Artificial Intelligence Technologies And Their Importance In Ensuring Cyber Security

Djamatov Mustafa Xatamovich, Senior Lecturer, Department of digital technology and Information Security, Ministry of Internal Affairs Academy,

Shukridillayeva Sevara Elmurod qizi Cadet of the Academy of the Ministry of Internal Affairs.

ABSTRACT

This article will focus on AI technologies and their role and importance in ensuring cybersecurity. The article examines the aspects of cybersecurity enforcement, information security, and the use of artificial intelligence technologies in cybersecurity.

Keywords: Artificial intelligence, artificial intelligence technologies, cyber security, cyber attacks, smart machines.

In the modern world, new technologies, electronic services have become an integral part of our daily life. In today's conditions, when science and information communication technologies are rapidly developing, the widespread use of the capabilities of modern information technology and artificial intelligence technologies in the world's developed countries in the field of state and Society Management, Economics, industry, social protection, education, medicine, employment, agriculture, defense, security, tourism and other areas is entering the urf. Given that society is becoming addicted to Information Communication Technologies day by day, the protection of these technologies and the use of houses have become a crucial and very relevant topic for the national interest.

Cybersecurity is one of the concepts that has just entered. Specifically, the CSEC2017 Joint Task Force source defines cybersecurity as: cybersecurity is an area of knowledge based on computations that embodies technology, human, information, and processes in itself to guarantee proper execution of actions in the context in which the disruptors exist. It includes the creation, implementation, analysis and testing of secure computer systems. In contrast, Cisco, a network-based organization, has defined cybersecurity as: cybersecurity – the practice of protecting systems, networks, and applications from digital attacks. These cyberattacks usually aim to manage, exchange or destroy confidential information; extort money from users; disrupt normal performance. Currently, the implementation of effective cybersecurity measures is becoming more complicated from a practical side as a result of an increase in the number of devices and their types and the potential of intruders than human beings.

Cybersecurity is the first time that the need for the field of knowledge began to emerge from the time mainframe computers were developed. In this case, multi-level security measures have been implemented to protect these devices and their functions. The increase in the need to ensure the security of the state

was the reason for the emergence of complex and technologically complex reliable security measures.

To date, every field that exists in our lives is digitized, even living a life based on digital management, from our birth to our death. On the basis of such digital technologies, incomparable comfort is created for us in our way of life. Unfortunately, there are also negative situations behind these amenities. For example, the devaluation of an individual, the spread of personal information around the world, the victimization of human fraud, is becoming easier than ever. The root cause of this is also precisely the digital world. M. In 1995.In the introduction to Ethan Katsh's Book, “law in the digital world”, a sentence is recited by William Gates: “in the future, everything will be digital” (Katsh, 1995). Many years have passed, and we see confirmation of this thought.

As a result of the achievements of Science, Information Technology has developed rapidly, creating technology-artificial intelligence technologies that allow a computer or information system to realize a person's ability to think. On the initiative of Stanford University professor John McCarthy in the field of artificial intelligence (AI) and its research, the concept of creating "intelligent machines" within the scientific community emerged in 1956. The term "intelligence", which comes from the Latin word "intellectus", denoting understanding and understanding, lies in the core of artificial intelligence. 1 given that there is no consensus on the definition of artificial intelligence and that the technology that can be understood under this unusual term is changing rapidly, it is not easy to give a single and clear definition of artificial intelligence 1 https://uz.wikipedia.org/wiki/Sun%CA%BCiy_ong#cite_note-FOOTNOTEGoogle2016-1 at present, artificial intelligence is rapidly developing, covering various areas of human life activity, being tested and implemented in practice in different areas. The technologies used make it possible to carry out something unimaginable even with science fiction a few years ago.

The process, which is now called the “new industrial revolution” by us, also poses a real danger on the other hand, if it is of positive importance on the one hand, as it presents a new society, a new environment. Despite the unprecedented development, the internet has brought us new manifestations of fear, new forms of risk. The complex nature of the crime that takes place in the borderless area of cyberspace is complicated by the increasing number of organized crime groups, and the new appearance of crime under the influence of these factors is becoming more and more dangerous.

