UDK 338:004
DOI

Baimukhamedova A.M.,
senior lecturer, djanin50@gmail.co[1]

Baimukhamedov M.F.,
Doctor of Technical Sciences, professor,
bmf45@mail.ru[2]

Aimurzinov M.S.,
Candidate of Economics Sciences, professor,
ams-66@mail.ru [2]

Gazi University
Turkiye, Emniyet Provincem, Bandirma st., 6/1[1]

Kostanay Social and Technical University
named after academician Z. Aldamzhar,
110000 Kostanay, ave. Koblandy Batyr, 27[2]

PROTECTION MEANS FOR ENSURING CYBERSECURITY OF THE ECONOMY OF KAZAKHSTAN BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract. *The scientific article reveals such an important and relevant topic today as the use of artificial intelligence technologies in the field of cybersecurity. The main areas of information protection, into which artificial intelligence modules are actively integrated, are analyzed. A concept of protection means using artificial intelligence based on existing domestic software is proposed, including for the purpose of ensuring the technological independence of the economy of the Republic of Kazakhstan. Based on an expert survey, the practical significance and feasibility of introducing protection systems based on artificial intelligence technologies in various sectors of the economy is confirmed. Recommendations for combating cybercrime in the economic sphere of Kazakhstan are proposed.*

Keywords: *economy, artificial intelligence, the Republic of Kazakhstan, cybersecurity, cyberattack.*

Introduction

Currently, the only domestic manufacturer of cybersecurity software in Kazakhstan that uses artificial intelligence (AI) technologies is MSSP Global, a Kazakhstani developer of products and solutions for information security and confidential data protection, producing tools for detecting malware. Our analysis of cybersecurity mechanisms in organizations of various industries showed that domestic solutions presented on the market are mainly fragmented: they are able to effectively counter certain types of cyber threats, but not all of their diversity, which does not allow them to be used to create a full-fledged cyberspace protection framework for an organization. For this reason, most large Kazakhstani enterprises have been actively using foreign-made security software for preventing cyberattacks and monitoring security based on artificial intelligence for many years, since a distinctive feature of foreign solutions was the high efficiency of detecting and blocking zero-day threats - threats against which protective mechanisms have not yet been developed [1]. The suppliers of this software were companies such as: Symantec, IBM, Cylance, Cisco and others.

In connection with these circumstances, Kazakhstan needs to develop its own set of information security tools, the functioning of which will be based on artificial intelligence. The need to use artificial intelligence in information security tools is due to the following reasons:

1) a shortage of specialists in the field of cybersecurity;

2) a significant increase in the volume of data processed by devices in recent years; 3) an 11-fold increase in the number of cyberattacks in March-September 2022 compared to the same period in 2021; 4) the use of AI technologies by attackers who are able to bypass security tools without using AI [2].

Methodology

There are 9 main areas of information security tools using AI technologies, which differ in usage scenarios and functional type. Fig. 1 shows all existing areas of protection and their share of the total number of products using AI technologies in the global cybersecurity market.

