Cybercrime as a Threat to the Banking System of Ukraine and Cryptology as a Means of its Prevention

[1]Marian Bedrii [0000-0003-4021-1980], [1]Maryana Syrko [0000-0003-3150-9208]
[1]Oksana Stolyar [0000-0002-3995-8414], [2]Oleh Kuzmin [0000-0002-6014-6437],
[2]Yurii Kryvenchuk[0000-0002-2504-5833]

[1]Ivan Franko National University of Lviv 79007, Ukraine
[2]Lviv Polytechnic National University, Lviv 79013, Ukraine
marian.bedrii@lnu.edu.ua, maryana.syrko@lnu.edu.ua,
oksan.stolyar@gmail.com, oleh.y.kuzmin@lpnu.ua,
yurkokryvenchuk@gmail.com

Abstract. In Ukraine and around the world, tens of thousands of crimes are committed every year using information and communication technologies, software, software and hardware, other technical and technological means and equipment. Every day, people and companies are robbed of personal data, funds from accounts, collect a lot of confidential and commercial information, block activities, and so on. However, the success of preventing such crimes, exposing them and bringing the perpetrators to justice is currently a rather rare phenomenon compared to the number of such offenses. This is not surprising, because cyberspace is limitless, and experienced hackers have all the necessary skills and tools to remain incognito. Today, cyber attacks harm not only individuals and legal entities, but also the state. Every year, hundreds of events of various levels are held around the world to discuss current cybersecurity issues. New definitions are constantly appearing in literary dictionaries: cyber intelligence, cyberterrorism, cyber espionage, cyberspace, critical infrastructure, and so on. Cybersecurity and the fight against cybercrime in the 21st century are among the most important issues that require in-depth analysis, development and implementation of high-tech solutions to prevent and detect cyber threats.

Keywords: cybercrime, data encryption, AES, cryptographic stability, banking system, cyber threats

1 Introduction

In modern conditions, the urgent problem of both banks and their customers is the threat of using information technology for criminal purposes, known as cybercrime. This is one of the most common types of economic crime in modern Ukraine. Cybercrime is considered to be a socially dangerous activity or inaction carried out by using modern technologies and computer equipment in order to harm the property or public interests of the state, enterprises, departments, organizations, cooperatives,

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

public organizations and citizens, as well as individual rights. Cybercrime in the scientific literature outlines different types (groups) of crimes in the field of high computer technology, which are classified according to different criteria. However, cybercrime and cybercrime are not identified by many researchers. According to them, the obligatory sign of computer crimes is considered to be a tool for committing a crime - computer technology, while a sign of cybercrime is a special environment for committing crimes, ie cyberspace (the environment of computer systems and networks). Instead, the Law of Ukraine “On Basic Principles of Ensuring Cyber Security of Ukraine” adopted in 2017 went against this doctrine and equated the mentioned concepts, establishing the following definition: “cybercrime (computer crime) is a socially dangerous criminal act in cyberspace and / or with its use, the responsibility for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine "(paragraph 8 of Article 1). Also cited law in paragraph 9 of Art. 1 gave a normative definition of cybercrime, defining it as "a set of cybercrimes"

The current stage of development of the banking sector is characterized by an increase in the number and intensity of such criminal phenomena as fraud with payment cards via the Internet, as well as phishing. Scammers resort to various tricks that force users to disclose confidential information on their own, such as sending emails asking them to verify the registration of an account that contains a link to a website on the Internet that looks exactly like the design of known resources. Cyber attacks on electronic banking systems and official Internet sites and programs have become more frequent. For such crimes, social engineering is also used, which is now actively used on the Internet to obtain confidential information or one that is of great value. The perpetrator obtains it, for example, by gathering information about the employees of the object of the attack by means of a regular telephone call or by accessing their Internet sites. The dynamic development of the information society has given impetus to the spread of cybercrime, which is increasingly committed in Ukraine and is becoming more widespread every year. Criminals' interest in cyberspace is growing due to a number of factors, including lack of physical contact with the victim or a financial institution, promptness, anonymity, availability of computer equipment, remoteness of the object of criminal encroachment, and so on.

