L.K. Kusainova[1] 🆔, M.G. Albekova[2*] 🆔, N.O. Dulatbekov[3] 🆔

1,2,3Karaganda Buketov University, Karaganda, Kazakhstan
(E-mail: albekova_m@mail.ru)

1ORCID ID: 0000-0002-8208-6623, Scopus Author: 57964019600, Researcher ID: ABT-3966-2022
2ORCID ID: 0000-0001-9301-6471
3ORCID ID: 0009-0001-7300-1958, Scopus Author: 57289281100

AI in AML: innovative approaches and potential to improve financial literacy of the population

The purpose of this study is to analyze the use of artificial intelligence (AI) for anti-money laundering (AML) and explore the potential of AI to improve the financial literacy of citizens in order to prevent fraud and participation in money laundering. With the development of modern technology, the ways in which crimes are committed have significantly changed, become more complex and transformed, especially the large-scale cyber-attacks that occur on a daily basis. Therefore, in the current realities, it is necessary to utilize effective technological solutions that can respond quickly to new threats. One such way is the application of artificial intelligence (AI) technologies, which is widespread across various industries, and AML is no exception. The study found that the advantage of using artificial intelligence in AML compliance is its functionality to allow for real-time monitoring and analysis. This makes it possible to detect potential threats or possible illegal activities in which citizens are involved, consciously and unconsciously, and conduct thorough investigations to protect citizens and the state. The main result, which the authors have reached, consists in practical proposals, based on foreign experience, to introduce AI into the AML systems of the Republic of Kazakhstan to detect, report and suppress suspicious money laundering operations.

Keywords: money laundering, artificial intelligence, digital technology, anti-fraud, citizen financial security, scams

Introduction

Money laundering has been a global problem for many years and has a great impact on the economic well-being of every country.

Money laundering is a type of offence in which criminal funds, passing through several stages of transformation, are introduced into the legal economy for further legitimate use. This negative phenomenon poses a serious threat to the national security of the country, adversely affects the stability, integrity, transparency and efficiency of financial systems, undermines economic welfare and hinders the economic development of the country.

The International Financial Action Task Force (FATF) lists drug trafficking, tobacco trafficking, jewelry trafficking, human trafficking, piracy, corruption, and illegal transactions in digital assets among the main types of crime characterized by money laundering [1].

The entire world community is fighting this criminal phenomenon, but despite all the efforts made by countries, billions of criminal funds are laundered every day. The current anti-money laundering system does not fully ensure the proper level of combating money laundering, so in the era of new technologies, it is necessary to create ways and methods that will allow to effectively resist this type of crime.

One of these ways is the implementation of artificial intelligence. AI opens up a wide range of opportunities in this area, providing innovative tools to monitor, analyze and prevent violations. With the ability to analyze large volumes of data, identify atypical transactions and track anomalies that are difficult for humans to spot, AI technologies can take fraud detection to a new level beyond classic risk control analysis by reducing resource intensity.

The purpose of this study is to comprehensively analyze the use of artificial intelligence to combat money laundering; to study the current problem of involving citizens as "droppers" and liability for this in the Republic of Kazakhstan; and to formulate proposals for the introduction of systems to monitor suspicious transactions to prevent the involvement of citizens in fraudulent schemes to launder money.

In order to achieve the established purpose, the following objectives are defined:

---

* Corresponding author's e-mail: *albekova_m@mail.ru*

- To conduct a study on the introduction of artificial intelligence technology to combat money laundering;

- to study the problem of involvement of citizens in fraudulent schemes as "droppers" and legal consequences for this;

- on the basis of foreign analysis to develop recommendations on introduction of AI technologies in monitoring systems of the Republic of Kazakhstan to combat fraud.

The issues of AI application in ensuring financial security and its impact on AML were considered in scientific articles of foreign scientists, such as Ray A., Shabsigh G., Afanasyeva D.V., Dyatlova A.F., Chebukhanova L.V. and others. However, the amount of study regarding the impact of AI on the AML system in the Republic of Kazakhstan, conducted by domestic authors was proved to be insufficient for further implementation of AI-based solutions. And hence, in our opinion, there is no detailed study of the actual problem of "droppers" in the country and measures that can contribute to combating this negative phenomenon.