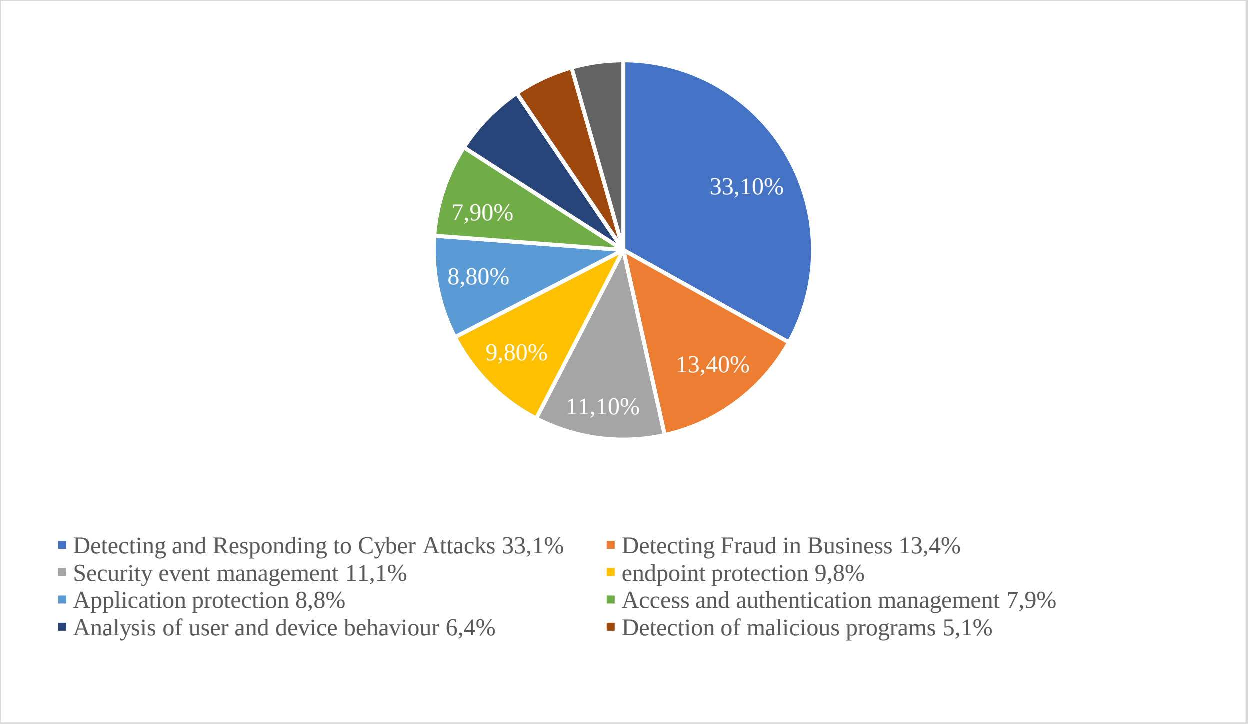

Fig. 1 – Distribution of products using AI technologies in the field of cybersecurity by use scenarios

According to Fig. 1, there is a significant preponderance of the share of cyberattack detection and response tools, which make up almost a third of the total number of AI-based protection tools, while malware detection tools (antiviruses) and anti-phishing tools, which were leaders in the cybersecurity market and were the most popular areas of protection just a few years ago, now collectively make up less than 10% of the total market share. These statistics confirm the high rate of development and change in cybersecurity trends and the need to use innovative technologies in its protection.

The use of all available types of protection tools will provide an opportunity to be protected from simple to the most complex attacks, but the cost of the necessary technical equipment for their maintenance may be too high for many critical information infrastructure (CII) facilities [3, 4], for which this set of tools is needed first and foremost, therefore, the proposed set of tools should use areas of protection that are suitable for most organizations in both the public and commercial sectors. For example, systems for detecting and preventing fraudulent transactions and threats in business processes are very useful for commercial enterprises, but for government agencies and most critical information infrastructure facilities, their use is impractical due to the small number or absence of business processes in their activities.

Results

The priority area in the proposed set of security tools will be the NDR (Network Detection and Response) cyberattack detection and response system. Its main task is to detect attacks in the network perimeter and promptly respond to them. The need to use this system is confirmed by its popularity in the global AI market, which accounts for 33.1% of the total number of security systems. The principle of operation of this system is to use generated and regularly updated databases of statistics and threats, continuously analyzed by artificial intelligence using deep learning technologies. As a result of the analysis of this data, the system determines threats in the network perimeter in advance and can automatically respond to them appropriately, changing the configuration of network devices and gateways.

The main difference from similar means of protection without the use of AI is the ability to build a model of potential threats, with the help of which it is possible to block even those attacks, the algorithm of which is not yet known to databases [5]. This is primarily necessary to repel cyberattacks that also use AI, because it is with its help that hackers bypass existing protection systems using the speed of modification of malicious files and the attack scenario in real time. An additional function of this system is the analysis of mail traffic for phishing, which eliminates the need to use a separate system to protect against it. According to research by the Capgemini Institute of Information Technology, 89% of organizations that have used AI technologies in systems for detecting and responding to cyberattacks report a reduction in response time and a decrease in the costs of detecting and preventing them. Statistical indicators of the effectiveness of AI in systems for detecting and responding to cyberattacks on organizations are given in Table 1.

