

Intelligent systems in information protection

S.F. Azamova

***Assistant, Tashkent University of Information Technologies named after
Muhammad al-Khwarizmi***

ABSTRACT

This article considers the use of intelligent systems in information security. The introduction highlights the problem of growing threats to information security and introduces the concept of intelligent systems and their potential in this area. It then discusses the definition of intelligent systems, their role in detecting and preventing information security threats, and the benefits of using them. The following are examples of the use of intelligent systems in various areas of information security. It then discusses the challenges and limitations associated with the use of intelligent systems. The conclusion summarizes and summarizes the benefits of using intelligent systems in information security, and also indicates potential directions for the development of this area.

Keywords: intelligent systems, information security, information security threats, artificial intelligence, efficiency, automation, machine learning, neural networks, genetic algorithms, challenges, limitations.

To protect information, highly effective plans are developed and implemented to detect access failures using hardware and software [1]. The last decade has seen the active development of a new generation of analytical systems that are based on advanced artificial intelligence technologies [2]. They are included in such a concept as “intelligent information systems”. They have great potential in the field of information security due to the ability to develop systems that learn and are able to make autonomous decisions, as well as detect and classify potential attacks or threats. The concept of intelligent information systems (IIS) was formed as a result of progress in the fundamentals of cybernetics, modern control theory, algorithmic theory, the development of information technology and the generalization of accumulated scientific knowledge, methods and tools in the field of artificial intelligence (AI).

Today, applications of artificial intelligence can be found in organizations in every sector, and include chatbots to help customers navigate websites, predictive analytics systems used to detect fraud, advanced decision support systems for knowledge workers, and autonomous systems in transportation, in defense and healthcare. Intelligent information systems, or IIS, have cognitive abilities due to their learning functions. IIS can learn in one of two main ways: supervised and unsupervised. In supervised learning, each entry in the training dataset is labeled with its correct

classification so that the machine learns what makes an entry more or less likely to be in each group. In a fraud detection exercise, each entry is flagged as either fraudulent or non-fraudulent, and the machine identifies other attributes in the entry that help distinguish between the two groups. The system looks for the best distinguishing features to describe one group compared to another. Thus, an intelligent information system (IIS) is a type of intelligent system containing a complex of software, logical-mathematical, and linguistic tools for solving certain problems, for example, the ability to conduct an advanced dialogue in natural language and search for information in this mode. At the moment, the following approaches are popular - immune system technologies, Bayesian network, genetic algorithms, neural networks, etc. Problems that can be solved by intelligent information systems (IIS):

- Data interpretation: determining the meaning of the data and analyzing multiple options to achieve consistency and correctness of results.
- Diagnostics: correlation of an object with a certain class of objects or detection of faults in the system.
- Monitoring: continuous analysis of data in real time and notification of exceeding permissible parameter values.
- Design: preparing specifications for creating “objects” with predefined properties.
- Forecasting: the ability to predict the consequences of certain events or phenomena based on data from a parametric dynamic model, in which parameter values are selected for a given situation.
- Planning: searching for action plans for specific objects that can perform certain functions.
- Training: identifying errors in the learning process and providing correct solutions, based on the accumulation of knowledge about a hypothetical “student” and his typical mistakes. Neural networks have this property and this is their main advantage over other algorithms. They are able to identify complex patterns between input and output data, as well as generalize. As a result, make predictions based on data that was not in the training set.

Management: maintaining a certain mode of operation of systems in accordance with given specifications. Decision support: helping specialists select the right alternative from a variety of choices when making critical decisions [5]. Intelligent systems are used in these information security systems:

- Biometric identification systems, used, for example, in the banking industry as a complete or partial replacement of conventional passwords for access control and management. Using neural network algorithms, the processing of biometric identification information takes place in 4 stages:
 - obtaining the user's biometric data through the use of sensors (devices for converting input signals);
 - extracting informative biometric characteristics;
 - creating a biometric user template using a neural network;

– application of a decision rule based on a neural network.

