Regular paper

Journal of the KIECS. pp. 219-228, vol. 17, no. 2, Apr. 30. 2022, t. 112, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2022.17.2.219

# 광섬유 통신 시스템의 정보 신호 침해에 대한 보호 시스템

Sobirov Asilzoda Alisher Ugli[*] · Nishonov Ilhomjon Umaralievich* · 김대익[**]

# Protection System Against The Infringement of Information Signals in Fiber Communication System

Sobirov Asilzoda Alisher Ugli[*] · Nishonov Ilhomjon Umaralievich[*] · Daeik Kim[**]

## 요 약

인간 활동 영역의 광범위한 변환 및 디지털화 조건에서 오늘날 가장 시급하고 까다로운 문제 중 하나는 정보 보안과 데이터 무결성 보장입니다. 정보 보안 분야의 주요 연구 개발은 효율성과 합리화를 향상시키는 데 있습니다. 정보 단지의 데이터 전송 및 운영의 주요 수단 중 하나는 광섬유 시스템입니다. 현재까지 이러한 통신 방식을 통해 불법적인 침입 및 정보 도용 사건이 발생하고 있습니다. 따라서, 오늘날 광섬유 데이터 전송 시스템에서 불충분한 정보 보안과 관련된 문제가 있습니다. 시스템의 불법 간섭 행위에 대응하는 가장 효과적인 도구 중 하나는 인공 지능과 정보 보호의 암호 알고리즘입니다. 이 두 도구의 공생은 광섬유 데이터 전송 시스템의 정보 보안 수준을 질적으로 향상시킬 수 있습니다. 따라서 이 기사의 저자는 지능형 암호화 알고리즘의 통합을 기반으로 하는 광섬유 데이터 전송 시스템의 위반으로부터 정보를 보호하기 위한 혁신적인 시스템의 설명과 관련된 목표를 추구합니다.

## ABSTRACT

One of the most pressing and demanding issues today in the conditions of widespread transformation and digitalization of spheres of human activity is information security and ensuring the integrity of data. The main research and development in the field of information security is aimed at improving efficiency and rationalization. One of the main means of data transmission and operation of information complexes are fiber-optic systems. To date, there have been incidents of illegal intrusion and theft of information, passing through this type of communication. Thus, today there is a problem associated with insufficient information security in fiber-optic data transmission systems. One of the most effective tools to counter acts of illegal interference in systems are artificial intelligence and cryptographic algorithms of information protection. It is the symbiosis of these two tools that can qualitatively improve the level of information security in fiber-optic data transmission systems. Thus, the authors of this article pursue the goal associated with the description of an innovative system for protecting information from violations in fiber-optic data transmission systems based on the integration of intelligent cryptographic algorithms.

Key words

Fiber-Optic Communication, Cryptography, Information Security, Artificial Intelligence, Information, Data Transmission System
키워드. 광섬유 통신, 암호화, 정보 보안, 인공 지능, 정보, 데이터 전송 시스템.

* 전남대학교 대학원 전자통신공학과
(Asilzoda007@mail.ru , ilhomjon0105@gmail.com)
** 교신저자 : 전남대학교 전기전자통신컴퓨터공학부

· 접 수 일 : 2022. 01. 06
· 수정완료일 : 2022. 02. 25
· 게재확정일 : 2022. 04. 17

· Received : Jan. 12, 2022, Revised : Feb. 25, 2022, Accepted : Apr. 17, 2022

· Corresponding Author : Dae-Ik Kim
School of Electrical, Electronic Communication, and Computer Engr.,
Chonnam National University.
Email : daeik@jnu.ac.kr

## Ⅰ.Introduction

The work examines the basic information, relevance and effectiveness related to the topic of the study. This research performs work through the application of statistical data and information, as well as empirical and theoretical methods of research. In this article it is used publications and materials of domestic and foreign sources to more fully disclose the topic and obtain reliable data.

Many scientific articles, papers and monographs, each of which explores more thoroughly separate aspects of the structure and systems of information security, are devoted to the approximate presented and related topics of this work. This article is based on scientific conclusions and results obtained by the authors K.A Kudryavtseva, Sh.U. Uktamzhonov, I.A. Kosimov, D.V. Afanasyeva, A.V. Balanovskaya, O.L. Tsvetkova, A.I. Kreper and others[1-8].