Table 1 - Statistics on the reduction of costs for detecting and responding to cyberattacks using AI technologies

Indicators	Percentage of organizations reporting improvement in this indicator:	
	By 1-20%	More than 20%
Reducing the cost of vulnerability detection	54	29
Reducing the cost of restoring IT systems from cyber attacks	51	19
Reducing vulnerability detection time	53	35
Reducing cyber-attack neutralization time	65	20

The second direction in the proposed set of information security tools is the SIEM (Security Information and Event Management) security event management system. The main task of this protection direction is to monitor information systems, analyze security events in real time, emanating from network equipment, information security systems and network infrastructure, IT services and applications, which in turn help to detect information security incidents. The main advantage of using AI technologies in this system is the ability to detect abnormal behavior and reduce false positives when changing templates and data models.

The main problem with SIEM systems is their heavy dependence on experts to handle the data due to its complexity and the huge volume of data that experts cannot process. According to Escal Institute of Technology, the use of artificial intelligence in SIEM systems allows for a very high level of automation and eliminates the need to expand the staff of information security specialists [6].

The third direction is not the most popular on the world market, but a very popular system of behavioral analysis of users and information entities UEBA (User and Entity Behavior Analytics). Its task is to detect cases of unusual behavior in order to detect external and internal threats. Artificial intelligence technologies in this type of system help to automatically identify anomalies in user behavior models (deviation from the norm or compliance with the threat template) for various elements of information systems.

The detected anomalies are identified by artificial intelligence as various threats and risks to business. Detection of abnormal behavior can be used for the purposes of monitoring and access control, detecting fraud among clients or employees, protecting personal data, checking compliance with certain regulations and normative acts. UEBA systems simplify the work of security personnel by automatically solving a variety of tasks, based on the formed models of user behavior and other elements of information systems, with the subsequent identification of "black sheep", thereby determining [7]:

- unauthorized access and movement of data;
- suspicious behavior of privileged users;
- malicious activity of employees;
- non-standard access and use of cloud resources.

If we talk about the use of AI technologies in cybersecurity protection in general, without reference to a specific protection scenario, then according to a survey by the cybersecurity consulting company Osterman Research, which covered more than 100 organizations belonging to medium and large businesses and operating in various industries and services, 81% of companies that have started using software for various protection scenarios using AI technologies note an increase in the efficiency of incident investigation, detection and response speed to threats. Many respondents also pay attention to the reduction in the number of false positives. More detailed statistics on the improvement of security indicators are presented in Table 2.

Table 2 - Statistics on improvement of information security indicators after the use of AI technologies, %

Advantages	**All organizations**	**Organizations with a share of AI application less than 10%**	**Organizations with an AI application share of 10% or more**
Speed of threat detection	60	47	71
Increasing the efficiency of security departments	59	45	70
Automation of data sorting	47	39	53
Optimizing of Threat Detection	46	42	52
Reduced number of false alarms	37	26	51
Automatic system recovery after a cyber attack	22	16	29

As can be seen from the data in Table 2, even organizations that use AI relatively little in their own information security system note significant improvements from its use to detect various types of threats. At the same time, organizations with a higher share of AI technologies use record an almost 2-fold improvement in the value of the parameter "Automatic system recovery after a cyberattack", a significant increase in efficiency is also observed in the parameters "Rapidity of threat detection" and "Reduction in the number of false positives". As statistics show, organizations that actively use AI technologies to ensure protection against cyber threats can more adequately build the current activities of security departments on their basis and increase the efficiency of data sorting automation.

To assess the feasibility and effectiveness of implementing AI in ensuring cybersecurity, as well as identifying the most popular security systems, a survey was conducted among 25 employees working with network infrastructure and ensuring its security in organizations of various types. Table 3 presents a list of questions and possible answers.

Table 3 - List of questions and answer options for employees of information security departments

Question number	Question	Answer options
1	How many information security incidents do you encounter each month?	1) 0-1 2) 2-5 3) 6-10 4) More than 10
2	How many of the above incidents are cyber-attacks?	1) 0-25% 2) 26-50% 3) 51-75% 4) 76-100%
3	Do you use any security protection tools other than antivirus software?	1) Да 2) Нет
4	If you answered “no” to question 3, do you consider this security measure sufficient?	1) Да 2) Нет
5	What percentage of cyber-attacks are prevented before they cause damage?	1) 0-25% 2) 26-50% 3) 51-75% 4) 76-100%
6	On a scale of 1 to 10, how secure do you consider your network infrastructure to be against current threats?	1 – абсолютно не защищена, 10 – абсолютно защищена
7	Do you need additional staff to deal with current issues more effectively?	1) Yes, a significant expansion of staff is necessary 2) Yes, 1 or 2 additional employees are needed 3) No need
8	In your opinion, could more advanced security measures using AI technologies help you solve your current problems?	1) Yes 2) No 3) I find it difficult to answer
9	Since February 24, 2022, have you noticed a significant increase in cyberattacks on your organization?	1) Yes 2) No
10	On a scale of 1 to 10, how necessary is it to purchase additional software and equipment for its functioning in order to more effectively counteract current problems?	1 - not necessary, 10 - critically necessary

Source: own development

The results of this survey are shown in Table 4.