Methods and materials

The methodological basis of the research is based on general scientific and special scientific methods of cognition of social and legal reality, such as cybernetic, empirical, statistical and comparative-legal methods. The application of cybernetic method allowed us to conclude how new AI technologies can be effective for citizens to avoid involvement in money laundering. The use of empirical and statistical methods allowed us to analyze court practice in criminal and civil cases related to the involvement of citizens in illegal transactions in the field of money laundering. Comparative legal method allowed studying foreign experience and formulating proposals for the implementation of this experience in the legal system of Kazakhstan.

Application of these methods allowed to analyze the practice the application of artificial intelligence for counteracting money laundering. The theoretical basis was formed by the works of domestic and foreign scientists who contributed to the study of artificial intelligence, its application in the AML system; materials of civil and criminal court decisions on this issue were studied. The empirical results are based on foreign practice of application of monitoring systems using AI technologies in existing financial systems to prevent AML risks.

Results

The analysis of this study reveals that despite the key benefits of digitalization, such as increased accessibility of financial services for citizens, there are a number of risks and challenges associated with the loss of data security and confidentiality, which can then be exploited by criminals for illegal purposes, involving citizens in fraudulent schemes. Judicial practice shows that citizens of the country are involved by criminals as "droppers" and carry out illegal transactions both at the conscious and subconscious levels. And since participation in such activities carries both civil and criminal liability, it is necessary to take a number of measures with regard to counteracting the participation of individuals in fraudulent money laundering schemes. Therefore, it is now becoming relevant for the financial sector to implement effective monitoring systems to detect suspicious transactions, meeting the requirements of AML legislation in the Republic of Kazakhstan.

Research by the FATF organization on the adoption of new technologies to meet AML/CFT standards has found that technologies such as artificial intelligence and application programming interfaces have the best outcome for customer due diligence [2].

The authors conclude that the field of financial AML monitoring is increasingly adopting artificial intelligence, which demonstrates fundamental abilities in solving financial and economic problems. By applying tools based on AI and machine learning, it becomes possible to analyze data quickly and accurately in real time, which can help solve problems related to the involvement of citizens in illegal financial transactions, as well as the misuse of personal data. However, apart from the positive side of using AI technologies in AML systems, there are risks ranging from data confidentiality issues to the quality of data sets and interpretability of AI models.

However, the positive experience of foreign countries has shown that the use of monitoring systems with the application of AI gives fast and effective results, helping to fight fraud and involvement of people in money laundering. This experience can be applied to the national financial system of the Republic of Kazakhstan.

Discussion

The ever-changing regulatory landscape, coupled with the increasing incidence of money laundering offences, has highlighted the need for better equipment with technologies to counter this offence [3]. Therefore, in order to achieve results, it is necessary to introduce new existing, low-cost and effective technologies that have the potential to improve anti-money laundering measures. Moreover, these measures are aimed at improving the quality of implementation of the FATF International Standards.

As early as 2021, the FATF has focused on such AI compliance tools in AML by publishing a handbook on "Opportunities and Challenges of New Technologies for AML/CFT". This publication contains the concept of AI, which is defined as a science that mimics human thinking abilities to perform tasks that normally require human intelligence, such as recognizing patterns, making predictions, recommendations or decisions [4]. AI, which uses advanced computational techniques to derive information from different types, sources, and quality (structured and unstructured) of analytical data to "autonomously" solve problems and perform tasks, has also been explored.

In the previously published article by Sidorova N.V. and the authors of this article it was noted that informatization and digitalization are already being introduced into various spheres of functioning of the state and society, using artificial intelligence, at a higher quality level [5; 82]. Government agencies and large corporations are using new AI technologies to protect citizens' personal data, especially in the banking sector. For example, due to biometric authentication, accelerated threat detection and prompt response to attacks with the help of AI security software embedded in applications, the safety of personal data is ensured and their leaks are prevented [6; 152].

Consider the strengths and weaknesses of using AI for anti-money laundering purposes. In terms of the benefits of AI for AML monitoring, AI allows for more sensitive and broader analysis, which radically expands the ability to assess money laundering risks. By using sophisticated algorithms, AI tools enable AML compliance to better understand money laundering risks, allowing for identification and analysis of illegal activity, providing a real digital solution. These digital AML tools can process huge amounts of data in a short period of time to gain insights into patterns and anomalies that may indicate the presence of money laundering or other financial crimes, which is quite difficult, time-consuming and labor-intensive for a typical individual. Artificial intelligence has great potential for automation, supporting fast processes and efficient workflows that enable professionals to perform higher-level tasks.

