International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 5 Issue 4, April - 2021, Pages: 79-82

The Use Of Artificial Intelligence In Data Security

Dilmurod Rakhmatov

Student of the Department of Applied Mathematics
Jizzakh branch of National University of Uzbekistan
Jizzakh, Uzbekistan
rakhmatov@workmail.com

Abstract: *An analysis of possible ways to use artificial intelligence in the field of information security was conducted. Conclusions have been drawn about the possibilities of using this high technology to prevent unauthorized access to data, as well as to reduce the consequences of information security breaches.*

Keywords— cybersecurity, information security, artificial intelligence, data, information**.**

1. INTRODUCTION

Information security, taking into account the increasingly widely implemented and used computer systems, occupies an important place in the modern world. Everyone, whether an individual or a company, wants to reduce the threat of theft, deletion, or alteration of their information. Including in the automated system, cybersecurity plays an important role.

According to an IDC study, "organizations will spend $ 101.6 billion by 2020 on cybersecurity software, services and hardware."

Leading organizations integrate dozens of security products, but nevertheless fear being vulnerable to attacks. This indicates that even after increasing security spending, security breaches show no signs of stopping or slowing down.

The introduction of advanced technologies in the field of cybersecurity takes time, which allows attacks to be detected in detail and resolved faster than cybersecurity specialists, such technology can be artificial intelligence. AI is a technology that, among other things, can detect threats and automatically take the necessary actions to eliminate and prevent them.

2. MAIN PART

As a result of the information revolution, a fundamentally new type of society is being created, with its own laws and principles of functioning, as well as risks and threats. This type of society, called the "information society", is characterized by a violation of linearity, continuity, stability and predictability of social development, which fundamentally distinguishes it from all previous types of society that existed in the history of our civilization. This society, created by the domination of information and its total influence on the consciousness and behavior of individuals, has the highest potential for scientific and technological development, but, at the same time, contains an equally high potential of threat to the security of society.

In the conditions of the formation of the information society, ensuring national security presupposes the need for a deep understanding of the specifics of this type of society, which consists in the fact that information and knowledge acquire a special status, becoming the main strategic resource for the development of society and the state. Therefore, for access to this resource, a competitive struggle unfolds in various spheres of society (politics, economy, culture, etc.) and at various levels (international, state, public). Penetrating deeper and deeper into various spheres of public life, modern information technologies not only affect the consciousness and behavior of individuals, but also determine the overall lifestyle of the individual and society, the nature of relations and interactions, as well as trends in the development of the economy, politics, culture, education, etc.

Five and a half decades ago (1956), the term Artificial Intelligence (AI) was proposed by J. McCarthy, a 29-year-old associate professor at Stanford University, an eminent computer science theorist and creator of the Lisp language. At that time, artificial intelligence was represented by a very modest set of programs, the authors of which set themselves a daring goal - the creation of intelligent, thinking computers capable of reaching and surpassing humans in their intellectual capabilities.

The phrase artificial intelligence, unsuccessfully translated into the Uzbek language, does not mean some kind of artificial entity endowed with a human mind, but rather the processes of thinking and reasoning, artificially recreated. In the English language there is a noun intellect, which is derived from the Latin intellectus (intellect, understanding, meaning, conception, idea - intellect, concept, meaning, understanding, cognitive ability), the meaning of which reflects the understanding of things. But the author of the phrase chose another word - intelligence, in which the suffix - ence (like the suffixes -ance, -ancy, -ency) is of Latin origin and allows nouns to be formed from verbs, for example: appear - to appear, appearance - to appear; depend - to depend; dependence - dependence. If intellect as a verb means in the aggregate "to understand", "to know", "to acquire and apply knowledge", "to think", "to reason reasonably", then the noun intelligence means "the ability to understand", "the ability to know", "the ability to think", " the

ability to acquire and apply knowledge". And the translation of the phrase from the end to the beginning, as is usually accepted in the English Uzbek translation, gives something like "the ability to cognize, think and reason rationally, recreated artificially." Moreover, the root "intelligence" in the word intelligence means a set of skills, abilities and qualities inherent in a person and is a common integrative property.

So, the founders of the new scientific direction of informatics, first of all, set themselves the goals of comprehending, identifying and formalizing the intellectual and thinking abilities of a person with their subsequent implementation on a computer.