Intrusion detection systems (IDS), based on intelligent systems, help detect, prevent and respond to incidents involving computer attacks. IDS are implemented using various methods for searching for special indicators that the transmission of network traffic is taking place within the framework of some kind of attack on the information system. Intelligent anti-virus protection systems, as well as IDS, use the signature analysis method in the fight against viruses. Anti-virus protection reports about “infection” with viruses, helps to “cure” from viruses and controls the channels of virus penetration. Tools for analyzing and managing information risks based on intelligent systems make it possible to determine the potential harm from attacks that exploit vulnerabilities in the system, as well as the likelihood of such attacks occurring. For effective risk management, the cognitive modeling method is used, which is based on the use of limited, unclear or contradictory information about the object under study, presented by experts. The goal of this approach is to identify key and significant relationships, determining the importance of each factor influencing the problem [5]. Using intelligent systems to protect information has a number of advantages. First and foremost, intelligent systems have the ability to analyze large volumes of data and detect potential threats with greater accuracy and efficiency than traditional methods. They can automatically monitor and analyze data, detect anomalies and suspicious activity that may indicate threats and attacks [6]. Also, the use of intelligent systems reduces the likelihood of errors associated with the human factor. They can conduct complex data analysis, taking into account multiple factors, which contributes to more accurate and reliable detection of threats and security incidents. Another important advantage of using intelligent systems in cybersecurity is their ability to self-learn based on experience. Experience from previous attacks will help improve existing behavior algorithms and provide more accurate detection of threats in the future [7].

In addition, intelligent systems can analyze and process large volumes of data to identify hidden patterns and trends. This allows you to predict potential threats and attacks and take measures to prevent them in advance. This increases the effectiveness of information protection measures. In addition, intelligent systems are capable of learning based on experience. They can adapt to new types of threats and update their algorithms and models based on new knowledge. This allows systems to continually improve and better cope with constantly changing information security threats. Intelligent systems can operate in real time, allowing you to quickly respond to security threats and incidents.



Figure 1 – Architecture of a hybrid IDS Fast response reduces response time and allows you to take timely necessary measures to minimize damage from incidents. Intelligent systems are used in various areas of information security. Neural networks can analyze data received from IDS to identify phishing attempts. They can detect suspicious emails, web pages, URLs, and other elements typical of phishing attacks. This allows IDS to prevent and block phishing attacks, minimizing the risk to users and systems. Neural networks can continuously learn based on new data about phishing attacks, which are detected and blocked by IDS. This allows neural networks to update their models and algorithms to better recognize and prevent new types of phishing attacks. Anomaly detection method uses algorithms to analyze large amounts of data. It builds a picture and compares data with this picture. If the data does not match the picture, it is considered an anomaly. In this case, network traffic is used as a data source. Network traffic data is presented in the form of network packets separated at the IP level. Raw data is used for analysis. After collecting and analyzing data, each action is checked for anomalies. If an anomaly is detected, a notification appears, otherwise the algorithm considers the action or data normal (Fig.. 2).

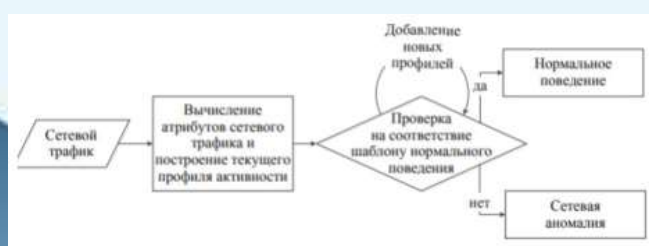


Figure 2. Network anomaly detection scheme

Even the most sophisticated systems have non-networking combined with IDS to recognize and prevent phishing attacks [8]. IDS is an information security tool designed to detect unauthorized access to an organization's information and telecommunications network, especially on the global Internet. IDS can be implemented at the level of individual nodes, providing protection for a specific host, or at the level of an entire organization's network or its subnets, providing overall protection. The most common detection methods include attack signature searching and anomaly detection. In

Fig. Figure 1 shows a schematic diagram of the operation of the IDS. Neural networks can be used within IDS. With their help, many tasks are performed. Neural networks can be trained from large amounts of network traffic data to recognize typical and anomalous activity patterns. It is possible to detect unusual traffic patterns associated with phishing attacks, such as redirects, data spoofing, or attempts to intercept information. This helps intrusion detection systems recognize phishing attacks early. Neural networks can analyze data received from IDS to identify phishing attempts. They can detect suspicious emails, web pages, URLs, and other elements typical of phishing attacks. This allows IDS to prevent and block phishing attacks, minimizing the risk to users and systems. Neural networks can continuously learn based on new data about phishing attacks, which are detected and blocked by IDS. This allows neural networks to update their models and algorithms to better recognize and prevent new types of phishing attacks. In addition, intelligent systems use machine learning to detect anomalies in network traffic. Anomaly detection method uses algorithms to analyze large amounts of data. It builds a picture and compares the data with the picture. If the data does not match the picture, it is considered an anomaly. In this case, network traffic is used as a data source. Network traffic data is presented in the form of network packets separated at the IP level. Raw data is used for analysis. After collecting and analyzing data, each action is checked for anomalies. If an anomaly is detected, a notification appears, otherwise the algorithm considers the action or data normal (Fig. 2). It is also possible to add or change normal behavior patterns manually or automatically [9]. Even the most complex systems have flaws. And artificial intelligence is no exception to this rule. Security is of utmost importance in the AI process. It must be integrated, starting with strategic planning throughout the cycle. Security aims to protect the privacy of users and their businesses from data leaks [10]. Many AI applications are based on huge amounts of data. And this data is often sensitive and personal in nature. The fact is that artificial intelligence systems rely on data and cannot do without it. The more artificial intelligence trains neural networks, the more vulnerabilities appear in the code. Systems become susceptible to data breaches and identity theft. To avoid data leaks, errors, and reputational risks, companies need to put AI security first. A possible solution is to thoroughly test artificial intelligence products and eliminate shortcomings before the products enter practice or enter the market [11].

