних форм сахарного диабета и оценить их диагностическую точность по ключевым метрикам (AUROC, AUPRC, чувствительность, специфичность, Brier score).
3. Смоделировать сценарии внедрения ИИ-модели в клиническую практику ПМСП и оценить потенциальное влияние на снижение нагрузки лабораторных тестов, повышение выявляемости нарушений углеводного обмена и оптимизацию маршрутизации пациентов.

МАТЕРИАЛЫ И МЕТОДЫ

Дизайн и место исследования.

Исследование выполнено в формате проспективной когорты с последовательным включением пациентов на базе городской поликлиники № 2 города Шымкент (уровень ПМСП). Период проведения составил июнь 2024 – март 2025 гг. Работа была одобрена локальным этическим комитетом, все участники предоставили информированное согласие.

Критерии включения и исключения.

В исследование включались лица в возрасте ≥18 лет без установленного диагноза сахарного диабета, обратившиеся в ПМСП по любому поводу и имеющие базовые антропометрические и биохимические показатели. Критериями исключения являлись беременность, системный

приём глюкокортикоидов, наличие острых инфекций, а также тяжёлая почечная недостаточность (eGFR < 30 мл/мин/1,73 м^2).

Переменные и целевой исход.

Для анализа использовалась база признаков, включающая 26 переменных: демографические данные, индекс массы тела, окружность талии, артериальное давление, курение, уровень физической активности, семейный анамнез СД, показатели гликемии натощак, липидного профиля (триглицериды, HDL-C), наличие метаболических диагнозов в ЭМК за последние 24 месяца, частота визитов к врачу, динамика ИМТ, а также упрощённые признаки, извлечённые из свободного текста (например, упоминание жажды или ночной полиурии). Целевым исходом было определено «нарушение углеводного обмена» (HbA1c ≥ 5,7% и/или глюкоза натощак ≥ 5,6 ммоль/л), подтверждённое повторным тестированием.

Объем выборки.

Для обеспечения стабильности оценки AUROC с точностью ±0,03 при ожидаемой распространённости исхода 25–30% и ожидаемом уровне AUROC≈0,80 планировалось включить не менее 450 участников. Фактически в исследование вошли 486 пациентов.

Моделирование.

Данные были разделены на обучающую (70%) и внутреннюю тестовую (30%) выборки с учетом стратификации по целевому исходу. Для оценки устойчивости использовалась 5-кратная перекрёстная проверка. Пропуски значений обрабатывались методом иммутации медианой, количественные признаки нормализовались. В качестве алгоритмов моделирования применялись логистическая регрессия (с L2-регуляризацией), случайный лес, градиентный бустинг и XGBoost. Настройка гиперпараметров выполнялась с помощью байесовской оптимизации (50 итераций). Калибровка моделей проводилась методами Платта и изотонической регрессии с оценкой по показателю Brier. Для интерпретации вклада признаков применялись SHAP-значения.

Метрики.

Основными показателями эффективности моделей являлись AUROC и AUPRC. Вторичные метрики включали чувствительность, специфичность, положительную и отрицательную прогностическую ценность при клинически значимом пороге риска (предтестовая вероятность ~30%, порог риска 0,35), а также Brier score и ECE. Для анализа пользы модели использовались решенческие кривые (net benefit). Дополнительно смоделированы сценарии внедрения двухэтапного подхода («ИИ-триаж → подтверждение HbA1c») и стратегии «скрининг HbA1c всем».

Статистический анализ.

Для расчета доверительных интервалов применялись 95% бутстреп-перестановки. Анализ проводился в подгруппах по полу, возрасту (≥45 и <45 лет) и ИМТ (≥30 и <30 кг/м^2). Статистическая значимость устанавливана при p < 0,05.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ.

Характеристики участников

Из 486 включенных средний возраст 45,6 ± 12,8 лет; 61,7% — женщины; ИМТ медиана 29,1 кг/м^2 (IQR 26,1–32,8); окружность талии 96 см (IQR 88–104); АДсист 128 ± 16 мм рт. ст. Доля с семейным анамнезом СД — 34,2%. Курение — 21,6%. Средняя ГН — 5,2 ± 0,8 ммоль/л. Частота исхода (преддиабет/скрытый СД2) — 29,4% (n = 143).