What is cybersecurity, how to create and provide it? The concept of cybersecurity refers to the protection, protection of the digital environment from various external risks. More specifically, cybersecurity is a set of tools, policies, security concepts, security guarantees, guidelines, risk management approaches, actions, trainings, best practices, trust and technologies that can be used to protect the cyber(digital) environment and organization and user assets. It includes computing devices connected to organization and user assets, personnel, infrastructure, applications, services, telecommunication systems and the sum of data transmitted or stored in a cyberspace. Cybersecurity seeks to achieve and ensure the maintenance of the security characteristics of the organization and user assets.

At present, measures are being taken by all states aimed at the development of cybersecurity. Today, the implementation of effective cybersecurity measures is becoming more complicated from the practical side as a result of an increase in the number and type of devices and the potential of intruders than in humans.

Cyber security is divided into 8 areas of knowledge:

1. Data security;
2. Software security;
3. Founders safety;
4. Communication security;
5. System security;
6. Human security;
7. Organization security;
8. Social Security.

Indeed, Uzbekistan was among the developing countries. Therefore, the economy

of our country and other sectors of the scale are digitized. The process of digitization is underway, from the banking sector to the medical sector, from the military to agriculture. This certainly raises security issues for the National Information System. In particular, information on the policy and military areas should not be disclosed at all. However, due to insufficient attention to cybersecurity in our country, cyberattacks and non-stop activities are being carried out in relation to the official Internet network of Uzbekistan.

In particular, to date, the absence of a state higher education institution, schools, lyceums and colleges that train cyber security specialists has a negative impact on the quality of personnel. The failure of the competent authority regulating cybersecurity to develop a unified methodology for training personnel, the absence of uniform qualification requirements to date, the failure of personnel to be prepared on a systematic basis, the failure of preschool education, school, Lyceum, College, Higher Education Institution, post-higher education on a consistent basis is causing a shortage of personnel in the field. For this reason, to date, a mechanism has been created for accepting candidates for cybersecurity units of the internal affairs bodies without physical training, due to the shortage of personnel, the demand for personnel with all-round potential to this day is huge in Jud in our country.

It is extremely necessary to strengthen the legal framework for cyber security. The digital world has not yet been able to accurately determine its status legally. The fact that new types and forms of threats appear from day to day requires the need to reflect them in the legislation. The development of a national strategy for cybersecurity regulates activities in the field of anti-crime construction in the National Cyberspace. After all, the harm and danger of crime in the virtual world is no less than in the real world.

On February 25, 2022, the law on cybersecurity was adopted in Uzbekistan in order to regulate relations in the field of cybersecurity. The law provides the following as the basic principles for ensuring cybersecurity:

- lawfulness;
- priority of protecting the interests of the individual, society and the state in cyberspace;
- the only approach to the regulation of the sphere of cybersecurity;
- priority of the participation of domestic manufacturers in the creation of a cybersecurity system;
- The openness of the Republic of Uzbekistan to international cooperation in ensuring cybersecurity.

In our opinion, as the only solution to these problems, the training of highly minded personnel in this direction, who are well versed in National, International foreign experience, improving the cybersecurity sector, should go from the bottom of the balcony to the top, not from the top link. Also, for organizations that want to succeed online today, AI is the best option for cybersecurity. AI algorithms are also powerful pattern recognition tools with a significant advantage over outdated list-based security methods. By identifying emerging threats that indicate alarming patterns, AI improves and surpasses these systems. This level of AI experience requires a large amount of learning and is only possible with reliable data sources for each risk vector. Artificial intelligence helps professionals solve a variety of problems, some of which are related to cybersecurity. Artificial intelligence and machine learning can help businesses fight hackers and secure their networks, systems and data by detecting automated threats, responding to threats faster than simple software-enabled methods, etc. In order to work effectively and protect their organization from cyber attacks, security professionals need significant support from advanced technologies such as smart machines and artificial intelligence. As an example of the security measures of innovative artificial intelligence technologies, we can say face recognition and identification.