Table 4 - Results of the survey conducted regarding models of information and cyber security

Question No	Answer option and frequency of its selection, %				
1	0-1	2-5	6-10	more than 10	
	0	8	52	40	
2	0-25%	26-50%	51-75%	76-100%	
	0	4	24	72	
3	Yes	No			
	24	76			
4	Yes	No			
	28	**72**			
5	0-25%	26-50%	51-75%	76-100%	
	20	44	24	12	
6	1-2	3-4	5-6	7-9	9-10
	4	12	28	8	4
7	Yes, a significant expansion of staff is necessary	Yes, 1 or 2 additional employees are needed	No need		
8	Yes	12	0		
	80	No	I find it difficult to answer		
9	Yes	0	20		
	96	No			
10	1-2	4			
	0	3-4	5-6	7-9	9-10
		12	24	34	30

Source: own development

The following conclusions can be drawn from the results of this survey: 92% of respondents noted that they encounter an average of 8 or more information security incidents per month. An information security incident, according to respondents, is the occurrence of one or more undesirable or unexpected events that are associated with a significant probability of compromise and the creation of a threat to the security structure of the entire organization [8,9].

Conclusion

According to the results of processing the respondents' answers, in 79.5% of cases, these incidents are caused by cyber-attacks, not by the human factor (visiting suspicious sites, failure to comply with the organization's information security policy, etc.), while 76% of organizations use only antiviruses as a means of protection, the main purpose of which is to protect against incidents related to the human factor. 72% of specialists noted that using only an antivirus is not enough. Damage can be prevented on average only from 45.5% of attacks, the remaining 54.5% of attacks to one degree or another become an obstacle to the work process of the entire organization.

The statistics for the sixth question are noteworthy: 44% of employees found it difficult to answer this question, because they do not have sufficient competencies or cannot cover the entire infrastructure of the organization. Mostly, these employees work in large organizations with more than 10 servers and more than 100 personal computers. This fact indicates the need for an IT audit of large organizations. It should be noted that this problem is typical for all regions and organizations of various industry and departmental affiliations without exception. 100% of employees considered it necessary to expand the security staff, while 88% need a significant expansion of the staff, which also indicates the need to use AI, which will simplify the routine work of information security department employees. Also, 100% of employees familiar with AI technologies agree with their effectiveness and the feasibility of their use. 80% of all surveyed employees consider it necessary to strengthen existing security measures and use AI technologies in them to one degree or another. From the above statistical data, one can also draw a conclusion about the advisability of introducing AI into the work process of organizations of various profiles.

Thus, taking into account the absence of the above-mentioned areas of protection in the Kazakhstan market, as well as the provided statistics on the improvement of key indicators of enterprise security from cyberattacks, we can conclude that it is promising and feasible from a technical point of view to create a set of protection tools using artificial intelligence based on domestic software solutions.

REFERENCES

1 Bulavin A.V. On the approaches of the USA and China to ensuring cyberbullying // Society, politics, economics, law. - 2017. – № 3. – pp. 28-32.

2 Minbaleev A.V. Problems of using artificial intelligence in countering cybercrime / [Electronic resource] Access mode: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-iskusstvennogo-intellekta-v-protivodeystvii-kiberprestupnosti/viewer (date of application: 09.11.2022).

3 Namiot D.E., Ilyushin E.A., Chizhov I.V. Artificial intelligence and cyberse-curity / [Electronic resource] Access mode: https://cyberleninka.ru/article/n/is-kusstvennyy-intellekt-i-kiberbezopasnost/viewer (accessed: 09/18/2022).

4. Official website of the National provider of cybersecurity technologies Ros-telecom-Solar [Electronic resource] Access mode: https://rt-solar.ru / (accessed:10/21/2022).