In each of above works, the authors produce research that is of great relevance from the field of information security today. So, for example, questions of scenarios of connection to optical fiber cables and protection against illegal interception of information in communication channels, ways of protection of information signal from unauthorized access, modern threats to information security and more are investigated.

Artificial intelligence (AI) and machine learning technologies are already widely used in information systems to increase labor productivity, increase sales, and training. Their use in protecting against cyber-attacks is becoming one of the key areas in information security.

Total investments in companies that create information security products using AI technologies are $ 3749 million at the end of 2019.  At the same time, the global market for information security products using technology AI will reach $ 30 billion in 2025 with an annual increase in 23%.

At the moment, the number of attacks is growing, and the landscape of threats is changing at lightning speed. For example, Kaspersky products reflect more than 700 million online attacks per quarter (data for the second quarter of 2019) worldwide, and Cisco claims to block 20 billion network attacks per day (more than 7 trillion attacks in 2018). It is obvious that with such volumes of malicious activity, cybercriminals are actively using tools to automate cyberattacks, including using artificial intelligence and machine learning technologies to improve and transform them, as well as to bypass known defenses. For example, the well-known Emotet Trojan is an effective prototype. The main channel for its distribution is spam phishing, and the group behind the creation of Emotet could easily use AI to amplify the attack, embedding itself in conversations natively and using natural language text analysis.

Another possible area of malicious use of artificial intelligence is better password guessing or bypassing two-factor authentication. Two years ago, researchers created a bot that was able to bypass CAPTCHA checks with an efficiency of 90% using AI technologies. By using a huge number of different data sources on the darknet to form a knowledge base of artificial intelligence, attackers can make attacks on humans truly effective[10].

In order to cope with the growing volume of attacks, security vendors are also beginning to actively implement artificial intelligence, machine and deep learning (ML/DL) technologies to detect, predict and respond to cyber threats in real time. Overall, according to Webroot (https://www-cdn.webroot.com), about 85% of security professionals believe that attackers use AI technologies in their attacks.

## II. The relevance of information security in fiber-optic data transmission systems

For a long time, it was believed that fiber-optic communication lines have maximum security and information secrecy, but modern research has shown that there are ways to remove radiation from optical fibers, thus information transmitted through them can be compromised, deleted or blocked. In accordance with the Federal Law "On communications", telecommunications operators are obliged to ensure the secrecy of communications and protection of communications equipment and facilities from unauthorized access to them. Unauthorized access to means of communication and information transmitted through them entails disciplinary, civil, administrative or criminal liability.

Contrary to the opinion that in a fiber-optic line to make a covert withdrawal of information is impossible, the methods of such connection exist and their implementation is possible in each of the enterprises, which use in the data transmission optical technology. Also, in this article we will consider methods of protection against these illegal connections. Considering the second type of threats - voice information interception, we can conclude that leakage of voice information can occur not only in operating, but also in non-operational, but laid fiber-optic networks, if an intruder artificially introduces a signal which will be modulated by acoustic waves into the cable [2].

It should be noted that the equipment used by an intruder does not necessarily have to be specialized for unauthorized data capture, it can be a variety of publicly available standard equipment, for example for the installation of communication lines. The main methods for protecting traffic from leakage in fiber-optic communication lines can be divided into three main groups of methods for protecting against the interception of such information by an intruder:

1. Physical means of information protection;
2. Hardware means of information protection;
3. Cryptographic protection of information.

Information protection is provided not by influence on leakage channel parameters, but by probabilistic transformation of information before its transmission via communication channel. Impossibility of information recovery by an intruder is based upon the property that leakage channel has lower bandwidth, than user's normal channel. Encryption method is chosen so that the number of errors arising in the leakage channel greatly increases, providing the effect of noise transmission signal, while the main channel provides a reliable connection Cryptographic method includes a method that makes the information for an attacker little useful - this is quantum cryptography, which is reflected just in the fiber-optic technology. Quantum cryptography is based on the Heisenberg uncertainty principle - it is impossible to measure one parameter of a photon without distorting another. Therefore, an intruder will not be able to change the state of the transmitted photons, as this could cause him to be exposed, by the fact of additional interference on the receiving side.

