END-TO-END ANALYSIS OF BIG DATA IN CYBERSECURITY: DETECTING ANOMALIES AND THREATS IN REAL TIME

Abstract

The spread of the Internet around the world with a huge number of connected devices has created conditions for the use of such a network for various fraudulent purposes, including through unauthorized influence on the computer system by special software (cyber-attacks). This situation has led to the need to take measures aimed at quickly and accurately detecting such attacks and preventing them.

Materials and methods

When writing the article, an integrated approach to the problems of research was implemented using various research methods. Among the general methods used in the research are the method of systematic, quantitative and qualitative analysis, synthesis, as well as the method of formal logical method and theoretical generalization.

Research results

It is proved that special requirements should be imposed on the real-time threat and anomaly detection system, in terms of the need for constant modernization in an ever-changing landscape of cyber threats and anomalies. To solve the problem of building an optimal threat and anomaly detection system, a system model is needed that can optimally take into account a complete list of cases of anomalies and threats, as well as anticipate zero-day attacks.

Conclusion

The study proposes end-to-end data-driven big data analysis based on the deeply deterministic Policy Gradient (DDPG) algorithm. The above algorithm simultaneously studies the Q-function and the policy. It uses data outside politics and the Bellman equation to study the Q-function and uses the Q-function to study politics and is perfectly suitable for use in environments with continuous action spaces (real-time on the Internet).

Keywords
Big data, real-time threat and anomaly detection, neural networks, end-to-end data analysis, data analytics

Introduction

The relevant measures taken in the field of cybersecurity include a whole range of measures. However, the most important of these activities is network security analytics. This is due to the fact that network security analytics is directly aimed at detecting anomalies and threats in the network.

Big data analytics, in turn, is an essential element of any cybersecurity solution. This is due to the need for fast processing of high-speed, large-volume data obtained from various sources to quickly detect threats and anomalies, as well as models of such threats and anomalies.

At the same time, existing research in the field of anomaly detection and threats to network security shows that existing approaches to detecting anomalies in the network are not effective enough, especially in cases involving the detection of anomalies and threats in real time [7, 8]. Despite the fact that over the past few years, it has also been developed and there are a sufficient number of approaches to big data analysis, the use of such approaches in the field of cybersecurity is problematic. Thus, existing approaches do not take into account such important aspects as: zeroday attack detection, real-time threat and anomaly analysis, data exchange between threat detection systems; data processing with limited resources; time series analysis to detect threats and anomalies.

The inefficiency of existing approaches in the field of detecting anomalies and threats to network security is primarily due to the accumulation of huge amounts of data through Internet-connected devices. Based on this, it seems to be an objective need to develop an approach focused on processing big data in real time and detecting threats and anomalies in networks.

Considering the above, in the context of this study, the analysis of modern technologies for processing big data in real time related to the detection of threats and anomalies is of particular relevance.

Materials and methods

When writing the article, an integrated approach to the problems of research was implemented using various research methods. Among the general methods used in the research are the method of systematic, quantitative and qualitative analysis, synthesis, as well as the method of formal logical method and theoretical generalization.

The reliability of the results obtained in the framework of the study is confirmed by a sufficient amount of analyzed material on the studied problem, the use of methods adequate to the tasks set and the use of modern methods of analysis. The validity of scientific conclusions and provisions is confirmed by the results of the conducted research. The conclusions objectively and fully reflect the results obtained.

Thus, within the framework of the conducted research, such relevant topics as neural network learning algorithms were touched upon in order to identify zero-day attacks and unknown types of attacks and threats. The author analyzes the research in this field. From a critical point of view, such studies were evaluated, including the advantages and disadvantages of already developed models and algorithms for endto-end analysis of big data in cybersecurity when detecting threats and anomalies in real time.

Results

The ability to quickly identify threats and anomalies in data is becoming an objective necessity to ensure reliable security and operational integrity. For these purposes, threat and anomaly detection systems are being developed that process data and identify violations or deviations in such data that differ significantly from established standards. To solve the problem of detecting threats and anomalies in real time, the requirements for threat and anomaly detection systems should be increased, since in real time there is an objective need for instant response to threats and anomalies as they arise.

Detection of anomalies and threats in the most general sense involves continuous analysis of data arrays in search of anomalies and threats that do not correspond or deviate from standard patterns [3, 4]. Such deviations from standard patterns may, for example, be associated with unusual spikes in network traffic, which indicate cyber-attacks, threats and anomalies in financial transactions, suggesting cases of fraud, and so on.

From a cybersecurity perspective, real-time threat and anomaly detection is aimed at identifying potential threats and anomalies (including: data leakage, unauthorized access to data, network intrusions or malicious actions) before such anomalies and threats escalate into serious security incidents.