2 State of arts

According to a study conducted by PwC in 2018, 31% of organizations in Ukraine suffered from cybercrime. 16% of Ukrainian respondents not only expect cyberattacks on their organizations in the next two years, but are also convinced that cyberattacks will be most significant for their organizations in terms of financial losses or other consequences. More than a third of Ukrainian organizations affected by cyberattacks have been affected by malware. As a result of cyberattacks, not only business processes of organizations were disrupted (according to 51% of Ukrainian respondents), but also significant losses were inflicted on organizations. Due to the growing level of development of tools, cybercrime requires less and less technical

knowledge. Experts note that it is hackers who will displace terrorism in the near future and become the number one threat to countries, because, despite the fact that crimes take place in the virtual world, they cause real damage. It is the financial sector of the economy, including banks and their services, that is considered the most attractive to cybercriminals, and financial data is one of the most popular targets of cyberattacks, as its use allows criminals to make significant money. According to Interpol, the profits from cybercrime in the banking sector rank third in the world after the proceeds from drug trafficking and illicit arms trafficking. Kohut believes that stealing money simply from bank accounts or using stolen personal data is not the only motive behind the hacking of security systems. Such cyberattacks can often be aimed at undermining the reputation of a financial institution. DDoS attacks are also used to distract bank security services from fraudulent schemes and account hacking. Attacks are often carried out on the websites of large banks, which do not have adequate protection. According to experts, four out of five banking resources are currently vulnerable, and three out of four attacks are carried out through unsecured applications, and one small vulnerability can pose a threat to the entire financial institution. Recently, cybercriminals have been actively using mobile technology. Most mobile malicious applications are focused primarily on the theft of money - now there is a clear "banking" orientation of the development of mobile crimes. The creators of the virus monitor the development of mobile banking services and, if a smartphone is successfully infected, immediately check whether it is tied to a bank card.

The traditional subject of cybercrime is a bank card. According to the results of collection, processing and analysis by the Ukrainian Interbank Payment Systems Association of information provided by banks-users of the Exchange-Online system, the main domestic trends in the field of cybercrime in Ukraine are:

- Skimming - a type of cybercrime committed by a skimming device to read information from plastic cards. As of 2013, 293 skimming devices were detected in ATMs of Ukraine. According to the representative of the Cyberpolice Department of the National Police Vitaliy Novik, in 2019, 100 skimming devices were found at Ukrainian ATMs, and 14 criminal cases were opened on 50 facts.
- Fraud in remote banking systems (RBI) is a type of cybercrime, as a result of which criminals are able to track any banking transaction. Since 2013, the banking institutions have introduced a response scheme in the DBO system, which is able to detect and stop 90% of unauthorized money transfers.

In addition, there are the following types of cybercrime in the banking sector:

1. Phishing as a type of Internet fraud, through which criminals manage to obtain bank customers' data: theft of passwords, numbers, credit card details, bank accounts and other confidential information. Through phishing, the personal data of customers of online auctions, currency transfer or exchange services, online stores, etc. are extorted from trusting or inattentive users of the Internet.

2. Wishing - a type of fraud using a mobile phone. The fake message contains a request to call a certain number, while the subscriber reports confidential data on bank accounts.
3. Duplicate site as a mirror of a real site. During an online purchase with a bank card, the customer enters his data, and at this time, attackers withdraw funds from it. It is possible to prevent entering such a site if you follow the following measures: enter the site address manually; do not go to advertising sites; check if this site has a secure connection. It is interesting to classify cybercrimes according to the methods of interfering in the data transmission process:

- interruption (blocking of the transmission process);
- interception (illegal access to transmitted data);
- modification (illegal change of data);
- production (organization of a falsified communication session).

4. Also, the methods of committing cybercrime include: interception of passwords of other users, use of software errors and software bookmarks, use of errors of user identification mechanisms, use of imperfections of data transmission protocols, obtaining information about users by standard operating systems, blocking service functions of the attacked system.

V. Kozlov singled out four types of cybercrimes: unauthorized access, malicious viral modification, interception of information, and combined non-use. It is important to note that bank employees (so-called internal users) commit about 60% of crimes, while external entities - only 40%. In the course of "internal" inspections of violations of the order of banking operations, employees of bank security services are detected about 10-15% of fraud committed by authorized employees of banks. The consequences of cybercrime can be divided into three main groups:

1. distortion (unauthorized modification) of data,
2. infiltration of information,
3. denial of service (violation of access to network services).

