UDC 004.56

N.A. Lukashuk PhD, Associate Professor;
V.P. Pirogovskiy, student (BSTU, Minsk)

CYBER SECURITY IN FINANCIAL SPHERE: ESSENCE AND APPLICATION OF ARTIFICIAL INTELLIGENCE

In the Republic of Belarus, a legal basis for the creation and operation of a national cyber security system has been defined, which is aimed at forming a comprehensive multi-level mechanism to counter cyber attacks, on government agencies and organizations, and critical information infrastructure [1].

By information security we mean the state of protection of the information space, information infrastructure and information resources from external and internal threats in the information sphere [2].

In 2017, the National Bank of the Republic of Belarus, based on blockchain technology, implemented applied tasks for maintaining registers of issued bank guarantees, as well as forming a register of transactions on securities, and created a center for monitoring and countering cyber attacks in the credit and financial sector (FinCERTby) [3].

Recently, in the Republic of Belarus, as well as in the world as a whole, cyber security problems in the financial sector have increased.

In 2024, fraudsters began to use artificial intelligence more often for complex multi-stage cyber attacks. The situation is worsened by the fact that hackers have developed specializations: target designation, searching for vulnerable resources, supplying the necessary means of attack, exploiting vulnerabilities and gaining access to infrastructure, exchanging attack results. Attackers continue to actively recruit insiders to gain access to organizations' networks and copy critical data [4].

As noted in the media, citizens and the state suffer from financial cyber crimes; cyber criminals having access to personal data extort money from individuals. An important area of work is interaction with global cyber partners for the effective exchange of information and experience in combating threats emanating from cyber space [5].

A new development in the fight against cyber extortionists was proposed by the British mobile operator O2. An artificial intelligence named Daisy (or dAIsy) imitates the most popular target among telephone scammers – an elderly woman [6]. The system can work around the clock without any human intervention. The scheme is as follows: first, the artificial intelligence converts the scammer’s voice into text, and then, using a special speech model with the character of a grandmother, generates a response also in text form, and then voices it.

During the conversation, the AI provides fraudsters with false banking data and asks dozens of ridiculous follow-up questions. Such conversations can last 40 minutes or longer – the technology is close to reality, which makes it difficult to quickly identify. In addition, Daisy numbers were specifically added to the list of "easy targets" for fraudsters [6].

The use of AI in the financial sector is becoming increasingly widespread, offering new opportunities for data protection and fraud prevention, as this is where huge amounts of theft occur. Here are the main applications:

1. Anti-fraud systems. AI is actively used to detect and prevent fraud. Machine learning algorithms analyze transactions in real time, identifying suspicious actions and anomalies. This allows banks to quickly respond to potential threats and prevent financial losses.

2. Customer behavior analysis. AI helps create customer behavior profiles, which helps identify unusual or suspicious activity. For example, if a customer suddenly starts making large transfers or using the card in unusual places, the AI system can recognize this as a potential threat and block the transaction until the circumstances are clarified.

3. Protecting personal data: AI helps protect customers' personal data using advanced encryption and authentication methods. This includes biometric authentication such as facial recognition and fingerprints, making access to data more secure.

Biometric authentication uses a person's unique physical or behavioral characteristics to verify their identity. AI improves the accuracy and reliability of these systems:

– Face recognition: AI analyzes facial features such as the distance between the eyes, the shape of the nose, and the contours of the jaw to identify a person. Modern deep learning algorithms allow achieving high accuracy even in low-light conditions or when the appearance changes;

– Fingerprint recognition: AI improves fingerprint recognition accuracy by analyzing the smallest details, such as pores and lines on the skin. This allows for more reliable authentication systems that are difficult to fool;

– Iris recognition: AI analyzes the unique patterns on the iris of the eye, which remain unchanged throughout a person's life. This method is considered one of the most reliable and secure for authentication;

– Voice recognition: AI uses the acoustic characteristics of a voice, such as timbre, pitch and intonation, to identify a person. This allows the creation of voice authentication systems that can be used in various applications, from banking services to smart homes;

– Combined systems: AI allows you to integrate several biometric methods into one system, which significantly increases the level of security. For example, the system can simultaneously use face and fingerprint recognition to authenticate the user;

– Data protection: AI helps protect biometric data using advanced encryption and authentication methods. This includes protection against counterfeiting and unauthorized access.

The use of AI in biometric authentication has a number of advantages: high accuracy; convenience; security. Despite its many benefits, the use of AI in biometric authentication also faces challenges such as data protection and ethical issues.

4. Ethical and legal standards. It is important to ensure that AI is used responsibly and does not violate the rights of customers. This includes protecting data privacy and preventing discrimination.

Conclusion: AI in the financial sector is thus a powerful tool for data protection and fraud prevention. However, its use requires careful consideration and ethical standards. Development prospects include improving algorithms, integrating with other technologies, and developing new data protection methods. This will allow for even more reliable and secure authentication systems in the future. Combining AI technologies with cyber security strategies will help create more resilient and effective defense systems against cyber threats.

LITERATURE

1. O cyber security: Decree of the President of the Republic of Belarus No. 40 of 14.02.23 – URL: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g (date of access: 01.01.2025) –_11 p.

2. On approval of the Concept of National Security of the Republic of Belarus : Decision of the All-Belarusian People's Assembly of April 25, 2024 No. 5 // National Legal Internet Portal of the Republic of Belarus, 04/26/2024, 1/21360 – URL : https://pravo.by/document/?guid=11031&p0=P924v0005 – (date of access : 15.01.25)

3. Concept of the State Program "Digital Development of Belarus" for 2021–2025. – 49 p.

4. Cyber security in Belarus and Russia: experts discuss current challenges and solutions at Cyber security Forum 2024 – URL : https :// mdait . by / newsroom / cyber - security - forum -2024/ (date of access : 20.01.25)

5. False leader and other methods of deception – the police explained how cyber fraudsters operate – URL : https :// www . sb . by / articles / lzherukovoditel - i - drugie - sposoby - obmana - v - militsii - rasskazali - kak - deystvuyut – cyber scammers . html (date of access : 29.01.25)

6. AI has learned to imitate the communication style of grandmothers and is now driving scammers crazy – URL : https :// tech . onliner . by /2024/11/17/ ii - learned - imitate –style - communication - grandmothers - and – now – lead – cheaters (date of access : 29.01.25)