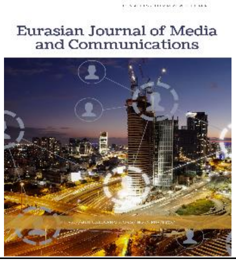

# The Importance of Artificial Intelligence Systems in Providing Information Security

**Mamasoliev Bakhodir Akhmadalievich**

Docent, Head of the department at the Academy of Armed Forces of the Republic of Uzbekistan

ABSTRACT

This article analyzes the importance of artificial intelligence systems in ensuring information security, and considers the main principles and importance of ensuring information security.

**Keywords:** information security, artificial intelligence, cyber threat, IT, information

Intellect is one of the concepts actively used in various fields of science, including computer linguistics, at the end of the 20th century and the beginning of the 21st century. At the same time, artificial intelligence is an interdisciplinary field, and in recent years this concept has been expressed side by side with computer linguistics. Artificial intelligence has an integrative nature, and its various forms and methods are used in a number of fields. Computational linguistics provides computer methods for studying speech and texts, and includes aspects of artificial intelligence, such as psychology, logic, and sociolinguistics.

The term "Artificial Intelligence" (AI) was officially used for the first time in 1955 within the framework of the conference. At this conference, for the first time, programs capable of playing chess were presented. 40 years later, the Deep Blue chess computer defeated world champion Garry Kasparov [2].

Today, when science and information and communication technologies are developing rapidly, in the developed countries of the world, modern information technologies are used in state and social management, economy, industry, social protection, education, medicine, employment, agriculture, defense, security, tourism and other fields. Wide use of artificial intelligence capabilities is becoming a tradition.

In our country, it has been set as a priority to take a place among the developed countries with innovative progress by 2030 through the development of information and digital economy.

It should also be noted that in the "Year of Development of Science, Enlightenment and Digital Economy" significant changes in information technologies and digitization were implemented and a number of important programs were adopted.

In particular, the decree of the President of the Republic of Uzbekistan "On measures for the widespread introduction of digital economy and electronic government", "On additional measures to automate the procedures for providing public social services and assistance to the population" and the decisions "On measures to create conditions for the rapid introduction of artificial intelligence technologies" and other regulatory legal documents are aimed at accelerating digitization in our country and introducing modern technologies into social and economic spheres.

With the decision of the President of the Republic of Uzbekistan on February 17, 2021 “On measures to create conditions for the rapid introduction of artificial intelligence technologies”, the program of measures for the study and introduction of artificial intelligence technologies in 2021-2022 is a clear example of this [3].

Actions taken by cyber security entities in relation to cyber security incidents can be carried out in the following forms:

eliminate vulnerabilities and errors in software and devices;

destruction of malicious programs, limitation of their spread, technical limitation of the source of cyber-attacks;

isolation of information objects from existing cyber threats;

providing information about cyber security incidents to law enforcement agencies [1].

Leading specialists and experts of the "Sber" group (Russia) were involved to participate as consultants in the development of artificial intelligence and in the activities of state bodies and other organizations, as well as in the preparation of the regulatory legal framework in this field. The number of cybercrimes is constantly and rapidly increasing. Thus, during the past year, the losses of the Russian economy from the activities of hackers amounted to about 6 trillion rubles. According to experts, criminals are often several steps ahead of information security specialists and law enforcement officers [4].

Artificial intelligence is one of the important components of modernity.

Due to the functionality and speed of execution of artificial intelligence, the digital economy paradigms, data processing and analysis that have emerged as a result of the creation of new systems are accelerating.

AI works by combining large amounts of data with fast, iterative processing capabilities and intelligent algorithms that enable programs to automatically learn from patterns and features in data. AI is a complex discipline with many theories, methodologies and technologies [5].

Artificial intelligence cannot do what humans cannot do. After all, the whole point of artificial intelligence is to create a machine that imitates human behavior. But AI can do things faster and analyze large amounts of data that would be too labor-intensive for a human. AI can automatically use sophisticated pattern recognition tools to detect signs of malware. Although artificial intelligence is not a powerful technology and cannot detect all threats, it is an important tool that reduces the time experts spend studying alerts. And this is perhaps the most important advantage of artificial intelligence.