However, the introduction and application of new technologies in the AML system are associated with certain difficulties and problems, which are either regulatory or operational in nature. This is mentioned in the Concept for the Development of Financial Monitoring for 2022–2026, which notes that combating money laundering is one of the priority tasks for the financial sector since almost all financial monitoring subjects are involved in this illegal activity. The situation is aggravated by insufficient information work and a lack of systematic training in AML and the financial security of citizens [2].

It should also be noted that the introduction of AI into AML involves significant risks that need to be carefully considered. A recent IMF report showed that artificial intelligence, especially generative AI, poses a significant risk to the financial system [7]. These threats include data privacy breaches, bias in AI algorithms, the risk of inaccurate predictions and conclusions, and potential system failures due to cyberattacks that could contribute to inaccurate information.

However, despite all the risks, integrating AI into financial systems to prevent fraud is important for citizens, financial organizations and the country as a whole.

In recent years, Kazakhstan has seen an increase in the number of people involved in fraudulent money laundering schemes, including people mostly from vulnerable groups, such as students, unemployed, retirees and others. Such persons are called "Droppers" — people, who are used by fraudsters for registration of bank cards and accounts on them for subsequent withdrawal of criminally obtained funds. This is mostly money from drug trafficking, cyber fraud, illegal gambling activities and other crimes. Fraudsters often place adverts for remote work with high income, send offers via email, messengers and social networks. Dropper accounts are used to transfer and cash out money, for which they receive a certain reward, not realizing all the consequences of their role in criminal fraud due to ignorance of possible administrative and criminal liability. In 2024, the FMA of the Republic of Kazakhstan established facts of use for laundering criminal proceeds of 6.2 thousand "drop cards" with a total turnover of 24 billion tenge [8].

Droppers can be divided into two groups, those who gave their account details in explicit way and those who participated in the criminal scheme unconsciously. In the first case, citizens are aware of the possible

liability and, due to frivolity and quick flow of money, intent to participate in the crime increases significantly, making victims to follow their fraudulent schemes. Individuals who are unaware that they are assisting fraudsters typically receive a message regarding an "erroneous transfer" and, at the sender's request, return the funds to another (fraudulent) account, the details of which are provided by the perpetrators. Despite the absence of criminal intent, such citizens will find it difficult to prove to the police that they are not part of a criminal scheme.

Participation in such schemes can have serious consequences, including confiscation of property, and administrative and criminal penalties. Also, citizens participating as droppers may suffer reputational damage in the banking sector, which may affect, for example, further obtaining a mortgage or loan.

For example, a ruling of the Judicial Collegium for Civil Cases of the Supreme Court of the Republic of Kazakhstan satisfied the claim of Mr T. to recover over 20 million tenge from the "droppers". The court found that Mr T, misled by the fraudsters, transferred the above amount to the accounts and cards of four Kazakhstan citizens. The latter, in turn, not fully realizing the criminal origin of the money received, transferred it to unidentified persons as previously agreed. Given that the "droppers" did not take measures to find out the reasons for the receipt of the money and transferred it to other persons, the court considered these actions as the disposal of them at their discretion and therefore ordered to return the received unjustified remuneration [9].

Regarding material liability, this recovery is possible based on Article 953 of the Civil Code of the Republic of Kazakhstan on unjust enrichment [10]. In practice, there are existing cases in which droppers are obliged to pay money to victims of fraud, even if they did not realize their actions. As of the end of 2024, claims from 83 victims for more than 160 million tenge have been filed with the courts, of which 52 have already been satisfied. For example, in the Kostanai region, two civil lawsuits were pending against 19-year-old students who were used by fraudsters for their purposes and the plaintiffs demanded to recover more than 9 million each [11].

Criminal liability can occur only for deliberate complicity in fraudulent actions under Article 28, 190 of the Criminal Code and provides up to 10 years of imprisonment [12]. Currently, the Criminal Code of the Republic of Kazakhstan does not provide a special article for "droppers".

However, the Prime Minister of the Republic of Kazakhstan Bektenov O.A., reported that the interdepartmental working group under the Ministry of Justice is developing the introduction of criminal liability for the group of "droppers" [13]. Criminals engage droppers to transfer money to their personal accounts, thereby making them complicit in the offence and criminally liable. It is also important to remember that the main responsibility for laundering and cashing illegal funds falls on the owner of the account through which these funds pass.