Accordingly, the damage to the integrity, confidentiality and accessibility of information is inflicted. The consequence of a significant number of cybercrimes in the banking sector is a decrease in public confidence in the reliability of the financial system, the institution of banking secrecy, the reliability of personal data protection, as well as financial transactions using the latest technologies. At the same time, public distrust in financial services markets does not allow for the active use of free funds of citizens as investment resources aimed at economic development. A. Bukhtiarova and A. Gushcha propose to divide the consequences of cybercrime on the banking system into the following groups: financial, image (reputational), legal, technological.

Negative factors that reduce the effectiveness of the fight against cybercrime in Ukraine include: lack of sufficient state financial support for basic and applied domestic research in the field of preventing and combating cybercrime; Ukrainian production of competitive means of informatization and communication and their protection is slowly developing; informatization of state and commercial

organizations is carried out mainly on the basis of foreign technology and computer technology (strategic technical and technological dependence on other states).

Cybercrime is by nature a cross-border phenomenon, which allows most scientists to point out that cybercrime is characterized by a maximum level of latency. The factors of cybercrime latency are as follows:

1. the complexity of the mechanism of cybercrime, combined with a very diverse field and criminal consequences, as well as "computer illiteracy" of most potential victims of cybercrime, their neglect of their security;
2. negative behavior of victims (eyewitnesses) of the crime, ie failure of the victim and persons who are aware of the crime to law enforcement agencies and failure to report the fact of committing a cybercrime;
3. shortcomings in the work of law enforcement agencies in responding to appeals and reports of cybercrime.

It is standard practice for organizations affected by cybercrime to report cyber-attack incidents to government or law enforcement agencies. However, 28% of organizations in Ukraine answered that they are unlikely or unlikely to report such facts to government or law enforcement agencies (compared to 12% of respondents worldwide). More than half (54%) of these respondents say they are not sure that law enforcement has the necessary qualifications in this area, and the other 41% do not trust law enforcement.

Ukraine is adopting relevant laws and other regulations governing relations in the field of combating cybercrime. As of the beginning of 2020, the regulatory framework of cyber security of Ukraine includes the following documents: the Constitution of Ukraine, the Criminal Code of Ukraine, the laws of Ukraine "On Basic Principles of Cyber Security of Ukraine", "On Information", "On Information Protection in Information telecommunication systems ",“ On the Fundamentals of National Security ”and other laws, the Doctrine of Information Security of Ukraine, the Council of Europe Convention on Cybercrime and other international agreements, the binding nature of which was approved by the Verkhovna Rada of Ukraine.

At the same time, experts note the problem of imperfect legal regulation and implementation of criminal liability for cybercrime, inefficient activities of public authorities, whose powers include combating cybercrime and so on. The priority areas of cyber security of the banking system of Ukraine include, in particular, the protection of information resources of the bank, taking into account the practice of developed countries; creation of a system of training in the field of cybersecurity in banks; cyberspace monitoring for timely prevention of cyber threats; development of international cooperation in the field of cybersecurity; etc.

Based on the above, we can conclude that cybercrime is becoming more global, the latest technology contributes to the anonymity of criminals, and the prospect of rapid enrichment encourages more and more people to join this criminal activity. The banking system of Ukraine is one of the areas where the most widely and actively used modern capabilities of information technology and the Internet. And given that these technologies are used for remittances, this area is attracting more and more attention from criminals. Despite all the measures taken by individuals, firms, and the

state, cybercrime continues to operate, increasing the profits of violators and reducing the content of the pockets of ordinary citizens to exist and evolve. That is why today it is especially important to review all existing measures and actively develop new ones that will bring greater benefits and more reliable protection against cybercriminals. Effective counteraction to cybercrime should combine a set of legal (legislative), technical, organizational and informational measures.

3 Data encryption using AES key

AES is a symmetric iterative block algorithm based on the principles of a new network of permutations. It has a new SQUARE architecture which is characterized by:

- representation of the encrypted block in the form of a two-dimensional byte array;
- encryption for one round of the entire data block (byte-oriented structure);
- performing cryptographic transformations, both on individual bytes of the mass-vu, and on its rows and columns.