The authors of the article agree with the point of view of artificial intelligence as a scientific direction, the purpose of which is to create artifacts that not just copy, but surpass the intellectual abilities of a person to solve industrial, technological and social problems. The development and widespread use of computational algorithms that differ from natural intellectual processes, but which allow achieving results, can be compared to solving the problem of "artificial flight". It was only after the Wright brothers and other researchers stopped imitating birds and began studying aerodynamics that it became possible to create systems aimed at solving the industrial, social and military needs of mankind. At the same time, the borrowing of natural mechanisms made it possible to qualitatively improve the existing engineering solutions. So, the wing lift is reflected in the presence of wide-open wings of airplanes and hang-gliders, the retractable landing gear is similar to shaking the paws during flight, the use of helicopter propeller blades is comparable to the high-frequency movement of the wings of a hummingbird, "hovering" over a flower or a kingfisher "hovering" over the water in anticipation extraction. The use of the mechanisms of natural selection, crossing and mutation was reflected in the creation of a family of computational algorithms, called genetic, and which made it possible to solve multidimensional optimization problems in a wide variety of fields of technology, economics, and finance.

In the overwhelming number of definitions of intelligence, its most important and significant component is the process of thinking, which, like intelligence, also has the property of integrality. Are we able to comprehend all its mechanisms and features of thinking? Are thinking processes subject to formalization for subsequent reproduction in computational procedures? Is it possible to create such procedures, the result of which will surpass a person not only in speed, but also in quality characteristics, such as consistency, rationality, noise immunity (in the sense of incompleteness and inaccuracy of the initial data)? Is it necessary and possible to realize in computational procedures the ability to develop thought processes or to immediately recreate the ideal mechanism of thinking? If necessary, how? The authors tried to give answers to these and similar questions in this work, as well as to provide an overview of projects to create software and hardware "cognizing, thinking and reasonably reasoning" systems built on the basis of copying the biological and mental abilities of the bearer of natural intelligence.

The technology of reading a person and transferring from a biological to a computer matrix, according to some forecasts, the work will be implemented in practice by 2020-2050. Progress in the performance of transistors will allow the computer to equal the power of the human brain in ten to fifteen years. What are the possibilities of this artificial carrier of our knowledge, thoughts and feelings? How many times will his capabilities surpass those of a person? Is it dangerous for humanity? If so, what threats does the dynamic development of artificial intelligence pose to humanity and human civilization as a whole?

AI-powered tools meet a variety of cybersecurity needs.

1. Biometric authentication.

Passwords can be cracked, compromising sensitive information of a user, company, or government agency. This is where AI-based authentication, whether it is fingerprint and palm scanning, is much safer and the system can scan them reliably. When biometric logins are associated with passwords, the likelihood of user data being compromised is significantly lower.

2. Acceleration of threat detection.

Conventional cybersecurity systems are not capable of handling different types of malware at the same time. In addition, not only the cybersecurity bar, but hackers have also raised the standard. To quickly identify advanced threats, you need to use advanced security tools that can address these issues.

Companies are adopting AI-driven systems that can easily detect threats through pattern recognition using advanced algorithms and codes that are constantly updated.

AI combined with machine learning is effective in analyzing site crawl paths, micro-behavior of malware, and any malicious activity that further helps decision-making.

3. Fast response to attacks.

Simply identifying threats in real time is meaningless if the system is unable to combat and prevent threats before they cause minor damage to the system.

When a team of hackers attacks a system from different points, the AI immediately connects the dots and automatically suggests plans to prevent the attack. AI uses intelligent analytics, which is a simpler and faster approach to detect and remediate attacks. For example, when the AI system finds a malicious file on the system, it predominantly isolates the file from the system.

4. Creation of a dynamic environment for authentication.

Data can also be intercepted on networks. This is an alarming situation for employees who gain remote access to

systems, which means that traditional authentication models are no longer secure. This is where AI comes to the rescue.

AI systems create a global real-time authentication environment that changes access privileges according to location or network using multi-factor authentication. This includes collecting data and analyzing user behavior in the application, device and network when accessing data remotely.

5. Reducing human participation.

No machine can surpass the creativity, imagination and thinking ability of humans. But decisions made by engineers are also backed up by the right set of data, opinions, and current trends.

Examining and using meaningful data is time-consuming and instantly impossible to solve a high-risk problem.

When companies build a secure application that uses AI technology, security personnel will get a breather by automating the detection and prevention of security threats without human intervention.

Continuous analysis of user behavior, in addition to predictive analytics, reduces engineer intervention to protect systems from a series of attacks. The time saved can be invested in creative and rewarding endeavors.

However, artificial intelligence systems are trained and operated by humans, and in some places the need for human engineers is mandatory, as they are able to go beyond anomalies that machines cannot detect and confirm that the alleged attack is genuine.