This surge in fraud in the country has been fueled by the low awareness of citizens in the field of anti-fraud and money laundering. Therefore, the government now needs to take practical steps to protect citizens by organizing interaction between banks and other organizations, regulators and law enforcement agencies.

One of the methods of fighting scams is anti-fraud systems, which perform their functions on predefined algorithms, helping to identify suspicious transactions in real time. Fraud is unauthorized actions aimed at deceiving users and illegally obtaining benefits. Modern anti-fraud systems use artificial intelligence to analyze huge data sets. Such systems are particularly effective in analyzing complex, non-linear relationships and are able to identify new methods of crime that may not be visible to humans. For example, they detect suspicious activity and help block a ford even before fraudsters do any damage. These systems detect, for example, unusual transaction times and locations, suspicious transfer amounts, or activity in time zones that are atypical for the user.

Since persons (groups of persons) committing fraudulent schemes to obtain unjustified income have certain, similar qualities and attributes, AI "biometrics" algorithms can identify them and prevent offences. This helps law enforcement officials to carry out a quick and complete investigation of economic crimes. Nevertheless, it should be noted that AI is only a tool for law enforcement agencies and cannot replace them yet [14; 228].

AI technologies can be used to detect unknown malware, automatically classify threats and respond to them independently by feeding data to a control center. Domestic scientists such as Sydykova S. Zh., Akhmetov A.A., Sardarbekova A.K. noted that with the help of artificial intelligence based on machine learning, new technologies are created that are constantly learning, collecting new information and regulating processes, which allows for solving the ever-growing problem of data density in AML. Such AI technologies

help to identify suspicious customer transactions that are quite difficult to detect by applying rules or human resources alone [15; 132].

AI is now being actively used for financial services. There are fintech chatbots that help customers manage accounts, track spending and receive financial advice. These chatbots can assist citizens in obtaining fast and reliable information about suspicious transfers, and the account to which they intend to transfer their funds, to secure their money and minimize the risks of being involved in fraudulent schemes.

It may also be noted that several functioning platforms for detecting fraudulent activities, such as FICO Falcon Platform and SAS Fraud Management, which use artificial intelligence and machine learning to analyze transactions and identify suspicious activity [16].

Also notable is a Cambridge-based startup called "Featurespace", which has developed its ARIC Risk Hub to monitor transactions and detect fraudulent transactions using advanced machine learning models. ARIC Risk Hub utilizes advanced, explainable anomaly detection, allowing customers to automatically identify risks, detect new attacks, and detect suspicious activity in real time [17].

An advanced AI tool called MuleHunter.AI, which has been developed by the Reserve Bank of India's (RBI) Special Innovation Unit, Reserve Bank Innovation Hub (RBIH), has emerged as a successful case study in the fight against fraud. The technology specializes in detecting and identifying "mule" accounts that are often used for money laundering and has already been piloted in two public sector banks in the country [18].

In the Russian Federation, second-tier banks, such as Tinkoff Bank, Sberbank and VTB use a recently created drop monitoring system that, based on the analysis of a large number of transactions, compiles scenarios of customer behavior and a portrait of the "dropper" to identify suspicious transactions and conduct additional checks [19].

Analyzing foreign experience of introducing AI into anti-fraud and anti-money laundering systems allows us to conclude that such tools are necessary to improve the current system and contribute to the effective prevention of emerging threats, which ensures a safe and secure environment for the entire state.

It should be noted that the Republic of Kazakhstan is making significant steps to prevent fraud in the country. At the moment, the Anti-Fraud Centre of the National Bank has already been created, which is working to identify and prevent fraudulent transactions. For six months of work it has already registered about 18 thousand incidents. The Centre has blocked fraudulent transactions totaling about 1.5 billion tenge [20]. All second-tier banks and leading microfinance institutions are connected to the Antifraud Centre.

Therefore, it is advisable to consider the possibility of applying foreign experience in the creation and implementation of Kazakhstan's monitoring systems based on artificial intelligence technology, which will allow for effectively combating financial threats, detecting money laundering and other suspicious transactions.