## III. Analysis of integration of artificial neural networks to improve the efficiency of cryptographic algorithms for information protection

Intelligent technologies, in particular artificial neural networks (ANN), which have enormous potential in solving various complex computational tasks, are most actively studied and integrated in modern information security systems. Colossal relevance of integration of artificial intelligence in these tasks is one of the highest in the modern world within the field of study. This factor is related to the fact that intelligent technology is used not only to solve problems of mathematical and engineering nature, but also successfully proven themselves in solving problems from information security, encryption, decryption and other processes.

ANN rather firmly enters the life of the modern man in solving various kinds of problems, and are also used where primitive algorithms are inefficient or even impossible tool. The list of tasks, the solution of which is based on the use of neural networks, includes: text recognition, contextual advertising on web sites, spam filtration, monitoring of suspicious transactions in the banking system, image restoration and many others [3].

Artificial neural networks are a key area of development from the field of artificial intelligence for solving information security problems. ANNs are a mathematical model that has its own implementation at the software and hardware level. Fig. 1 illustrates the scheme of a simple artificial neural network: Green-input neurons; blue -hidden neurons; yellow -output neuron

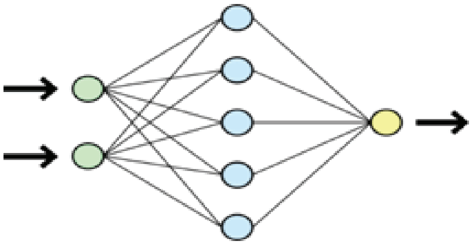

Fig. 1 Schematic diagram of a simple neural network.

Let us consider the mathematical meaning of artificial neural networks. In the mathematical interpretation ANNs are represented as a non-linear function. Under w it is characterized by connections, it is through them that signals from some neurons are fed into input signals of other neurons. Each artificial neural network neuron includes a single output, called a synapse. It should be noted that each output of a neuron is connected (or can be connected) with an unlimited number of outputs of other neurons (Fig. 2). The following mathematical model of artificial neuron is presented for understanding:

$$y=F(\sum_{i=1}^{n}(w_i{*}x_i+b_i),$$

Where: $w_i$ - represent the weights of the corresponding inputs;

$x_i$ - represent signals at the inputs of the neuron;

$b_i$ - represent the input and weight of the displacement neuron.

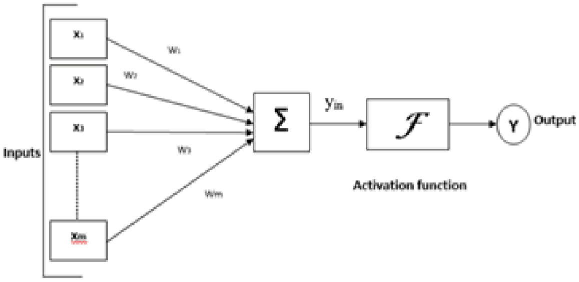

Fig. 2 Schematic diagram of an artificial neuron

Cryptography has a distinctive feature relative to other methods of protection of information flows, namely concentration of algorithmic work on physical processes and methods. Information and ciphers received by means of physical methods can be transferred and formed on the basis of objects of quantum mechanics. All processes as a whole, in this method of information encryption, take place by means of execution of physical methods. One of the examples of quantum-cryptographic algorithms work is movement of some number of electrons in electric field or photons in fiber-optic communication lines. Such a circuit includes a quantum channel and special equipment placed at both ends of the system. Fig. 3 schematically depicts the principle of operation of such a scheme for transmitting information flows [4].

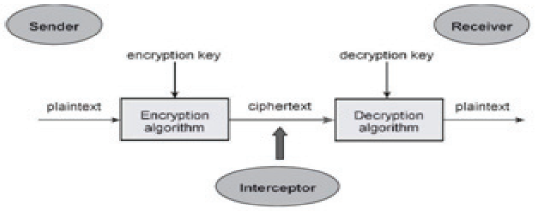

Fig. 3 Cryptographic algorithm of information protection

As seen from the diagram, the key principle of quantum-cryptographic algorithms operation is uncertainty of quantum system behavior. The main idea of this principle lies in the fact that there is no possibility to express simultaneously coordinate and momentum of a particle without parallel distortion of another.