Another problem is that the artificial intelligence algorithm analyzes huge data, which requires enormous computing power. Until now, the problem has been solved using cloud computing and parallel processing. However, as the volume of data increases and more complex deep learning algorithms emerge, today's computing power will not be enough to meet complex requirements. More memory and computing power will be needed to process huge amounts of data in exabytes and zettabytes. Also, modern artificial intelligence systems can learn things that are not what the developers intended. The performance of these systems depends heavily on the data on which they are trained. If there is unusual activity in the source data, the artificial intelligence may

perceive it as normal and not detect the anomaly. Of course, the system can be further trained during use, but such complexities must be taken into account and not ignored. The problem of repelling new cyber attacks is due to the fact that at the moment it is difficult for AI to predict the actions of cybercriminals. In this regard, other, less debugged artificial intelligence algorithms are used in cybersecurity. In the field of information security, using old data for training does not make much sense, while in traditional areas of artificial intelligence (face and voice recognition, machine translation, inventory management, autopilots) this approach is basic practice. The use of signature-based algorithms makes it possible to detect already known attacks without the participation of artificial intelligence [12]. The above problems are certainly not insoluble. However, this requires rapid development of technology and cooperation of people. Experts have a long way to go in developing principles, methodologies and frameworks to ensure that powerful technology such as artificial intelligence is not misused, which could lead to unintended consequences. References:

1. Avdeeva I. L., Polyanin A. V., Golovina T. A. Digitalization of industrial economic systems: problems and consequences of modern technologies //

News of Saratov University. New gray Ser. Economy. Control. Right. **2019. T. 19, issue 3. pp. 238–245.**

2. **Sharapova T. N., Selivanov S. A. Analysis of threats to information security and methods of its protection**

// Scienceosphere. Economic Sciences. 2021. No. 1(1).

3. **Korovin A. M. Intelligent systems: text of lectures. Chelyabinsk: SUSU, 2015. 60 p.**

4. **Classification of problems solved by IIS. URL: <https://studfle.net/preview/7411411/page:2/5>. Интеллектуальные системы управления информационной безопасностью / В. А. Табакаева, В. В. Селифанов, В. Р. Ан, С. А. Буларга, А.С. Ворожцов // Сборник научных трудов НГТУ. 2019. № 3–4 (96). С. 165–176.** 6. **Advantages of AI in Cyber Security. URL: <https://www.analyticssteps.com/blogs/6>**
7. **Роль искусственного интеллекта в кибербезопасности. URL: <https://vc.ru/dev/621020-role-iskusstvennogointellekta-v-kiberbezopasnosti>**

8. Depren O., Topallar M., Anarim E., Ciliz M. K. **АнИИДУСТРИАЛЬНАЯ ЭКОНОМИКА № 4, 2023 75 intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks // Expert Systems with Applications. 2021. № 29. С. 173.**

9. Kotov V.D., Vasiliev V.I. Current state of the problem of detecting network intrusions // Bulletin of the Ufa State Aviation Technical University. 2021. T. 16. No. 3 (48). P. 198-204.

10. Detection of anomalies in network traffic using machine learning methods / I. A. Ushakov, F. Kh. Ismoilov, A. E. Fedorova [etc.] // Current issues of modern science and education: collection of



articles of the XX International Scientific and Practical Conference . At 2 o'clock, Penza, June 20, 2022 Part 1. Penza: Science and Education (IP Gulyaev G.Yu.), 2022. P. 96-98.

11. “Arms race”: artificial intelligence and cybersecurity. URL:
<https://www.osp.ru/cio/2017/10/13053560>

12. Artificial intelligence: opportunities and threats. URL:
<https://www.it.world.ru/cionews/security/175459>.