This provides diffusion of data simultaneously in two directions - in rows and columns. The SQUARE architecture is inherent, in addition to the AES cipher (RIJNDAEL), SQUARE ciphers (its name gave the name to the whole architecture), CRYPTON (one of the candidates for AES). General characteristics of AES:

AES encrypts and decrypts 128-bit data blocks.

AES allows you to use three different keys with a length of 128, 192 or 256 bits (depending on the length of the key version of the cipher is denoted by AES-128, AES-192 or AES-256).

The number of rounds of encryption depends on the size of the key:

- • length 128 bits - 10 rounds;
- • length of 192 bits - 12 rounds;
- • length 256 bits - 14 rounds.

All rounds, except the last, are identical. Let's see how the keys are created in the AES-128 version. The processes for the other two versions, except for minor changes, are the same. Figure 1 shows how to get 44 words from the source key.

Figure 1 shows the key extension scheme AES-128 version.

The first four words (w_0, w_1, w_2, w_3) are derived from the cipher key. The cipher key is represented as an array of 16 bytes (k_0 to k_{15}). The first four bytes (k_0 to k_3) become W0; the next four bytes (k_4 to k_7) become w1; and so on. In other words, the sequential connection (concatenation) of words in this group copies the key cipher.

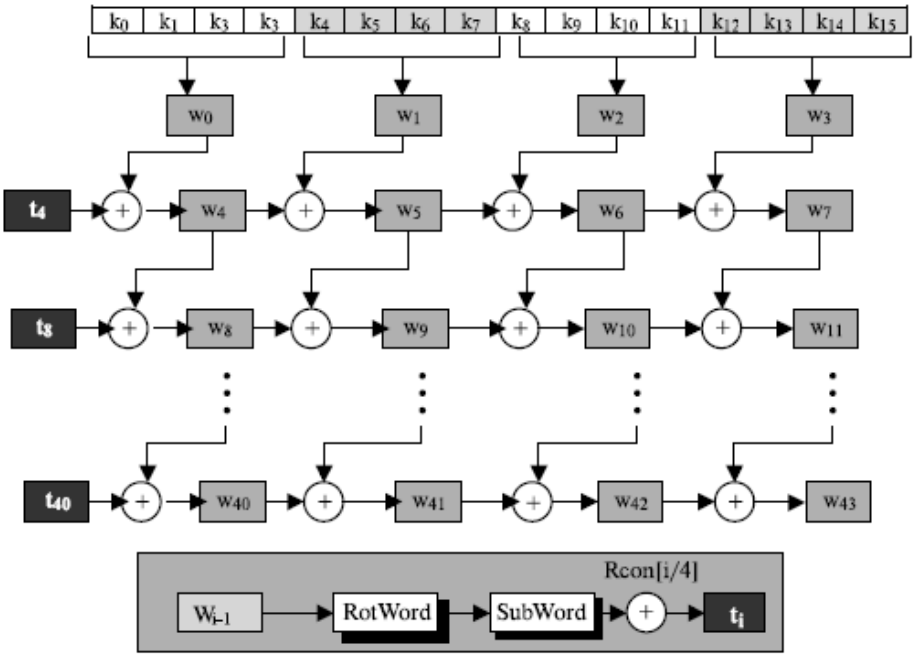

Fig. 1. Key extension scheme for AES-128

The rest of the words (w_i) from i = 4 - 43 are obtained in the following ways:

a)

$$(i \bmod 4) \neq 0, w_i = w_{i-1} \oplus w_{i-4} \quad (1)$$

Then, according to Figure 1, this means that each word is derived from one left and one upper.

b)

$$(i \bmod 4) \neq 0, w_i = t \oplus w_{i-4} \quad (2)$$

Here t - is a temporary word, the result of the application of two processes, sub-word and rot-word, with the word w_{i-1} and the application of the operation excludes or the constant of the round Rcon. In other words, we have:

$$t = SubWord(Rotword(w_{i-1})) \oplus RCon_{i/4} \quad (3)$$

RotWord (rotate word) is a procedure similar to the ShiftRows conversion, but applies to only one line. The procedure takes a word as an array of four or four bytes and shifts each byte to the left with the conversion.

SubWord (substitute word) is a procedure similar to the SubBytes transformation, but applies to only one line. The procedure takes each byte in the word and replaces it with another. Each constant of the Rcon round is a 4-byte value, in which the right three bytes are always zero. Table 1 shows the values for the AES-128 version (with 10 rounds).