By means of work of quantum processes nowadays various communication systems and means of transferring of information flows are widely implemented and developed, having an ability of hundred percent detection of eavesdropping and interception of information. This ability is achieved by means of the following factor: any attempt to measure interconnected parameters of a quantum system introduces disturbances into it, in parallel destroying initial data.

In recent years researches in the field of construction of methods of protection of information with use of theory of cryptography and noise-resistant coding are actively conducted and exactly these systems are most actively exposed to computer attacks. Traditionally existing information security systems do not have the possibility of self-learning and use only certain rules, laid in their software or hardware. Creation of perspective information security systems is identified recently with use of intellectual tools, such as: expert systems, fuzzy logic systems, neural networks, genetic algorithms. These approaches implement evolutionary properties of adaptation, self-organization, learning, possibility of inheritance and representation of information security experts′ experience in the form of a system of fuzzy rules available for analysis [5].

The traditional algorithm does not take into account the problem of terminal and server authentication. It has low security; it requires a lot of computation to encrypt or decrypt. To solve these problems, a new intelligent encryption algorithm for network transmission of parallel data is proposed. After the user is registered, the registered ID, the user′s password and two random numbers are entered. The first authentication data is obtained by calculation and then transmitted over a secure channel to the server for the first authentication. After successful authentication of the identity, the information user is granted permission to release. The key matrix is created using the parallel MapReduce engine. The source information data file is divided into blocks, and each block is encrypted with a key matrix. After separating the plaintext matrix and the key matrix, the plaintext is encrypted according to the encryption principle. After receiving the ciphertext and the key matrix, the plaintext is decrypted using the decryption principle. Experimental results show that the proposed algorithm has high safety and efficiency.

Based on the theory of artificial intelligence and artificial neural networks, as well as studying the basic operation of cryptographic algorithms for information encryption, we can propose the following, shown in Fig. 4 algorithm of intellectual cryptographic protection of information in fiber-optic data networks.

The increasing emergence of unwanted (malicious) software that exploits new vulnerabilities has increased the requirements for modern information security systems and has led to the use of artificial intelligence systems.

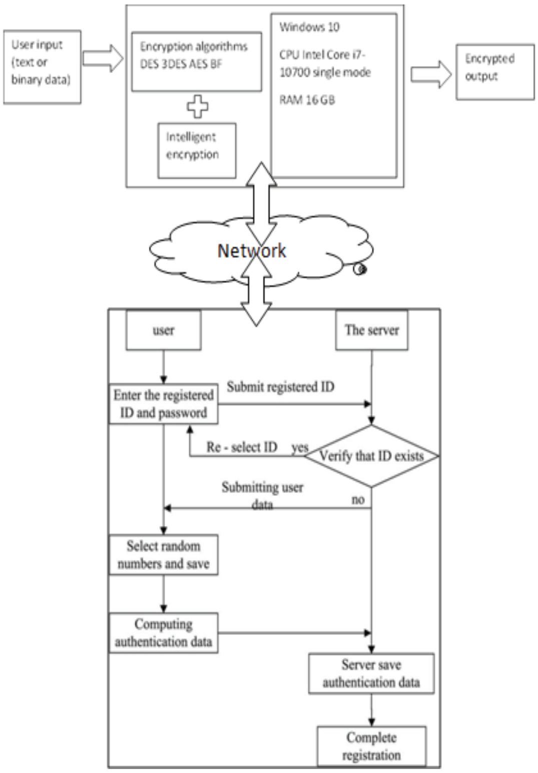
User input (text or binary data)
Encryption algorithms DES 3DES AES BF
Intelligent encryption
Windows 10
CPU Intel Core i7-10700 single mode
RAM 16 GB
Encrypted output
Network
user
The server
Enter the registered ID and password
Submit registered ID
Re - select ID
yes
Verify that ID exists
Submitting user data
no
Select random numbers and save
Computing authentication data
Server save authentication data
Complete registration

Fig. 4 Intelligent encryption algorithm for network communication

Intelligence tools are actively used to solve information security problems. Classification and clustering are the main tasks solved by intelligent tools for information security (IS) of telecommunications channels in space communications, because constant monitoring of system vulnerabilities and threat fields of channels is required [6].