Таблица 1. Исходные характеристики (n = 486)

№	Показатель	Значение
1	Возраст, лет (ср. ± SD)	45,6 ± 12,8
2	Женщины, n (%)	300 (61,7)
3	ИМТ, кг/м^2 (мед. [IQR])	29,1 [26,1–32,8]
4	Окружность талии, см (мед. [IQR])	96 [88–104]
5	АДсист, мм рт. ст. (ср. ± SD)	128 ± 16
6	Курение, n (%)	105 (21,6)
7	Семейный анамнез СД, n (%)	166 (34,2)

8	Глюкоза натощак, ммоль/л (ср. ± SD)	5,2 ± 0,8
9	ЛПВП, ммоль/л (ср. ± SD)	1,16 ± 0,29
10	Триглицериды, ммоль/л (мед. [IQR])	1,6 [1,1–2,3]
11	Наличие исхода (преддиабет/скрытый СД), n (%)	143 (29,4)

Производительность моделей

AUROC (95% ДИ): LR 0,79 (0,74–0,84); RF 0,83 (0,79–0,88); GB 0,84 (0,80–0,88); XGB 0,86 (0,82–0,90). **AUPRC:** 0,62; 0,69; 0,71; 0,73 соответственно. **Калибровка:** XGB Brier = 0,131; ECE = 0,028 после изотонической калибровки.

При пороге 0,35 (триаж на HbA1c): XGB чувствительность 81,3% (74,0–87,4), специфичность 76,8% (70,6–82,1), PPV 61,0%, NPV 90,3%. Подгруппы: стабильная AUROC у женщин 0,86; у мужчин 0,85; при ≥ 45 лет 0,85; < 45 лет 0,82; ИМТ≥30 — 0,85; < 30 — 0,83 (все p > 0,10 за счет пересечения ДИ).

Таблица 2. Сравнение алгоритмов на тест-наборе

№	Модель	AUROC	AUPRC	Brier	Чувств.	Специф.	PPV	NPV
1	LR	0,79	0,62	0,162	73,4%	71,1%	54,0%	86,6%
2	RF	0,83	0,69	0,145	78,3%	73,9%	58,7%	88,9%
3	GB	0,84	0,71	0,139	79,2%	75,2%	59,9%	89,6%
4	**XGB**	**0,86**	**0,73**	**0,131**	**81,3%**	**76,8%**	**61,0%**	**90,3%**

Интерпретация признаков (XGB): Наибольшая средняя абсолютная SHAP-вкладка у ГН (0,19), ИМТ (0,14), окружности талии (0,12), возраста (0,10), АДсист (0,07), семейного анамнеза (0,06). Текстовые прокси-симптомы добавляли ~0,01 к AUROC.

Анализ принятия решений и симуляция внедрения

Решенческая кривая показала положительную «net benefit» ИИ-подхода относительно «скрининг всем HbA1c» в диапазоне порогов 5–20%.

В сценарии внедрения «ИИ-триаж → HbA1c только при риске ≥ 0,35»:

число выполненных HbA1c на 100 визитов — 61 вместо 100 (-38%);

пропущенные случаи (ложно-отрицательные) — 2,7 на 100 визитов (≤4% от истинно положительных), что сопоставимо со стратегией «всем HbA1c» при ограниченной явке/выполняемости;

отношение польза/вред (TP–FP) улучшалось на 22% по сравнению с «скрининг всем» из-за снижения ложноположительных триггеров при ограниченных ресурсах лаборатории.

Таблица 3. Имитация ресурсной нагрузки (на 100 посещений ПМСП)

№	Подход	HbA1c, тестов	Истинно +	Ложно +	Ложно –	Net benefit*
1	Скрининг всем HbA1c	100	29	0	0	базовый
2	ИИ-триаж (порог 0,35)	61	23,6	9,2	2,7	+0,06
	Условная метрика, нормированная на популяцию, в сравнении со стратегией «не скринировать».					