For example, network monitoring helps to detect threats from various network infrastructure elements, for example, substitution or duplication of a MAC address or IP address, virus detection, detection of anomalies in terms of network connection speed.

In modern research, the disadvantages of existing threat and anomaly detection methods are reduced to a high level of false alarms based on unknown behavior of the threat and anomaly detection system [4]. In the specialized literature, threats and anomalies are differentiated by categories (Table 1).

Table 1

Categories and descriptions of anomalies and threats to network security

Categories of anomalies and threats	Description of anomalies and threats
Point - based	The data of a particular type does not conform to the standard of such data in relation to the rest of the data
Contextual	A data instance that is abnormal in a certain context
Common	A set of related data instances that is abnormal with respect to the entire dataset

The categories of anomalies and threats to network security presented in table 1 are standard. In addition to such standard anomalies and threats to network security, there are threats and attacks aimed at cloud servers (Table 2).

Table 2

Categories and characteristics of anomalies and threats to network security aimed at cloud servers

Categories of anomalies and threats	Characteristics of anomalies
Speculative	Atypical execution of hardware performance optimization functions, for example, performed not in the order of hardware prediction and caching
By side channels	Temporary attacks with leakage of the secret key of symmetric key ciphers or the private key of public key ciphers
Software	Buffer overflow (the recorded data exceeds the size of the allocated buffer)

One of the solutions to network security problems to minimize the risks of anomalies and threats to network security aimed at cloud servers in the specialized literature is called high-performance computing [2], as well as controlled neural networks [1, 5, 10]. This is due to the fact that high-performance computing is aimed at monitoring system performance and debugging software, for example, when detecting malware. In turn, trained neural networks can detect malware and intrusions based on embedded learning algorithms, respectively.

The main disadvantage of using supervised deep learning to detect threats and attacks is the specificity of neural network learning models based on learning algorithms based on available attack examples. In this case, zero-day attacks that cannot be embedded in the training dataset for neural networks cannot be tracked by the neural network in a timely manner. High-performance computing also has its drawbacks related to the inability to account for all unknown anomalies and threats affecting system performance.

At the same time, the statistics of cyber-attacks (Table 3) show the need to take drastic measures aimed at timely detection of anomalies and threats in real time.

Table 3

Cyber-attack statistics for 2023 [13, 14, 15]

The name of the indicator	The value of the indicator
Frequency of cyber attacks	Once every 39 seconds
The number of victims of cyber attacks	800,000 people annually
Approximate losses from cyber-attacks for companies in various countries of the world	More than $17,000 every minute
The most common causes of data leakage	Malware infection

As can be seen from the data presented in Table 3, the damage from cyberattacks is enormous. At the same time, the main reason for cyberattacks on big data is malicious software. Such software is designed to take control of the victim's computer infrastructure or disrupt its operation. Posing as harmless files or links, these programs trick users into downloading them – thus giving outsiders access not only to the victim's computer, but also to the entire network within a particular organization.

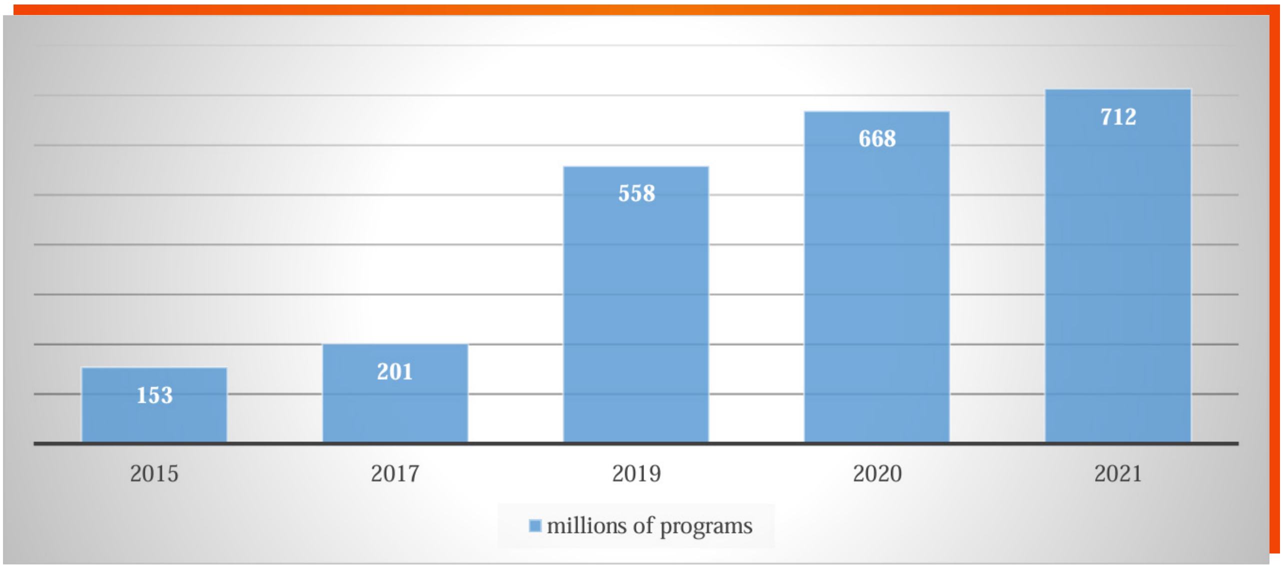

Figure 1 – Cumulative number of malware detections worldwide from 2015 to 2021 [13, 14, 15]