Also, any scientific discoveries to be made in this area should be carried out in order to preserve universal values and serve to

further strengthen it, thereby taking the path to achieve common interests by further improving the living conditions of people. As artificial intelligence enters our lives intensively, there is a need for a certain set of rules in its impact on human life. In this regard, a number of countries, especially China, the United States and the European Union, have had time to develop common mechanisms. Experts point out that among these, in addition to the fact that the mechanisms for the legal regulation of Artificial Intelligence in Europe, which are expected to have the widest impact on the world, are the most promising, the EU is given responsibility by kata. In this regard, Uzbekistan has already taken a number of initial steps, realizing how important this industry is, especially in Uzbekistan —the president's decision to create conditions for the rapid introduction of artificial intelligence technologies also adds advanced innovations in this field in our country, ensuring the possibility of effective use of digital data and their high quality, a program of a number of practical measures has been approved, which should be carried out in order to create favorable conditions for the training of qualified personnel in this area. But this process is only the first effort in which the kata database (big data) plays a high role in the development of this process at maximum speed. In addition, personnel who are able to correctly apply regulatory norms are also important in their place. However, artificial intelligence technologies can also cause a number of harmful consequences listed below:

- the presence of errors in AI-generated results due to limited knowledge bases;
- Relying on human intervention when AI systems have difficulty making decisions;
- the emergence of heavy costs associated with artificial intelligence systems.

In general terms, in today's much faster-moving digital world, first of all, the security of the individual, as well as the data, depends in every way on the scale of the measures being taken and the level of influence. As noted above and analyzed, cybercrime is becoming one of the most dangerous enemies of society and the state. And in the fight against it, it is required to introduce the most effective systems, put into practice and strengthen integration. Another important aspect is noted as cybersecurity, digital law and the formation of digital hygiene, making it an integral part of everyday life a requirement of the time.

References.

1. Ganiyev S.K. “Kiberxavfsizlik asoslari”. O‘quv qo‘llanma.
2. Thomas A.Johanson. “Cyber-security, Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”.
3. Niall Adams, Nicholas Heard. “Data Analysis for network cyber-security”.
4. O’zbekiston Respublikasi prezidentining “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to’g’risida”gi qarori. 2018 yil 21 noyabr, PQ- 4024- son.
5. www.itu.int - Xalqaro elektroaloqa uyushmasining rasmiy sayti
6. https://tace.uz - Kiberxavfsizlik markazi davlat unitar korxonasi rasmiy sayti 6. https://perconcordiam.com/perCon V10N4 RUS.pdf.
7. https://lib.itsec.ru/articles2/job/defitsit-kadrov-v-sfere-ib-ipodgotovkamolodyh-spetsialistov.
8. O‘zbekiston Respublikasi Prezidentining 2021-yil, 17 fevraldagi PQ-4996-son qarori
9. Patri A.K. (2009). Cyber Law. Lucknow.
10. Akbarov D.Y.Axborot xavfsizligini ta’minlashningkriptografik usullari va ularning qo‘llanilishi. – Toshkent, “O‘zbekiston markasi” nashriyot, 2009-432 bet.
11. Rakhimjon, H. (2022). 6 NEW PROGRAMMING LANGUAGES TO LEARN. Academicia Globe: Inderscience Research, 3(04), 126-135.
12. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, U.Xolimtayeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. T: M.Ulug‘bek nomidagi OzMU, 2018-144 bet.
13. Yar, Majid, and Kevin F. Steinmetz. (2019). Cybercrime and society. SAGE.

14. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: «Aloqachi», 2020, 221 bet.
15. Goodman, Brenner. (2002). The emerging consensus on criminal conduct in cybercrime. International journal of law and information technology, 144.
16. Gercke D.M. (2012). Understanding cybercrime: phenomena, challenges and legal response. Geneva: International Telecommunication Union (ITU). 17. https://hashdork.com/uz/artificial-intelligence-in-cybersecurity/