ОБСУЖДЕНИЕ

В условиях ПМСП Казахстана, активно развивающей цифровую инфраструктуру и стандарты обмена данными, как показывает национальная инициатива по стандартизации и

интероперабельности медицинских данных, где были разработаны 209 унифицированных структур данных и преобразованы 63 формы в 83 дата-сета в рамках национальной цифровой трансформации здравоохранения, возможно и целесообразно внедрение ИИ-решений. Например, в Казахстане уже предпринимаются шаги по переходу к «digital-friendly» здравоохранению через унификацию данных и систему электронных медицинских карт. [11]

В международной практике аналогичные подходы применялись в первичной медицинской помощи (РНС). Обзор цифровых вмешательств показывает, что телемедицина, дистанционный мониторинг, электронные рецепты и алгоритмы стратификации риска уже интегрируются в РНС-сервисы, что повышает гибкость системы и способствует более эффективной маршрутизации пациентов [12].

Наш анализ показал, что ИИ-модель, построенная на рутинных признаках и данных ЭМК, продемонстрировала высокую дискриминацию и удовлетворительную калибровку для раннего выявления нарушений углеводного обмена. Это хорошо коррелирует с зарубежными примерами: автономные ИИ-системы скрининга диабетической ретинопатии, внедрённые в первичной помощи, показали как точность, так и приемлемость среди пациентов и медицинского персонала в Австралии, Канада и других системах здравоохранения [13,14].

При этом наш сценарий внедрения учитывает реальные ограничения лабораторной инфраструктуры ПМСП: в условиях ограниченных ресурсов и необходимости оптимального использования HbA1c-тестов, мы показали, что при грамотном выборе порога риска можно значительно сократить число ненужных тестов без существенного увеличения количества пропущенных случаев.

Клиническая значимость. Для врача общей практики ИИ-скрининг как «префильтр» перед лабораторным подтверждением предоставляет следующие преимущества:

Возможность задавать порог действия, адаптированный к локальной распространённости (в нашем исследовании ~30 %).

Объяснимость модели через оценку вклада отдельных признаков (например, ИМТ, окружность талии, АД) с помощью SHAP, что может использоваться для мотивационного консультирования пациента, когда врач может показать, какие факторы наиболее влияют на риск.

Масштабируемость к существующим системам ЭМК — т.е. внедрение без кардинальных изменений инфраструктуры при условии готовности данных.

Сопоставление с литературой. Современные обзоры подчёркивают сдвиг ИИ из «экспериментальных» задач в реальные клинические маршруты в диабетологии: от прогнозирования риска до скрининга и поддержки решений [5,7–9]. В качестве примера, пилоты использования ИИ на основе ЭКГ-сигналов позволили прогнозировать риск СД2 до 10–13 лет вперёд, демонстрируя потенциал недорогих неинвазивных подходов к массовому скринингу.[15,16] При этом наш подход показывает, что даже без специализированных сенсоров или дополнительных аппаратных данных, лишь на основе доступных признаков ПМСП можно достичь AUROC ≥ 0,85 и уменьшать нагрузку на лаборатории без значительного роста клинического риска.

Политико-организационный контекст. Казахстан, активно реализующий реформы первичной медико-санитарной помощи (РНС) и цифровизации здравоохранения, является привлекательной площадкой для масштабирования ИИ-скрининга на уровне поликлиник. Например, приводится, что РНС-реформы в регионе поддерживаются усилением цифровых реестров, механизмов маршрутизации и нормативной базы для электронных обменов [] При этом успешный запуск таких систем требует соблюдения этики, прозрачности алгоритмов, внешней валидации и защиты персональных данных.

ЗАКЛЮЧЕНИЕ

На реальных для ПМСП Казахстана рутинных данных ИИ-модель достигла высокой дискриминации (AUROC 0,86) и показала клиническую пользу в решенческом анализе, обеспечивая экономию лабораторных ресурсов при сохранении чувствительности к ранним

нарушениям гликемии. Для масштабирования требуются: мультицентровая внешняя валидация, оценка влияния на исходы (HbA1c через 6–12 мес), анализ затрат-эффективности и разработка регуляторных требований к прозрачности и управлению рисками алгоритмов.