Table 1. Константи RCon

Round	***Constant RCon***	***Round***	***Constant RCon***
1	$(01\ 00\ 00\ 00)_{16}$	6	$(20\ 00\ 00\ 00)_{16}$
2	$(02\ 00\ 00\ 00)_{16}$	7	$(40\ 00\ 00\ 00)_{16}$
3	$(04\ 00\ 00\ 00)_{16}$	8	$(80\ 00\ 00\ 00)_{16}$
4	$(08\ 00\ 00\ 00)_{16}$	9	$(1B\ 00\ 00\ 00)_{16}$
5	$(10\ 00\ 00\ 00)_{16}$	10	$(36\ 00\ 00\ 00)_{16}$

The key extension procedure may use either the larger table presented when laying out the words or the GF field (28) when selecting the leftmost bits dynamically, as shown below.

$$
\begin{aligned}
&RC_1 \to x^{1-1} = x^0 \bmod prime = 1 \to 00000001 \to 01_{16}\\
&RC_2 \to x^{2-1} = x^1 \bmod prime = x \to 00000010 \to 02_{16}\\
&RC_3 \to x^{3-1} = x^2 \bmod prime = x^2 \to 00000100 \to 04_{16}\\
&RC_4 \to x^{4-1} = x^3 \bmod prime = x^3 \to 00001000 \to 08_{16}\\
&RC_5 \to x^{5-1} = x^4 \bmod prime = x^4 \to 00010000 \to 10_{16}\\
&RC_6 \to x^{6-1} = x^5 \bmod prime = x^5 \to 00100000 \to 20_{16}\\
&RC_7 \to x^{7-1} = x^6 \bmod prime = x^6 \to 01000000 \to 40_{16}\\
&RC_8 \to x^{8-1} = x^7 \bmod prime = x^7 \to 10000000 \to 80_{16}\\
&RC_9 \to x^{9-1} = x^8 \bmod prime = x^4 + x^3 + x + 1 \to 00011011 \to 1B_{16}\\
&RC_{10} \to x^{10-1} = x^9 \bmod prime = x^5 + x^4 + x^2 + x \to 00110110 \to 36_{16}
\end{aligned}
\tag{4}
$$

The far left byte, denoted by RCi is x^{i-1}, where i is the round number. The AES you-uses is not a given polynomial (x8 + x4 + x3 + x +1).

4 Conclusions

It is impossible to completely protect against cyberattacks. However, compliance with at least the minimum rules of network safety will significantly increase the chances that criminals will not break the system. When conducting transactions between banks or in the client-bank system in Internet banking, it is important to use cryptological

tools such as AES keys with different bit rates, and the higher the bit rate, the greater the protection. However, increasing the bit rate of the key is directly proportional to the performance of the system, so it is advisable to use from 128-bit key to 512-bits. Implementation of these security measures will only minimize the possibility of accidental unauthorized intrusion into the system. However, it is impossible to provide a full guarantee of avoidance of breakage.