### 3.1 Performance assessment of information security system based on the principle of intelligent cryptography

AI has a significant impact on many sectors of our society and the economy (for example, predicting police, justice, precision medicine, marketing, political propaganda). AI sectoral applications are characterized by various problems and cannot be properly discussed in this report, which provides a general overview of the main issues related to the interaction between data protection and AI. Thus, this last section briefly sheds only on two main areas: the public sector and the workplace. In particular, in most cases, the introduction of AI technologies in the organization′s information security reduces the time to identify problems and respond to incidents, as well as expenses for personnel management. Operators note an increase in the effectiveness of detecting unknown threats, as well as the speed of analysis and detecting malicious activity at endpoints and in applications [8].

AI Applications increases a number of specific questions when used in the public sector, largely due to the imbalance of power between citizens and administration and the necessary services provided. Moreover, the adoption of comprehensive and unclear solutions AI from governments and their agencies indicate that they are more difficult to comply with their accountability obligations, not only regarding the data in processing [9].

This state of affairs, apparently, justifies the adoption of more stringent guarantees, except for the transfer of special committees or audit. Protection should also contain an evaluation process that critically evaluates the need for the proposed AI solutions and their suitability for the delivery of services by government agencies or private companies operating on their behalf. This process requires "at least they [AI applications] should be available for public audit, testing and consideration, as well as in accordance with the accountability standards."To achieve this goal, state procurement procedures can impose specific duties of transparency and previous evaluation by AI suppliers.

## Ⅳ. Overview of cryptographic algorithms

The tests took into account the block size (randomly generated data), key size and time of encryption and decryption, CPU processor time in the form of bandwidth and power consumption with symmetric algorithms DES, AES, 3DES, Intelligent algorithm. Intelligent algorithm performed better than other algorithms.Intelligent algorithm is safer and faster processing algorithm. This reduces execution time and provides greater security and consumes less memory than any other algorithm

Table 1. Comparison of the algorithm's time performance in milliseconds

| Input size (bytes) | DES | 3DES | AES | BF | Intelligent encryption |
|---|---|---|---|---|---|
| 20,527 | 2.4 ms | 7.2 ms | 3.9 ms | 1.9 ms | 1.7 ms |
| 36,002 | 4.8 ms | 12.3 ms | 7.4 ms | 3.5 ms | 2.9 ms |
| 45,911 | 5.7 ms | 15.6 ms | 9.4 ms | 4.5 ms | 3.7 ms |
| 59,862 | 7.4 ms | 20.2 ms | 12.6 ms | 5.8 ms | 4.8 ms |
| 69.646 | 8.3 ms | 24.3 ms | 14.3 ms | 6.7 ms | 5.6 ms |
| 137,325 | 16 ms | 46.1 ms | 28.5 ms | 13.6 ms | 11.1 ms |
| 158,959 | 19 ms | 54.3 ms | 32.4 ms | 15.8 ms | 12.9 ms |
| 166,364 | 19.8 ms | 56.9 ms | 35.5 ms | 16.2 ms | 13.5 ms |
| 191,383 | 22.7 ms | 65.5 ms | 37.8 ms | 17.6 ms | 15.5 ms |
| 232,398 | 27.6 ms | 79.9 ms | 46 ms | 21.9 | 18.8 ms |
| Average time (sec) | 13.4 ms | 38.3 ms | 22.8 ms | 10.8 ms | 9 ms |
| Bytes/sec | 8,350 ms | 2,920 ms | 4,910 ms | 10,360 ms | 12,360 ms |

Graphical representation of the Table 1 is can be seen in Fig. 5 which illustrates comparative execution times on a single core mode of Intel Core i7-10700 3.0GHz machine. DES, 3DES, AES, BF and Intelligent algorithms are tested on various size files such as 20527, 36002, 45911, 59862, 69646, 137325, 158959, 166364, 191383 and 232398 bytes respectively. All tests are implemented on Python programming language by Python 3.10 version.