5. Safonova M.F., Tsiplyaeva S.A.: Cybersecurity: Problems and solutions /

[Electronic resource] Access mode: https://cyberleninka.ru/article/n / kiberbezopas-nost-problem-i-resheniya/viewer (accessed: 09/21/2022).

6. Malik, T.N. Cybersecurity: problems and prospects. // Young scientist. - 2021. - No. 7 (349). - pp. 10-12. - URL: https://moluch.ru/archive/349/78602/.

7. Temirzhanova L.A. Cybersecurity in the Republic of Kazakhstan: problems, recommendations for countering cybertheft. // Young scientist. - 2019. - No. 15 (253). - pp. 119-122. - URL: https://moluch.ru/archive/253/58106/.

8. Kairzhanov E.I. Criminology. General part. Almaty: Rick, 2005. – 41 p.

9. Cybersecurity concept ("Cybershield of Kazakhstan") [Electronic resource]. — Access mode: http://adilet.zan.kz/kaz/docs/P1700000407

Баймухамедова А.М.,
аға оқытушы, djanin50@gmail.co[1]

Баймухамедов М.Ф.,
техника ғылымдарының докторы, профессор,
bmf45@mail.ru[2]

Аймурзинов М.С.,
экономика ғылымдарының кандидаты, профессор,
ams-66@mail.ru[2]

Гази университеті
Түркия, Емниет облысы, Бандырма көш., 6/1[1]

Академик З. Алдамжар атындағы
Қостанай әлеуметтік-техникалық университеті,
110000 Қостанай қ., Қобыланды батыр даңғылы, 27[2]

ҚАЗАҚСТАН ЭКОНОМИКАСЫ ҮШІН КИБЕР ҚАУІПСІЗДІК ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫ НЕГІЗІНДЕ ҚОРҒАНЫС ҚҰРАЛДАРЫ

Аңдатпа. *Бұл ғылыми мақалада киберқауіпсіздікте жасанды интеллект технологияларын пайдаланудың маңызды және өзекті тақырыбы қарастырылады. Жасанды интеллект модульдері белсенді түрде біріктірілген ақпараттық қауіпсіздіктің негізгі бағыттары талданды. Қолданыстағы отандық бағдарламалық жасақтама негізінде, оның ішінде Қазақстан Республикасы экономикасының технологиялық тәуелсіздігін қамтамасыз ету мақсатында, жасанды интеллектке негізделген қауіпсіздік шешімдерінің тұжырымдамасы ұсынылды. Сараптамалық сауалнама* *нәтижесінде жасанды интеллект технологиялары негізделген қауіпсіздік жүйелерін әртүрлі экономикалық салаларда енгізудің практикалық маңыздылығы мен орындылығын растайды. Қазақстанның экономикалық секторындағы киберқылмыспен күресу бойынша ұсыныстар берілді.*

Түйінді сөздер: *экономика, жасанды интеллект, Қазақстан Республикасы, киберқауіпсіздік, кибершабуыл.*

Баймухамедова А.М.,
старший преподаватель, djanin50@gmail.co[1]

Баймухамедов М.Ф.,
доктор технических наук, профессор,
bmf45@mail.ru[2]

Аймурзинов М.С.,
кандидат экономических наук, профессор,
ams-66@mail.ru [2]

Университет Гази
Турция, Провинция Эмниет, ул.Бандирма, 6/1[1]

Костанайский социально-технический университет
имени академика З.Алдамжар,
110000 г.Костанай, пр-т. Кобыланды Батыра, 27[2]

СРЕДСТВА ЗАЩИТЫ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ЭКОНОМИКИ КАЗАХСТАНА НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *В научной статье раскрывается такая важная и актуальная на сегодняшний день тема, как применение технологий искусственного интеллекта в сфере кибербезопасности. Проанализированы основные направления защиты информации, в которые активно интегрируются модули искусственного интеллекта. Предложена концепция средств защиты с использованием искусственного интеллекта на базе существующего отечественного программного обеспечения, в том числе в целях обеспечения технологической независимости экономики Республики Казахстан. На основе экспертного опроса подтверждена практическая значимость и целесообразность внедрения систем защиты на основе технологий искусственного интеллекта в различных отраслях экономики. Предложены рекомендации по борьбе с киберпреступностью в экономической сфере Казахстана.*

Ключевые слова: *экономика, искусственный интеллект, Республика Казахстан, кибербезопасность, кибератака.*