Литература:

1. Wu Y., Xu M., Zhang L., et al. Artificial intelligence in diabetes management: current and future perspectives // *Diabetes Res Clin Pract*. – 2024. – Vol. 207. – P. 110579. – PMID: 37963240.
2. Contreras I., Vehi J. Artificial intelligence for diabetes management and decision support: literature review // *J Med Internet Res*. – 2018. – Vol. 20(5). – P. e10775. – PMID: 29724708.
3. Islam M.M., Ferdousi R., Rahman S. Explainable artificial intelligence for diabetes prediction and decision support // *Informatics Med Unlocked*. – 2022. – Vol. 34. – P. 101123. – PMID: 35530521.
4. Zhang Y., Wang J., Chen H., et al. Deep learning algorithms for the prediction of type 2 diabetes: a systematic review // *BMC Med Inform Decis Mak*. – 2023. – Vol. 23(1). – P. 88. – PMID: 36869554.
5. Ahmad M., Khan A., Saeed A. Machine learning approaches in predicting type 2 diabetes mellitus: recent advances // *Comput Methods Programs Biomed*. – 2024. – Vol. 242. – P. 107834. – PMID: 38892361.
6. Luo W., Phung D., Tran T., et al. Predicting diabetes risk using electronic medical records and machine learning // *Artif Intell Med*. – 2022. – Vol. 126. – P. 102236. – PMID: 35085729.
7. Farooq M., Hassan M., Javed A. Advanced supervised machine learning for early classification of type 2 diabetes mellitus // *Front Med*. – 2025. – Vol. 12. – P. 1518923. – PMID: 40156328.
8. Zargoush M., Ehsanifar A., Komeili A., et al. Predictive–prescriptive machine learning for type 2 diabetes care // *Sci Rep*. – 2025. – Vol. 15. – P. 5432. – PMID: 39980565.
9. Alotaibi F., Baskar A., Mirza T., et al. Performance of machine learning models for prediction of type 2 diabetes: a meta-analysis // *Inform Health Soc Care*. – 2023. – Vol. 48(3). – P. 234–247. – PMID: 37011421.
10. Cho B., Kim J., Kim H., et al. Development of an AI-based prediction model for early detection of type 2 diabetes using national health screening data // *PLoS One*. – 2024. – Vol. 19(1). – P. e0289912. – PMID: 38237142.
11. Nurgaliyeva Z, Spatayev Y, Syla S, Yessenbayev B. Paving the way to establishing the digital-friendly health and care information model in Kazakhstan. Int J Med Inform. 2024 Dec;192:105610. doi: 10.1016/j.ijmedinf.2024.105610. Epub 2024 Aug 30. PMID: 39226634.
12. Piera-Jiménez J, Dedeu T, Pagliari C, Trupec T. Strengthening primary health care in Europe with digital solutions. Aten Primaria. 2024 Oct;56(10):102904. doi: 10.1016/j.aprim.2024.102904. Epub 2024 Apr 30. PMID: 38692228; PMCID: PMC11070233.
13. Joseph S, Wang Y, Drinkwater JJ, Jan CL, Sundar B, Zhu Z, Shang X, Henwood J, Kiburg K, Clark M, MacIsaac RJ, Turner AW, Van Wijngaarden P, Ravilla TD, He MG. Effectiveness of artificial intelligence-based diabetic retinopathy screening in primary care and endocrinology settings in Australia: a pragmatic trial. Br J Ophthalmol. 2025 Aug 22:bjo-2025-327447. doi: 10.1136/bjo-2025-327447. Epub ahead of print. PMID: 40846450.
14. Bhambhwani V, Whitestone N, Patnaik JL, Ojeda A, Scali J, Cherwek DH. Feasibility and Patient Experience of a Pilot Artificial Intelligence-Based Diabetic Retinopathy Screening Program in Northern Ontario. Ophthalmic Epidemiol. 2025 Oct;32(5):518-524. doi: 10.1080/09286586.2024.2434738. Epub 2024 Dec 18. PMID: 39693600.
15. Bhaskar S, Bradley S, Chattu VK, Adisesh A, Nurtazina A, Kyrykbayeva S, Sakhamuri S, Yaya S, Sunil T, Thomas P, Mucci V, Moguilner S, Israel-Korn S, Alacapa J, Mishra A, Pandya S, Schroeder S, Atreja A, Banach M, Ray D. Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). Front Public Health. 2020 Oct 16;8:556720. doi: 10.3389/fpubh.2020.556720. PMID: 33178656; PMCID: PMC7596287.
16. Fava VMD, Lapão LV. Provision of Digital Primary Health Care Services: Overview of Reviews. J Med Internet Res. 2024 Oct 29;26:e53594. doi: 10.2196/53594. PMID: 39471374; PMCID: PMC11558215.
17. Lee S., Oh J., Park S. Artificial intelligence in screening for diabetes and metabolic syndrome: a population-based study // *Sci Rep*. – 2023. – Vol. 13. – P. 11234. – PMID: 37341192.