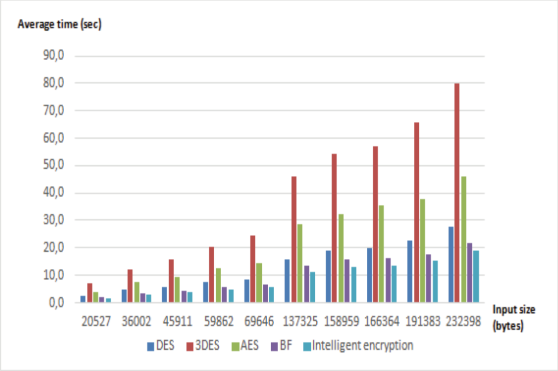

Fig. 5 Comparative execution times on a single core mode of Intel Core i7-10700 3.0GHz machine.

In addition, procurement procedures may also solve issues related to the protection of IP protection of trade secrets that introduce certain contractual exceptions to increase transparency and make a possible AI audit.

As for the consequences of AI for the future of work, leaving in the direction of its influence on the labor market, AI solutions can affect the relationship in the workplace. First, they can increase the control of the employer over employees in a situation that is often characterized by an imbalance of power.

Moreover, the use of hidden and unregulated data processing forms can convert the workplace to a social experiment by raising additional important questions about the role of transparency, ethics committees and voluntary participation in data processing.

Finally, devices paid to employees by employers may have double use. For example, in the workplace at the workplace, you can wear wearable well-being devices to collect biological data designed to protect the health of the employee, but employees can also use them outside work to track their sports fitness. If only the consequences for data protection and individual freedom are not studied, such double use can blur the boundaries between the work and personal life, increasing the issues of common control and the right to shut down. In Fig. 6 is an efficiency of using artificial intelligence technologies for different scenarios:

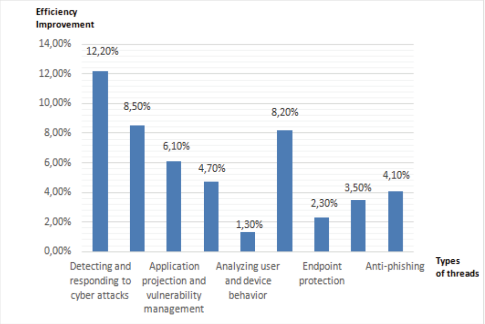

Fig. 6 Efficiency of using artificial intelligence technologies for different scenarios compared to traditional anti-malware systems

Having examined the relevance of the use of intellectual systems, in particular, artificial neural networks in information protection tasks, it is necessary to focus in more detail on the aspect of the integration of network data integration into the area studied.

It should be noted that according to SANS data, about 30% of information security experts are convinced that artificial intelligence technologies are able to increase the efficiency of detecting unknown threats.

Consider in the percentage relative to the standard methods of information security metrics, improved by integrating artificial neural networks

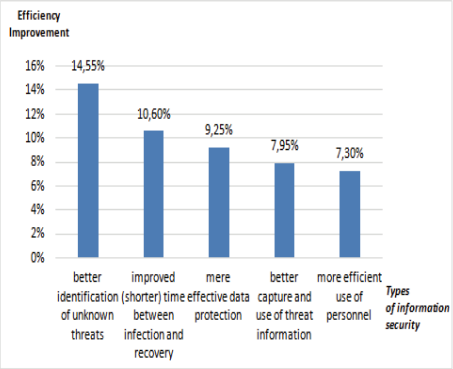

Fig. 7 Improvement by integrating artificial neural networks compared to traditional anti-malware systems

Based on the above data, it is clear that the technologies of ANN make a colossal contribution to the fight against modern information threats. In overwhelming majority faces, intelligent technologies reduce the operation time to identify problems and subsequent response to incidents, and also reduce the managing personnel. Inc companies operating in their systems note a significant increase in the efficiency of detecting unknown threats, as well as an increase in the speed of analyzing and detecting malicious activity on servers.

