AXBOROT VA SUN’IY INTELLEKT TEXNOLOGIYALARINING JAMIYAT XAVFSIZLIGINI TAMINLASHDAGI O‘RNI

Meliev Mirobid Murodjon o‘g‘li
Biznes va tadbirkorlik oliy maktabi MVA yo‘nalishi magistranti

Annotatsiya: Maqolada sun’iy intelektning jamiyat taraqqiyotidagi o‘rni, xususan, davlat boshqaruvida, ishlab chiqarishda va boshqa jarayonlardagi faoliyati ilmiy-nazariy jihatdan tahlil qilib berildi. Hozirgi kunda axborotlarning istemochilari talabini qondirishda tabiiyki ularni xavfsizligini himoya qiladigan kiberhujumlarni olidini olish va unga qarshi turaoladigan mexanizmni yaratishni taqozo etadi. Biz ayni mana shu jarayonlar tahlili bayonini keltirdik.

Kalit so‘zlar: Global, internet, suniy intelekt, axborot xavfsiziligi, kiberhujum, kiberjinoyat, super aql.

Annatation: In the article, the role of artificial intelligence in the development of society, in particular, its activity in state management, production and other processes was analyzed from a scientific and theoretical point of view. Today, meeting the demands of information consumers naturally requires the creation of a mechanism capable of preventing and countering cyberattacks that protect their security. We have provided a statement of the analysis of these processes.

Keywords: Global, internet, artificial intelligence, information security, cyberattack, cybercrime, super intelligence.

In the global world, the intensive penetration of the Internet and digital technologies into our lives leads to an increase in crime (cybercrime) and excessive freedom in the development of society. The world does not choose a place - today it has an impact on the minds of all sections of the population, especially on the minds of children who are just growing up. Humanity today could not imagine fulfilling its wishes without the Internet. At the same time, digitized technologies ensure uniform fulfillment of daily work norms, which leads to violation of existing labor norms (mental and physical labor) among people. Just imagine what changes may occur in world civilization by the next 2040s. Unfortunately, the "artificial intelligence", which is expected to become the owner of everything, puts us in a situation where humanity is already ready for such digital changes. In this regard, cybercriminals are developing their cyberattacks at a more aggressive level using digital technologies. Due to the COVID-19 pandemic, the transition of organizations to virtualized information and communication technologies and the introduction of online services to the population has also shown a unique shift in cyber attacks on the information resources and network infrastructures of organizations.

Research shows that theft of money (in a plastic card or account number), intellectual property, personal and financial information, online fraud, hacking and destruction of information resources and systems, damage to reputation, etc. the global damage of a number of cybercrimes in 2022 is 8.44 trillion. If it consisted of US dollars, by 2027 this indicator will be 23.84 trillion. It is expected to reach USD[1].

In this regard, cyber-attacks on web resources in our country are increasing more and more. According to the analysis of the data collected in the automated protection systems against local or global network attacks, in 2022, network attacks were carried out in 2022 on the web resources of state organizations in cyber protection, and timely blocking was ensured.

Introduction of innovative technologies in the practice of statistics based on the decision of the President of the Republic of Uzbekistan on April 9, 2019 "On additional measures to ensure the openness and transparency of the state administration and increase the statistical potential of the

[1] O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston –2030 strategiyasini tasdiqlash va uni samarali amalga oshirish chora -tadbirlari to‘g‘risida” 2020 yil 5 oktabrdagi PF-6079-son Farmoni.

country" No. PQ-4273 a number of information resources and systems such as e-stat - information system for receiving state statistics reports, "Selective observations" information system, DLP - information system for preventing information leakage were launched. The official website of the Statistics Agency - stat.uz is used by more than 4,000 visitors per day on average, more than 500,000 legal organizations submit statistical reports in electronic form through the e-stat information system, and over a month through the "Selective Observations" information system. Considering that the prices of more than 1.2 million goods and services are studied per year, it is not difficult to imagine how big the damage of cyber-attacks on the websites and information systems of the Agency of Statistics will be.

The ongoing measures show that the monitoring of constantly emerging cyber threats to the information systems of the Statistics Agency requires many highly qualified specialists. But the effective implementation of artificial intelligence technologies in the processes of ensuring information security can take over a part of the work of specialists. Because artificial intelligence can find vulnerabilities in information systems and networks, encode and identify threats at high speed. The perimeters of human-controlled information systems are expanding, and the detection of threats and vulnerabilities and the protection of data are becoming a huge problem.

The advantages of using artificial intelligence in statistical data security are as follows:

First, threat detection: In this regard, AI-based systems can analyze large amounts of data from various sources, such as network traffic, logs, and user behavior, at high speed to detect anomalies that indicate cyber threats. This allows faster and more accurate detection of anomalies and potential threats in real time compared to traditional systems. By automating the threat detection process, artificial intelligence is able to identify correlations that human analysts may miss, resulting in greater efficiency in detecting cyberattacks.

Second, robust incident response: In this, AI can help more effectively respond to, contain, and mitigate cyber incidents by automating certain tasks such as analyzing information security logs, data correlation, and alert prioritization . Artificial intelligence tools can analyze the nature of the attack, determine the most effective response, and even initiate remedial actions.

Third, predictive analytics: It is by analyzing historical data and learning from past security incidents that AI can help predict and prevent future attacks. This enables organizations to proactively address vulnerabilities and improve their overall security posture.

Fourth, security automation: For example, artificial intelligence can automate repetitive and time-consuming tasks such as log analysis and vulnerability scanning, freeing information security professionals to focus on more strategic issues. frees up valuable time.

Fifth, advanced risk assessment and management: These processes demonstrate the ability of artificial intelligence algorithms to process and analyze large amounts of data from various sources, such as user behavior, network traffic, and device configuration, to identify potential vulnerabilities and assess overall risk.

Scientific research conducted in recent years shows that today there are three main types of artificial intelligence:

a) Weak artificial intelligence - programmed to perform a single task, such as watching the weather, playing chess, or analyzing corporate data. Such artificial intelligence can work in real time, but it uses only a limited set of data. As a result, this system can only solve the specific problem it is trained to solve.

b) Strong artificial intelligence - similar to human intelligence. In other words, he can successfully perform any mental task and has the cognitive abilities that humans can, including consciousness.

c). Super artificial intelligence is defined by philosopher Nick Bostrom as: "Any intelligence that is significantly superior to human cognitive abilities in almost all domains." Super intelligence (artificial intelligence) will be superior to humans in all aspects - from creativity to life wisdom and problem solving. Machines can display intelligence that we have not seen in even the most capable representatives of humanity.

In conclusion, with the help of artificial intelligence in our society and public administration, anti-cyber attack systems will work more reliably and faster, which will increase the confidence of users of official information and allow to drastically reduce the costs of ensuring information security in state and non-state organizations.

Artificial intelligence can protect, monitor and prevent 99% of malware attacks in hybrid environments.

In addition, if artificial intelligence is based on cloud technology, when the load on information systems increases dramatically (for example, when hackers "attack" a server), artificial intelligence will automatically expand the perimeter of information security in the "cloud".