Conclusions

Countering money laundering threats is crucial as they are constantly evolving, posing significant risks to the integrity and stability of the financial system, requiring proactive measures. Therefore, a relevant tool to help combat this problem is the application of artificial intelligence. AI has the potential to improve the accuracy and efficiency of measures to detect and prevent suspicious activity, thus countering new ways of money laundering. While machine learning alone will not solve the money laundering problem, it is a tool that significantly improves the efficiency and effectiveness of AML processes.

Innovative artificial intelligence technologies are facilitating more accurate risk assessment in digital identification and monitoring, assessing risks in a cost-effective manner and streamlining customer due diligence processes. A distinctive feature of these technologies is their ability to process large amounts of information in record time, sometimes beyond human capabilities, transferring data to others in simple and reliable ways, as a result of data standardization. However, the application of AI carries risks that can affect the correctness of decisions made, the reliability of information and the loss of sensitive data.

The study found that AI has revolutionized fraud prevention by offering advanced technologies that increase the effectiveness of fraud detection and prevention efforts. The implementation of these techniques can enable the Republic of Kazakhstan to better respond to new risks and improve the financial well-being of citizens due to the increasing involvement of citizens in fraudulent money laundering schemes.

References

1 Financial Action Task Force. FATF Recommendations: International standards on combating money laundering, terrorist financing and financing the proliferation of weapons of mass destruction. — 2023. — [Electronic resource]. — Access mode: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

2 Указ Президента Республики Казахстан от 6 октября 2022 года № 1038 «Об утверждении Концепции развития финансового мониторинга на 2022–2026 годы». — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/U2200001038

3 Ray A. Emerging Solutions in Anti-Money Laundering Technology — [Electronic resource]. — Access mode: http://celent.com/reports/emerging-solutions-anti-money-laundering-technology

4 ФАТФ. Возможности и проблемы новых технологий для ПОД/ФТ. — 2021. — [Электронный ресурс]. — Режим доступа: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html

5 Сидорова Н.В. Искусственный интеллект как правовая категория и объект правового регулирования [Электронный ресурс] / Н.В. Сидорова, Н.О. Дулатбеков, Л.К. Кусаинова // Вестн. Караганд. ун-та. — 2024. — № 3. — С. 78–90. — Режим доступа: https://doi.org/10.31489/2024l3/78-90

6 Афанасьева Д.В. Применение искусственного интеллекта в обеспечении безопасности данных [Электронный ресурс] / Д.В. Афанасьев // Известия Тульского государственного университета. Технические науки. — 2020. — № 2. — С. 151–154. — Режим доступа: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-obespechenii-bezopasnosti-dannyh

7 Shabsigh G. Generative Artificial Intelligence in Finance: Risk Considerations, in NOTE/2023/006, 2023, International Monetary Fund. — [Electronic resource] / G. Shabsigh, E.B. Boukherouaa. — Access mode: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570

8 Пресс служба АФМ РК. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/afm/press/news/details/915000?lang=ru

9 Пресс-служба Генеральной прокуратуры. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/prokuror/press/news/details/765459?lang=ru

10 Гражданский кодекс Республики Казахстан (Особенная часть) от 1 июля 1999 года № 409-I. — [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=1013880

11 Пресс-службы Костанайской и Кызылординской облсудов. Суды указали на незаконность обогащения дропперов. — [Электронный ресурс]. — Режим доступа: https://sud.gov.kz/rus/news/sudy-ukazali-na-nezakonnost-obogashcheniya-dropperov

12 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. — [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=31575252&pos=5;-106#pos=5;-106

13 Ответ на депутатский запрос Премьер-Министра Республики Казахстан Бектенова Олжаса Абаевича от 08.10.2024, №16-13-3 Д/С. — [Электронный ресурс]. — Режим доступа: https://senate.parlam.kz/storage/e8a60a9d2c6e4c3086d4c4f8eb1e9348.pdf

14 Дятлова А.Ф. Технологии искусственного интеллекта в сфере экономической безопасности [Электронный ресурс] / А.Ф. Дятлова, В.С. Свирина // Вестник Московского университета МВД России. — 2024. — № 2. — С. 227–232. — Режим доступа: https://doi.org/10.24412/2073-0454-2024-2-227-232

15 Сыдыкова С.Ж. Влияние искусственного интеллекта на противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма / С.Ж. Сыдыкова, А.А. Ахметов, А.К. Сардарбекова // Финансовая безопасность. Современное состояние и перспективы развития: материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ (14-15 декабря 2022 года). — Москва: Национальный исследовательский ядерный университет «МИФИ», 2022. — Т. 1. — С. 129–137. — EDN: VLBJLC.

16 Чебуханова Л.В. Искусственный интеллект и его влияние на трансформацию финансовых инструментов [Электронный ресурс] / Л.В. Чебуханова // Вестник Академии знаний. — 2024. — № 5 (64). — С. 486–491.— Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ego-vliyanie-na-transformatsiyu-finansovyh-instrumentov

17 Featurespace's official website. — [Electronic resource]. — Access mode: https://www.featurespace.com/

18 What is MuleHunter.ai, RBI's latest initiative to tackle financial frauds. — [Electronic resource]. — Access mode: https://www.businesstoday.in/personal-finance/banking/story/what-is-mulehunterai-rbis-latest-initiative-to-tackle-financial-frauds-456480-2024-12-06

19 Крупные банки запускают системы дроп-мониторинга. — [Электронный ресурс]. — Режим доступа: https://frankmedia.ru/162977?utm_referrer=https%3a%2f%2fwww.google.com%2f

20 Пресс-центр Национального банка РК. — [Электронный ресурс]. — Режим доступа: https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/17388

Л.К. Кусаинова, М.Г. Альбекова, Н.О. Дулатбеков

AML саласындағы ЖИ: инновациялық тәсілдер және халықтың қаржылық сауаттылығын арттыру әлеуеті

Зерттеудің мақсаты — ақшаны жылыстатумен (AML) күресу үшін жасанды интеллекті (ЖИ) пайдалану мүмкіншіліктерін талдау және алаяқтықтың алдын алу мен ақшаны жылыстатуға қатысуын болдырмау мақсатында азаматтардың қаржылық сауаттылығын арттыру үшін ЖИ әлеуетін зерттеу. Заманауи технологиялардың дамуымен қылмыс жасау тәсілдері айтарлықтай өзгерді, күрделене түсті және түрленді, әсіресе бұл күнделікті жасалатын ауқымды кибершабуылдарға қатысты. Сондықтан, қазіргі жағдайда жаңа қауіптерге тез жауап бере алатын тиімді технологиялық шешімдерді қолдану қажеттілігі туындап отыр. Осындай әдістердің бірі көптеген салаларда кеңінен қолданылып жүрген ЖИ технологиялары және AML-де тыс қалған жоқ. Зерттеу барысында, AML талаптарын орындау саласында жасанды интеллекті пайдаланудың артықшылығы оның нақты уақыт режимінде мониторинг пен талдауға жасауға мүмкіндік беретіні ең басты функционалдығы екендігі анықталды. Бұл, азаматтар саналы түрде де, бейсаналық түрде де қатысатын ықтимал қауіпті немесе ықтимал заңсыз әрекеттерді анықтауға және азаматтар мен мемлекетті қорғау мақсатында мұқият тергеу жұмыстарын жүргізуге мүмкіндік береді. Авторлар зерттеу нәтижесінде мынадай негізгі қорытынды жасаған: ақшаны жылыстату бойынша күдікті операцияларды анықтау, хабарлау және жолын кесу үшін, шетелдік тәжірибеге сүйене отырып жасалған Қазақстан Республикасының AML жүйесіне ЖИ енгізу бойынша практикалық ұсыныстарын беру.

Кілт сөздер: ақшаны жылыстату, жасанды интеллект, цифрлық технологиялар, антифрод, азаматтардың қаржылық қауіпсіздігі, алаяқтық.

Л.К. Кусаинова, М.Г. Альбекова, Н.О. Дулатбеков

ИИ в сфере AML: инновационные подходы и потенциал повышения финансовой грамотности населения

Цель данного исследования — проанализировать использование искусственного интеллекта (ИИ) для борьбы с отмыванием денег (AML) и изучить потенциал ИИ для повышения финансовой грамотности граждан с целью предотвращения мошенничества и участия в отмывании денег. С развитием современных технологий способы совершения преступлений значительно усложнились и трансформировались, особенно это касается масштабных кибератак, которые совершаются ежедневно. Поэтому в нынешних реалиях необходимо использовать эффективные технологические решения, которые способны быстро реагировать на новые угрозы. Одним из таких способов является применение технологий искусственного интеллекта (ИИ), который повсеместно применяется во многих отраслях, и AML не является исключением. В рамках исследования установлено, что преимущество использования искусственного интеллекта в сфере соблюдения требований AML заключается в его функциональности, позволяющей осуществлять мониторинг и анализ в режиме реального времени. Это позволяет обнаружить потенциальную угрозу или возможную противоправную деятельность, в которой участвуют граждане как сознательно, так и бессознательно, также провести тщательное расследование с целью защиты граждан и государства. Основной результат, к которому пришли авторы, заключается в практических предложениях, основанных на зарубежном опыте, по внедрению ИИ в AML системы Республики Казахстан для обнаружения, сообщения и пресечения подозрительных операций по отмыванию денег.

Ключевые слова: отмывание денег, искусственный интеллект, цифровые технологии, анти-фрод, финансовая безопасность граждан, мошенничество

References

1   (2023). Financial Action Task Force. FATF Recommendations: International standards on combating money laundering, terrorist financing and financing the proliferation of weapons of mass destruction. *fatfgafi.org.* Retrieved from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

2   Ukaz Prezidenta Respubliki Kazakhstan ot 6 oktiabria 2022 goda № 1038 «Ob utverzhdenii Kontseptsii razvitiia finansovogo monitoringa na 2022–2026 gody» [Decree of the President of the Republic of Kazakhstan from 6 October 2022 No 1038 "On approval of the Concept of development of financial monitoring for 2022–2026"]. (2022, 6 October). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/U2200001038 [in Russian].

3 Ray, A. Emerging solutions in anti-money laundering technology. *celent.com.* Retrieved from http://celent.com/reports/emerging-solutions-anti-money-laundering-technology

4   (2021). FATF. Vozmozhnosti i problemy novykh tekhnologii dlia POD/FT [FATF. Opportunities and Challenges of New Technologies for AML/CFT]. *fatf-gafi.org.* Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html [in Russian].

5   Sidorova, N.V., Dulatbekov, N.O., & Kusainova, L.K. (2024). Iskusstvennyi intellekt kak pravovaia kategoriia i obiekt pravovogo regulirovaniia [Artificial Intelligence as a Legal Category and Object of Legal Regulation]. *Vestnik Karagandinskogo universiteta — Bulletin of Karaganda University,* 3, 78–90. Retrieved from https://doi.org/10.31489/2024l3/78-90 [in Russian].

6   Afanasyeva, D.V. (2020). Primenenie iskusstvennogo intellekta v obespechenii bezopasnosti dannykh [Application of Artificial Intelligence in Ensuring Data Security]. *Izvestiia Tulskogo gosudarstvennogo universiteta. Tekhnicheskie nauki — Bulletin of Tula State University. Technical Sciences,* 2, 151–154 [in Russian].

7   Shabsigh, G., & Boukherouaa, E.B. (2023). Generative artificial intelligence in finance: Risk considerations. NOTE/2023/006, International Monetary Fund. *imf.org.* Retrieved from https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570

8   Press-sluzhba AFM RK [Press service of AFM RK]. *gov.kz.* Retrieved from https://www.gov.kz/memleket/entities/afm/press/news/details/915000?lang=ru [in Russian].

9   Press-sluzhba Generalnoi prokuratury [Press-service of the General Prosecutor's Office]. *gov.kz.* Retrieved from https://www.gov.kz/memleket/entities/prokuror/press/news/details/765459?lang=ru [in Russian].

10 Grazhdanskii kodeks Respubliki Kazakhstan (Osobennaia chast) ot 1 iiulia 1999 goda № 409-I [Civil Code of the Republic of Kazakhstan (Special Part) No 409-I of 1 July 1999]. (1999, 1 July). *online.zakon.kz.* Retrieved from https://online.zakon.kz/Document/?doc_id=1013880

11 Press-sluzhby Kostanaiskoi i Kyzylordinskoi oblsudov «Sudy ukazali na nezakonnost obogashcheniia dropperov» [Press-services of Kostanay and Kyzylorda oblast courts "Courts pointed out the illegality of enrichment of droppers"]. *sud.gov.kz.* Retrieved from https://sud.gov.kz/rus/news/sudy-ukazali-na-nezakonnost-obogashcheniya-dropperov [in Russian].