3. Conclusion

Thus, at the moment, the info communication infrastructure of Uzbekistan is in the strongest dependence on foreign manufacturers and developers, actively introducing their solutions (from software libraries to hardware platforms and control systems).

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

Artificial intelligence makes a significant contribution to the fight against modern information threats. In particular, in most cases, the introduction of AI technologies in the information security of the organization reduces the time to identify problems and respond to incidents, as well as the costs of personnel management. Operators have noted an increase in the efficiency of detecting unknown threats, as well as in the speed of analysis and detection of malicious activity on endpoints and applications.

The total investments in companies that create information security products using AI technologies amount to $ 3,749 million at the end of 2019. At the same time, the global market for information security products using AI technologies will reach $ 30 billion in 2025 with an annual growth of 23%.

4. Acknowledgement

This research was supported by my supervisor, DSc, Professor Akmal Akhatov. We thank our colleagues from the Department of Applied Mathematics and Computer Science in the Jizzakh branch of National University of Uzbekistan who provided insight and expertise that greatly assisted the research.

5. References

[1] Rakhmatov Dilmurod, Akhatov A., & Rakhmatov D. (2020). Research on Effective Ways to Intelligence Quotient of Perception Through Mobile Games. The American Journal of Applied Sciences, 2(08), 89-95.

[2] Rakhmatov Dilmurod & Nomozova Elmira. (2020). The use of multimedia technologies in the educational system and teaching methodology: problems and prospects. International Journal of Discourse on Innovation, Integration and Education, 1(2), 28-32.

[3] Rakhmatov Dilmurod & Akhatov Akmal. (2020). Distance learning system in the higher education system of Uzbekistan: hybrid technology. Vol 6 (2020): Conference of Management of Islamic Education Leadership in The Era of Revolution 4.0, 150-153.

[4] Rakhmatov D.R., Artificial intelligence: today and future. Материалы V Международной научно-практической конференции «Наука и образование в современном мире: вызовы XXI века». Состоявшейся 12 декабря 2019 г. В г. Нурсултан, Казахстан, Мцнс «Бобек». с. 19-23

[5] Рахматов Д.Р., Прикладные космические исследования на основе нейронных сетей: идентификация новых экзопланет и космических объектов, Студенческий вестник: электрон. научн. журн. 2020. № 16(114). с. 74-77

[6] Рахматов Д.Р., Ахатов А.Р., Сунъий тафаккурнинг инсониятга таъсири: ютуқ ва инқирозлар тахлили. "Этика ва эстетиканинг долзарб масалалари" даврий журнали 2021. № 5.

[7] Рахматов, Д., & Ахатов, А. Р. (2020). Кибер жиноятларни юзага келиш омиллари ва кибер этика: муаммо ва истиқболлар. Science and Education, 1(1), 227-234.

[8] Dilmurod, R., & Fazliddin, A. (2021). Prospects for the introduction of artificial intelligence technologies in higher education. ACADEMICIA: an international multidisciplinary research journal, 11(2), 929-934.

[9] Юсупов, Р. М., Рахматов, Д. Р., & Рахматов, Д. Р. (2020). Безопасность мультимедийной коммуникации с использованием криптографии. безопасность, 20(10).

[10] Mosteanu, N. R. (2020). Artificial intelligence and cyber security–face to face with cyber attack–a maltese

case of risk management approach. Ecoforum Journal, 9(2).

[11] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[12] Mosteanu, N. R. (2020). Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. Quality-Access to Success, 21(175).

[13] Demertzis, K., & Iliadis, L. (2015). A bio-inspired hybrid artificial intelligence framework for cyber security. In Computation, cryptography, and network security (pp. 161-193). Springer, Cham.

[14] Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. International Journal of Cyber Criminology, 13(2), 564-577.

6. AUTHOR INFORMATION

Dilmurod R. Rakhmatov, Bachelor degree in Computer Science from Jizzakh branch of the National University of Uzbekistan. Currently, he is mobile developer in the Include LLC. He has published about 50 research papers in proceedings of international conferences, workshops and archival journals, and also about 4 certificates about official registration of software in State Patent Department Republic of Uzbekistan. His research interests include information technologies, modern education technology, mobile technology, artificial intelligence, cyber security, deep learning and machine learning. During the period of his activity he is engaged in research of a digital economy and artificial intelligence. He was a laureate of the Scholarship of the Hokim of Jizzakh region, established for students in 2020. He is a winner of the grant One Million Uzbek Coders and holder of the badge "Best Student of the CIS". He actively participates in reports at the scientific and methodological seminar, reads lectures. He is a speaker at more than 20 conferences and seminars on modern professions. He is a President of the Student Council, a member of the Student Association of Uzbekistan.