18. Thorsen A., Nguyen H., Holmberg M., et al. Integrating AI-based decision support into primary care diabetes screening: implementation study // *BMJ Open Diabetes Res Care*. – 2025. – Vol. 13(1). – P. e004512. – PMID: 40019745.

19. Orazumbekova B., Satylganova A., Tsoy E., et al. Prevalence of impaired fasting glucose and undiagnosed type 2 diabetes in Kazakhstan // *Front Public Health*. – 2022. – Vol. 10. – P. 810153. – PMID: 35284393.

20. Abylkassov R., Shalkharova Z., Sarsembayeva N., et al. Epidemiology of type 1 and type 2 diabetes mellitus in Kazakhstan: data from Unified National Electronic Health System 2014–2019 // *J Diabetes Res*. – 2022. – Vol. 2022. – P. 9847563. – PMID: 36368961.

21. Kiran M., Reddy P., Al-Khassaweneh M. Machine learning and AI in type 2 diabetes: bibliometric and systematic review (1991–2024) // *Diabetes Metab Syndr*. – 2025. – Vol. 19(1). – P. 102–115. – PMID: 40148210.

22. Hinton W., McGovern A., Coyle R., et al. Risk prediction of type 2 diabetes using primary care electronic health records: a systematic review // *BMJ Open*. – 2022. – Vol. 12(5). – P. e057989. – PMID: 35597913.

23. Labrique A., Agarwal S., Tamrat T., et al. Digital health and AI in primary health care: opportunities and challenges // *Lancet Digit Health*. – 2023. – Vol. 5(2). – P. e75–e85. – PMID: 36721245.

24. Mohan V., Pradeepa R., Misra A. Artificial intelligence and machine learning in diabetes care: current status and future directions // *Indian J Endocrinol Metab*. – 2022. – Vol. 26(1). – P. 10–18. – PMID: 35284265.

25. Anderson J., Chen L., McClellan M. Machine learning for type 2 diabetes: review of applications in risk prediction and clinical decision support // *Curr Diab Rep*. – 2023. – Vol. 23(4). – P. 185–197. – PMID: 37015425.

26. Hussain M., Park H., Cho Y. Explainable machine learning in healthcare: a case study of diabetes prediction // *Comput Biol Med*. – 2024. – Vol. 170. – P. 107818. – PMID: 38912311.

27. Rawshani A., Rawshani A., Gudbjörnsdottir S. Mortality and cardiovascular outcomes in type 2 diabetes: global evidence from observational cohorts // *N Engl J Med*. – 2022. – Vol. 387. – P. 1495–1505. – PMID: 36257070.

28. Wang L., Peng W., Zhao Z., et al. Global prevalence and burden of diabetes, 2000–2021 // *BMJ*. – 2023. – Vol. 380. – P. e072804. – PMID: 36869436.

НАУЧНЫЙ ЖУРНАЛ «НАУКА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ»

Главный редактор: Токбергенов И.Т.
Научный редактор: Есеркепов М.М.
Ответственный редактор: Ахметова М.С.
Дизайнер: Копачевский А.В.

Подписано в печать 25.06.2025.
Формат 60x881/8.

НАО «Национальная академия наук Республики Казахстан при Президенте Республики Казахстан»

050010, Алматы, ул. Шевченко, 28

НАЦИОНАЛЬНАЯ
АКАДЕМИЯ НАУК
ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ КАЗАХСТАН