12 Ugolovnyi kodeks Respubliki Kazakhstan ot 3 iiulia 2014 goda № 226-V [Criminal Code of the Republic of Kazakhstan from 3 July 2014 No 226-V]. (2014, 3 July). *online.zakon.kz.* Retrieved from https://online.zakon.kz/Document/?doc_id=31575252&pos=5;-106#pos=5;-106 [in Russian].

13 Otvet na deputatskii zapros Premer-Ministra Respubliki Kazakhstan Bektenova Olzhasa Abaevicha ot 08.10.2024, №16-13-3 D/S [Response to the deputy enquiry of the Prime Minister of the Republic of Kazakhstan Bektenov Olzhas Abayevich from 08.10.2024, №16-13-3 D/S]. (2024, 8 October). *senate.parlam.kz.* Retrieved from https://senate.parlam.kz/storage/e8a60a9d2c6e4c3086d4c4f8eb1e9348.pdf [in Kazakh].

14 Dyatlova, A.F., & Svirina, V.S. (2024). Tekhnologii iskusstvennogo intellekta v sfere ekonomicheskoi bezopasnosti [Artificial intelligence technologies in the field of economic security]. *Vestnik Moskovskogo universiteta Ministerstva vnutrennikh del Rossii — Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* 2, 227–232. Retrieved from https://doi.org/10.24412/2073-0454-2024-2-227-232 [in Russian].

15 Sydykova, S.Zh., Akhmetov, A.A., & Sardarbekova, A.K. (2022). Vliianie iskusstvennogo intellekta na protivodeistvie otmyvaniiu dokhodov, poluchennykh prestupnym putem, i finansirovaniiu terrorizma [The impact of artificial intelligence on combating money laundering and terrorist financing]. *Finansovaia besopasnost. Sovremennoe sostoianie i perspektivy razvitia: materialy VIII Mezhdunarodnogo nauchno-prakticheskoi konferentsii Mezhdunarodnogo setevogo instituta v sfere POD/FT (14-15 dekabria 2022 goda) — Financial Security: Current State and Development Prospects: Proceedings of the VIII International Scientific and Practical Conference of the International Network Institute in the field of AML/CFT Security — Current state and prospects of development* (pp. 129–137). Moscow: Natsionalnyi issledovatelskii yadernyi universitet «Moskovskii Inzhenernyi Finansovyi Institut» [in Russian].

16 Chebukhanova, L.V. (2024). Iskusstvennyi intellekt i ego vliianie na transformatsiiu finansovykh instrumentov [Artificial intelligence and its impact on the transformation of financial instruments]. *Vestnik Akademii znanii — Bulletin of the Academy of Knowledge,* 5(64), 486–489. Retrieved from https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ego-vliyanie-na-transformatsiyu-finansovyh-instrumentov [in Russian].

17 Ofitsialnyi sait Featurespace. *featurespace.com.* Retrieved from https://www.featurespace.com/

18 Shto takoe MuleHunter.ai, posledniaia initsiativa RBI po borbe s finansovymi moshennichestvami [What is MuleHunter.ai, RBI's latest initiative to tackle financial frauds]. *businesstoday.in.* Retrieved from https://www.businesstoday.in/personal-finance/banking/story/what-is-mulehunterai-rbis-latest-initiative-to-tackle-financial-frauds-456480-2024-12-06

19 Krupnye banki zapuskaiut sistemy drop-monitoringa [Large banks launch drop-monitoring systems]. *frankmedia.ru.* Retrieved from https://frankmedia.ru/162977?utm_referrer=https%3a%2f%2fwww.google.com%2f [in Russian].

20 Press-tsentr Natsionalnogo banka RK [Press center of the National Bank of Kazakhstan]. *nationalbank.kz.* Retrieved from https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/17388 [in Russian].

Information about the authors

Kusainova Larisa Kanatovna —Professor of the Department of Criminal Law, Procedure and Criminalistics, Karaganda Buketov University, Karaganda, Kazakhstan; e-mail: Klarisa_777@mail.ru

Albekova Madina Gairatovna — Senior Lecturer, PhD. Student of the Department of Criminal Law, Procedure and Criminalistics, Karaganda Buketov University, Karaganda, Kazakhstan; e-mail: albekova_m@mail.ru

Dulatbekov Nurlan Orynbasarovich — Chairman of the Board — Rector of Karaganda Buketov University, Karaganda, Kazakhstan; e-mail: office@buketov.edu.kz