5 References

1. Cheswick W.R., Bellovin S.M.: Firewalls and Internet Security: Repelling the Wily Hacker. Addison - Wesley Publishing Company. p. 397. (1994)
2. Cohen F.: Protection and Security on the Information Superhighway. New York. John Wiley & Sons. p.320. (1995)
3. Stallings W.: Network and Internetwork Security Principles and Practice. Prentice Hall. Englewood Cliffs. NY. p. 457. (1995)
4. Bilenchuk P.D., Zuban M.A.: Computer crimes: socio-legal and criminological-forensic aspects. Textbook. Ukrainian Academy of Internal Affairs. p 72. (1994)
5. Butuzov V.M.: Correlation of the concepts of "computer crime" and "cybercrime". Information security of man, society, state. № 1(3). p. 16-18. (2010)
6. Bukhtiarova A.G., Gushcha A.V.: Countering cybercrime in the banking sector. Priazovsky Economic Bulletin. №.3 (14). - p. 355-361. (2019)
7. Kryvenchuk Y.,Vovk O., Chushak-Holoborodko A., Khavalko V., Danel R.: Research of servers and protocols as means of accumulation, processing and operational transmission of measured information. Advances in Intelligent Systems and Computing. Vol.1080. p.920-934. (2020)
8. Card fraudsters robbed Ukrainians of 360 million in a year. URL: https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikraly-ukrayintsiv-za-rik-na-360-mln
9. Klimchak M.: World Study of Economic Crimes and Fraud 2018: a survey of Ukrainian organizations. Removing fraud from the shadows. URL: https://www.pwc.com/en/en/survey/2018/pwc-gecs-2018-ukr.pdf
10. Kozlov V.E.: Theory and practice of combating computer crime. Gorya-chaya liina – Telekom. p.336. (2002)
11. Kravtsova M.: The current state and directions of combating cybercrime in Ukraine. Bulletin of the Criminological Association of Ukraine. № 2 (19). p.155-166. (2018)
12. Krupka I.M.: Financial and economic security of the banking system of Ukraine and prospects for the development of the national economy. BUSINESSINFORM. №6. p. 168-175. (2012)
13. Boyko N., Pylypiv O., Peleshchak Y., Kryvenchuk Y., Campos J.: Automated document analysis for quick personal health record creation. 2nd International Workshop on Informatics and Data-Driven Medicine. IDDM 2019. Lviv. p. 208-221. (2019)
14. Luta N.V., Zachosovna N.V.: Cybercrime as a modern threat to the financial security of banks and their clients. Science: theory and practice: collection. thesis add. III All-Ukrainian scientific-practical correspondence Conf. Cherkasy. p. 247–252. (2014)
15. Hornovyi V.M.: Methodological bases of ensuring information security of the object. Protection of information. Confident. - № 1. p. 75. (2000)
16. Katsera M.: Cybercrime - a threat to the banking system. Bulletin of the National Bank of Ukraine. № 4. p. 55-58. (2015)

17. Kryvenchuk, Y., Shakhovska, N., Melnykova, N., & Holoshchuk, R.: Smart Integrated Robotics System for SMEs Controlled by Internet of Things Based on Dynamic Manufacturing Processes. Springer, Cham. pp. 535-549. (2018).
18. On the basic principles of cybersecurity of Ukraine: the law of Ukraine dated 05.10.2017. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#n5
19. Kryvenchuk, Y., Shakhovska, N., Shvorob, I., Montenegro, S., & Nechepurenko, M.: The Smart House based System for the Collection and Analysis of Medical Data. CEUR, Vol-2255. pp 215- 228. (2018).
20. Stetsyshyn Y., Awsiuk K., Kusnezh V., Raczkowska J., Jany B., Kostruba A., Harhay K., Ohar H., Lishchynskyi O., Shymborska Y., Kryvenchuk Y., Krok F., Budkowski A. Shape-controlled synthesis of silver nanoparticles in temperature-responsive grafted polymer brushes for optical applications. Applied Surface Science. Vol. 463.p. 1124–1133. (2018).
21. Davydova I., Marina O., Slianyk A., Syerov Y. Social Networks in Developing the Internet Strategy for Libraries in Ukraine. CEUR Workshop Proceedings. 2019. Vol 2392: Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks, COAPSN-2019. P. 122–133.
22. Fedushko S., Benova E. Semantic analysis for information and communication threats detection of online service users. The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019) November 4-7, 2019, Coimbra, Portugal. Procedia Computer Science, Volume 160, 2019, Pages 254-259. https://doi.org/10.1016/j.procs.2019.09.465
23. Khavalko V., Khudyy A.: Application of Neural Network Technologies for Information Protection in Real Time. IEEE First International Conference on System Analysis & Intelligent Computing. Kyiv p. 173-177. (2018)
24. Kryvenchuk Y., Mykalov P., Novytskyi Y., Zakharchuk M., Malynovskyy Y., Řepka M.: Analysis of the architecture of distributed systems for the reduction of loading high-load networks. Advances in Intelligent Systems and Computing. Vol.1080. p.759-550. (2020)
25. Tsmots I., Skorokhoda O., Tsymbal Yu., Tesliuk T., Khavalko V.: Neural-Like Means for Data Streams Encryption and Decryption in Real Time. In: IEEE Second International Conference on Data Stream Mining & Processing. pp.438-443 (2018).
26. Khavalko V., Tsmots I.: Image classification and recognition on the base of autoassociative neural network usage. UKRCON. p. 1118-1121. (2019)