## Ⅴ. Conclusion

An overview of the state of artificial intelligence segment in information security allows you to make the following conclusions:

The main methods for protecting traffic from leakage in fiber-optic communication lines can be divided into three main groups of methods for protecting against the interception of such information by an intruder:

1. Physical means of information protection;
2. Hardware means of information protection;

3. Cryptographic protection of information.

Artificial neural networks are a key area of development from the field of artificial intelligence for solving information security problems.

All processes as a whole, in this method of information encryption, take place by means of execution of physical methods. One of the examples of quantum-cryptographic algorithms work is movement of some number of electrons in electric field or photons in fiber-optic communication lines. Such a circuit includes a quantum channel and special equipment placed at both ends of the system. Artificial intelligence makes a noticeable contribution to the fight against modern information threats.

As a result of the work, it can be seen that ANN technologies are among the most innovative and breakthrough achievements of science today. These funds are widely introduced in almost all spheres of life of a modern person, ranging from domestic ones, and ending with professional. In this paper, issues related to the integration of artificial neural networks in the information security systems of modern enterprises were in more detail.

## References

[1] K. A. Kudryavtseva and Y. F. Katorin, “Code noise and other ways to protect the fiber optic communication line,” *Natural and mathematical sciences in the modern world*, vol. 35, no. 11-12, 2015, pp. 85-89.

[2] S. Uktamjonov, I. Kosimov, and J. Otakhujaev, “Method of protecting information signals from unauthorized access to fiber optic,” *European science*, vol. 45, no. 3, 2019, pp. 30-34.

[3] Y. F. Katorin, V. V. Korotkov, and A. P. Nyrkov, “Information security in data transmission channels in the coastal networks of the automated identification system,” *Bulletin of Admiral Makarov State University of Sea and River Fleet*, vol. 13, no. 1, 2012, pp. 98-102.

[4] D. V. Afanasyeva, “Application of artificial intelligence in data security,” *Technical science news of the Tula State University*, issue 2, 2020, pp. 151-154.

[5] B. A. Vyacheslavovna, “Analysis of the current threats to information security of business organizations,” *Local Information security*, vol. 20, no. 3, 2015, pp. 9-16.

[6] I. V. Bogachkov, S. S. Lutchenko, and E. Y. Kopytov, “Determination of the availability factor of fiber optic communication lines depending on external actions and diagnosis errors,” *T-Comm*, vol. 12, no. 6, 2018, pp. 51-55.

[7] D. A. Tershukov, “Analysis of modern information security threats,” *NBI-technologies*, vol, 12. no 3, 2018, pp. 6-12.

[8] O. L. Svetkova and A. I. Kreper, “On the application of the theory of artificial neural networks in solving the problems of ensuring information security,” *Symbol of science*, vol. 2, no. 4, 2017, pp. 105-107.

[9] D. Reisman, J. Schultz, K. Crawford, and M. Whittaker, “Algorithmic impact assessments: a practical framework for public agency accountability,” *Technical report*, Apr. 2018.

[10] J. Yang, K. Seok, and H. Sin, “Technological and Social Significance of the Revision of the Radio Law,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 4, 2019, pp. 627-636.

## 저자 소개

### A. A. Sobirov

2019년 6월 Fergana Branch of Tashkent University of Information 졸업(공학사)
2019년 9월 ~ 전남대학교 대학원 전자통신공학과 석사과정

※ 관심분야 : artificial intelligence, fiber-optic communications

### I. U. Nishonov.

2012년 6월 Fergana Polytechnic Institute 졸업(공학사)
2014년 6월 Fergana Polytechnic Institute 졸업(공학석사)
2018년 9월 ~ 전남대학교 대학원 전자통신공학과 석박사통합과정

※ 관심분야 : artificial intelligence, fiber-optic communications

### 김대익(Dae-Ik Kim)

1991년 전북대학교 전자공학과 졸업(공학사)
1993년 전북대학교 대학원 전자공학과 졸업(공학석사)
1996년 전북대학교 대학원 전자공학과 졸업(공학박사)
2002년~현재 전남대학교 전기전자통신컴퓨터공학부 교수

※ 관심분야 : VLSI 설계, 저전력 회로설계