In the last 3-5 years, the speed of development and changes in cyberspace amazes not only inexperienced users, but also experienced specialists in the field of IT and information security. Not even in the amount of data processed, the number of devices or applications/services connected to the Internet, but in the concepts and technologies themselves, in the comprehensive digitalization and the transition of most businesses online, there is an exponential development. The 2020 pandemic only accelerated this trend. Wide use of high- and ultra-high-level programming languages, powerful frameworks and development environments, development of cloud infrastructures and virtualization and containerization technologies allow to “assemble” a new application in an unprecedentedly short time. Cyber-threats are also increasing rapidly as attackers use such highly efficient development tools for their own purposes. This will bring the level of cyber countermeasures to a new level: if earlier the conflict with hackers could be described as a battle of minds and adaptive means of protecting information, now it will be between artificial cyber intelligence it can be called “battle of cars”.

The idea of artificial intelligence and research in this field - a scientific approach to the production of "intelligent machines" first appeared in a scientific group founded in 1956 based on the initiative of Professor John McCarthy of Stanford University (USA) [6].

The use of artificial intelligence in the field of information security and cyber security began in the early 2000s with very simple things, namely the construction of systems that facilitate the work of specialists of a certain profile, in particular, virus analysts. By this time, the number of malicious file samples had grown to such an extent that manual or simple automated analysis was no longer sufficient. These were systems that detected patterns (similarities) in malicious code and allowed at least minimal attribution. That is, they provided certain information to reverse experts and virus analysts, which allowed to assign this or that malicious program to a certain group or class. Actually, it was clustering and working with big data [7].

The use of artificial intelligence in information security is driven by two factors: the need for rapid response in the event of a cyber-incident and the lack of skilled cyber defense professionals. Indeed, in modern reality, it is very difficult to fill the staff list with qualified information security specialists with the necessary experience, and large-scale information security incidents can develop quickly: minutes often count. If the company does not have a round-the-clock estimate of information security analysts, then it will be difficult to provide high-quality protection outside working hours without a rapid autonomous response to cyber incidents. In addition, threat actors can implement distractions before their attacks, such as launching a DDoS attack or actively scanning the network. In such situations, a cyber-incident response system based on artificial intelligence helps, which allows processing a large number of information security incidents at the same time, automating the routine actions of information security analysts and quickly responding to incidents without human intervention [8].

To date, the scope of artificial intelligence to ensure information security is quite wide. There are global companies that analyze large amounts of data on the Internet that can reveal or predict new threats. These companies have systems that collect data sets, analyze them using AI-class technology, identify cluster data and predict threats. Without these technologies, it is almost impossible to process this amount of data. Of course, both neural networks and clustering are widely used here. AI systems are also used for threat monitoring, that is, they are used to predict information security threats based on data collected from open and closed sources. Thus, over the past two decades, the scope of tasks for applying artificial intelligence in the field of information security has grown significantly.

Today, artificial intelligence is no longer some kind of magic, but an effective assistant in protecting against cyber threats.

**Literature:**

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni. 2022-yil 25-fevral https://www.goethe.de/prj/umi/uz/the/sfi.html.
2. O’zR Prezidentining «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarori. PQ-4996-son. 17.02.2021y.
3. “Raqamli texnologiyalar: iqtisodiyot va ta’lim tizimini rivojlantirish tendensiyalari” mavzusidagi xalqaro ilmiy-amaliy konferensiya materiallari to‘plami. - 34.
4. Science and innovation international scientific journal. ISSN: 2181-3337. 2022 No. 2 - 35 p.
5. David Poole Alan Mackworth Artificial Intelligence: Foundations of Computational Agents, Cambridge University Press, 2010
6. A.Fishman. Искусственный интеллект: возможности и угрозы. Безопасность (IT-world.ru). Jurnal IT Manager. 01.06.2021
7. Ruslan Raxmetov Искусственный интеллект в информационной безопасности / www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti/