CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 04 Issue: 04 | Apr 2023 ISSN: 2660-5317
https://cajotas.centralasianstudies.org

Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems

Tojimatov Dostonbek

Senior teacher, Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khorazmi, Fergana, Uzbekistan

Mirzaev Jamshid

Assistant, Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khorazmi, Fergana, Uzbekistan

Received 28th Feb 2023, Accepted 23rd Mar 2023, Online 17th Apr 2023

Abstract: *This article proposes ways to prevent cyber-attacks and emergency situations with a high probability of occurrence using the capabilities of artificial intelligence (AI) in the early detection of threats to the information systems of enterprise organizations. The article presents the important elements for the development of a smart protection system that includes the analysis of the possible origin of natural and artificial threats, threat isolation, level determination, and decision-making functions.*

Keywords: *cyber attack, emergency, geophysical event, geological event, threat, cyber criminal, intelligent defense system, Machine Learning (ML), hacker, firewall.*

Introduction

It is known that threats are divided into natural and artificial types. The study of threats in the field of information security is considered very important, and the elimination of possible damages to enterprises and organizations depends on identifying the threat and reducing its impact by correctly assessing its level.

A natural threat is a process that causes an extraordinary situation with a high probability of occurrence due to natural phenomena. Sources (carriers) of natural hazards are parts of the lithosphere, hydrosphere, atmosphere and space where various unfavorable natural processes occur and dangerous natural phenomena can occur.

Dangerous natural phenomena that are sources of natural emergency situations can be divided into:

- dangerous geophysical events (earthquakes, volcanic eruptions);

- dangerous geological phenomena (landslides, erosion, washing of slopes, institutions);

- dangerous hydrometeorological phenomena, including meteorological (hurricanes, hurricanes, tornadoes, very heavy snow, hail, rain, fog, extreme cold, heat), agrometeorological (frosts, dry winds, soil and atmospheric drought), hydrological (floods, glaciers, traffic jams, floods), marine hydrological and heliogeophysical hazards (strong magnetic storms, strong disturbance radiation situation in the ionosphere with the interruption of short-wave communication) and asteroid-comet hazard;

- natural fires[1].

Usually, natural threats are not considered a cyber threat, but when an emergency situation occurs, the damage it causes to the information systems of enterprises and organizations can be much higher than that of a cyber attack.

Natural threats have little direct impact on information systems, and mainly cause damage by destroying the devices on which the system is installed. Therefore, in the development of security systems, it is appropriate to take measures aimed at identifying natural threats and preventing emergency situations.

Artificial threats directly depend on the person and are divided into types of accidental or intentional threats.

Accidental threats arise due to carelessness, carelessness, ignorance, hiring an untested employee, errors in technical and software systems. Such threats are considered aimless and it is difficult to determine in advance the damage they will cause to the enterprise-organization [2].

Intentionally organized threats are aimed at a specific goal and are divided into internal and external threats. Internal threats mainly include mercenary spies and threats of revenge. External threats include potential cyber attacks and computer viruses. Intentionally organized threats are aimed at destroying enterprise-organizational information systems, disrupting their stable operation, stealing, copying, and changing data[5].

Methods of reducing the impact of threats. Enterprise organizations with any valuable asset use security methods using various physical and hardware tools to protect information systems from potential threats. As an example of physical protection methods and means, a protected area (wire fence, concrete wall), durable object (building), security service (guard, security guard), surveillance cameras, signaling devices, information system safe room, door locks, fire extinguishers, ventilation, heating or cooling systems. Hardware and software tools are directly connected to information systems and the computers on which they are installed. These include inter-network screen tools, network routers, switches, antivirus programs, network analyzers, anti-ddos attack tools, and cryptographic methods, authentication methods, and role-based methods used in the information system [3].

While all existing methods for protecting information systems are currently considered robust, they have the ability to detect threats when they already exist or when they occur. In addition, the management of such tools depends on the human factor. This leads to a loss of time in distinguishing types of threats aimed at information systems and choosing methods for protection. Sometimes the right protection systems are put in place after the threat has occurred. Until then, threats have damaged information systems[8]. Currently, hackers are widely using artificial intelligence in many attacks. This makes existing systems vulnerable to tolerance levels. Through machine learning systems, neural networks

perfectly learn protection systems and reveal their weak points. In some cases, it tries to confuse protection systems by creating a fake threat[4].

Early detection of threats gives us the opportunity to study the specifics of the type of threat, assess its consequences and take the necessary measures against it. But cyber threats to the information system occur at a much higher speed [6]. Because the speed of information exchange and calculation on a computer is higher than the human factor. For this reason, early detection of threats through artificial intelligence can help to quickly and accurately assess the type of threats and choose the right means of protection against them. This, of course, requires the development of a separate intelligent security system using the capabilities of artificial intelligence and the integration of information systems of enterprises and organizations into this system[9].

Result and discussion

Based on the above types of threats and the means of protection against them, the following artificial intelligence model is proposed for early detection of threats.

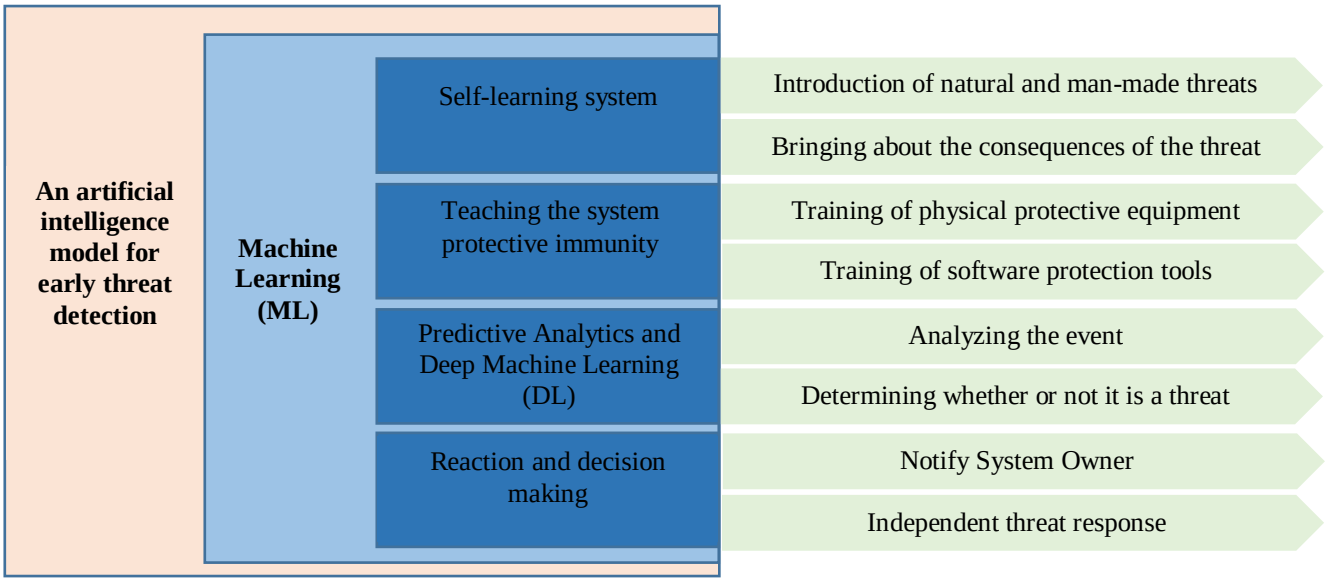

Figure 1. An artificial intelligence model for early threat detection and decision-making against it.

Through the above model, it is possible to develop a smart protection system using artificial intelligence. In the model, it is intended to carry out work in the following sequence.

1. Various natural and artificial threats are implemented by integrating the developed protection system into the test information system. An artificial intelligence neural network recognizes all threats through machine learning (ML). (The longer the testing process lasts, the more threats the system will recognize).

2. While recognizing the threats, it records the consequences that the threat causes. (This may have various effects on the test information system: system shutdown, damage, etc. In such cases, it is recommended to integrate the smart protection system with another test information system).

3. Introduction of physical methods and tools for eliminating threats to the mental protection system. (locks, alarm devices, fire extinguishers, etc.)

4. Introduction of software methods and tools for eliminating threats to the intellectual protection system. (internet screen, anti-viruses, DDOS protection tools etc.)

5. Analysis of processes and events around the information system (based on the collected large data base).

6. Determining whether events and processes are a threat or not (based on a large database collected).

7. Notifying the system owner to take measures when events and processes are assessed as a threat.

8. Application of independent means of protection when there is a high risk of a threat or when serious damage to the information system is detected.

It is recommended to use the following hardware and software tools and programming language in the development of a smart protection system using the capabilities of artificial intelligence for early detection of threats to information systems.

When identifying physical threats:

• thermal thermovisors;
• surveillance cameras;
• motion sensors;
• sound signaling devices;
• humidity sensors;
• air sensors;
• heat sensors;
• electronic locks;
• laser devices;
• ultraviolet lamps;
• trained animals;
• telescope;
• measuring tools.

When identifying artificial threats:

• 1-factor authentication methods (passwords, pin codes, keywords);
• 2-factor authentication tools (uniquely calculated devices);
• 3-factor authentication methods (biometric unique members);
• expert programs;
• antiviruses;
• firewalls (internet screen);
• backup copy programs;
• service programs;
• network analyzers;
• network scanners;
• network devices;
• surveillance cameras;
• radio wave amplifiers, extinguishing means.

Programming languages:

1. Python;
2. C++;
3. Java.

The recommended tools serve to identify threats to enterprise-organizational information systems and apply measures against them. Tools and methods can be enriched based on the characteristics of information systems.

Conclusion

As a result of the research, it was decided that there is currently no perfect intelligent protection system for protecting information systems. Developed systems are becoming unsustainable as a result of increasing types of threats. Until new threats are studied and analyzed by the human factor, and protective measures against them are developed, the consequences of the threat cause considerable damage to the information systems of enterprises and organizations. The proposed intelligent protection system studies threats using the artificial intelligence model presented in the article, regularly forms a large database, and compares new threats with existing threats and offers existing protection tools based on their similar characteristics. Evaluates security tools for new threat tolerance and exposes weaknesses to experts.

If an intelligent protection system is developed using the proposed model, it is possible to destroy information systems, prevent data theft and eliminate unauthorized access.

References

1. D.X.Tojimatov: Kiberxavfsizlik: tahdilar, muammolar, yechimlar, “Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar” Respublika Ilmiy-texnik anjumani TATU Farg‘ona filiali 2022 yil 15-16 aprel.
2. D.X.Tojimatov: Sun’iy intelekt yordamida kiberxavfsizlikni ta’minlashning dolzarbligi. “Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar”Respublika Ilmiy-texnik anjumani TATU Farg‘ona filiali 2022 yil 16-17 aprel.
3. MIRZAYEV J. B., TOJIMATOV D. H. O. G. L. I. KIBERXAVFSIZLIKNI TA’MINLASH, KIBERHUJUMLARNI OLDINI OLISH BO’YICHA DAVLAT SIYOSATI YURITILISHI //ИНТЕРНАУКА Учредители: Общество с ограниченной ответственностью" Интернаука". – С. 36-37.
4. Turdimatov M., Mirzaev J. MATHEMATICAL MODEL FOR DESIGNING A CLOSED VIRTUAL SHELL FOR INFORMATION PROTECTION //Science and Innovation. – 2022. – Т. 1. – №. 6. – С. 430-436.
5. С.В. Горбунов, Е.С. Ермакова: Методические подходы к прогнозированию тенденций угроз природного характера на долгосрочную перспективу, Вестник Воронежского института ГПС МЧС России, №2(19), 2016.
6. Nik Botsrom: Superintelligence Paths, Dangers, Strategies, 2014.
7. С.А.Петренко, Д.Н.Бирюков, А.С.Петронко: Умная кибербезопасность, III International Conference «The 2019 Symposium on Cybersecurity of the Digital Economy — CDE’19»

8. Петренко А. С., Петренко С. А. Технологии больших данных Big Data в области информационной безопасности // Материалы Второй международной научно-технической конференции CDE18. – 2018. – СПб. – С. 248–2
9. Khusanova M. K. NETWORK SECURITY AND MONITORING //Research Focus. – 2022. – Т. 1. – №. 4. – С. 177-183