As can be seen from the data presented in Figure 1, as of 2015, the total number of newly detected malware worldwide amounted to 153 million programs, and in 2021 exceeded 700 million. Ransomware has become one of the most widespread and fastest growing threats to individuals and organizations around the 153 201 558 668 712 2015 2017 2019 2020 2021 millions of programsworld. In addition to malware infection, the most popular types of attacks are attacks on the Internet of Things (IoT), denial of service (DDoS), the number of which is growing uncontrollably (Figure 2).

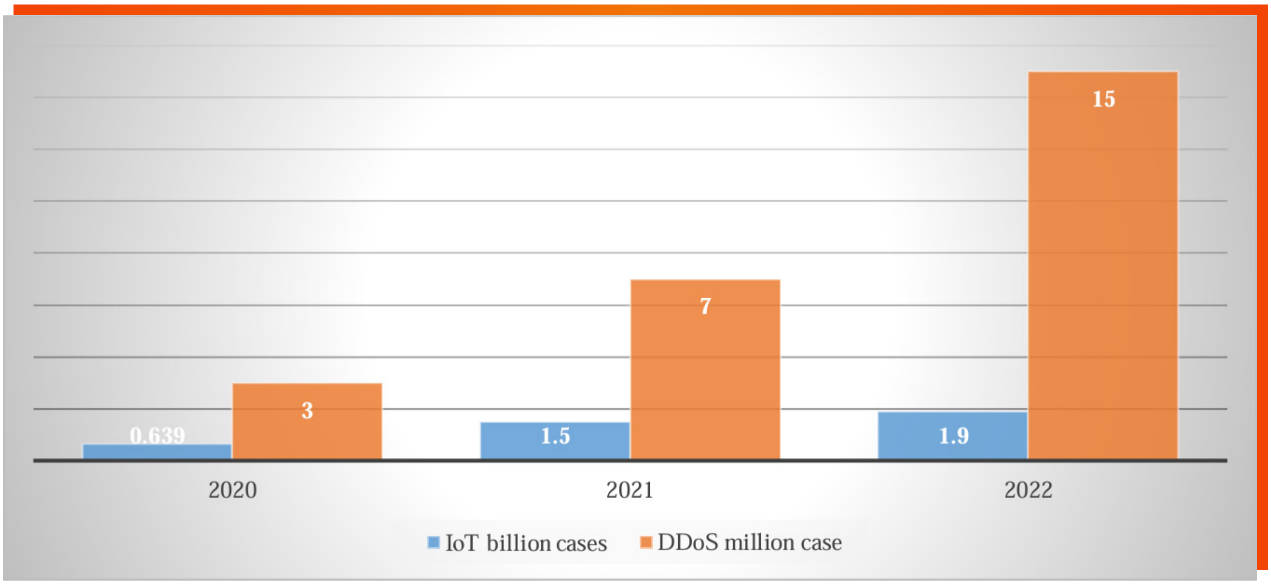

Figure 2 – Cumulative number of IoT hacking and DDoS attacks detected from 2020 to 2022 [13, 14, 15]

According to Statista–a German company specializing in market and consumer data for 2022, attackers committed more than 1.9 billion Internet of Things (IoT) hacks, compared with just 639 million in 2020. At the same time, most IoT network attacks occur through the telnet protocol, an interface that facilitates remote connection to a server or device.

Like many other types of threats and attacks, real-time digital security has shown a significant increase in activity since the start of the COVID-19 pandemic, and the activity of such threats and attacks is only increasing every year.

As can be seen from the data presented in the figure, the number of global DDoS attacks reached 15 million by the beginning of 2023.

Attacks on IoT devices have tripled in the last three years, while according to Statista, 90% of attacks on remote code execution are related to crypto mining, and 1 out of every 36 mobile devices, including phones and tablets, contains a high-risk application.

As the number of real-time cyber threats increases every year, it is only natural that the cybersecurity market is also expanding. In addition, Statista experts expect that by 2028 the total volume of the cybersecurity market will reach a total estimate of 366.1 billion dollars, while in 2023 the global cybersecurity market is estimated at 172.32 billion dollars, showing annual growth (Figure 3).

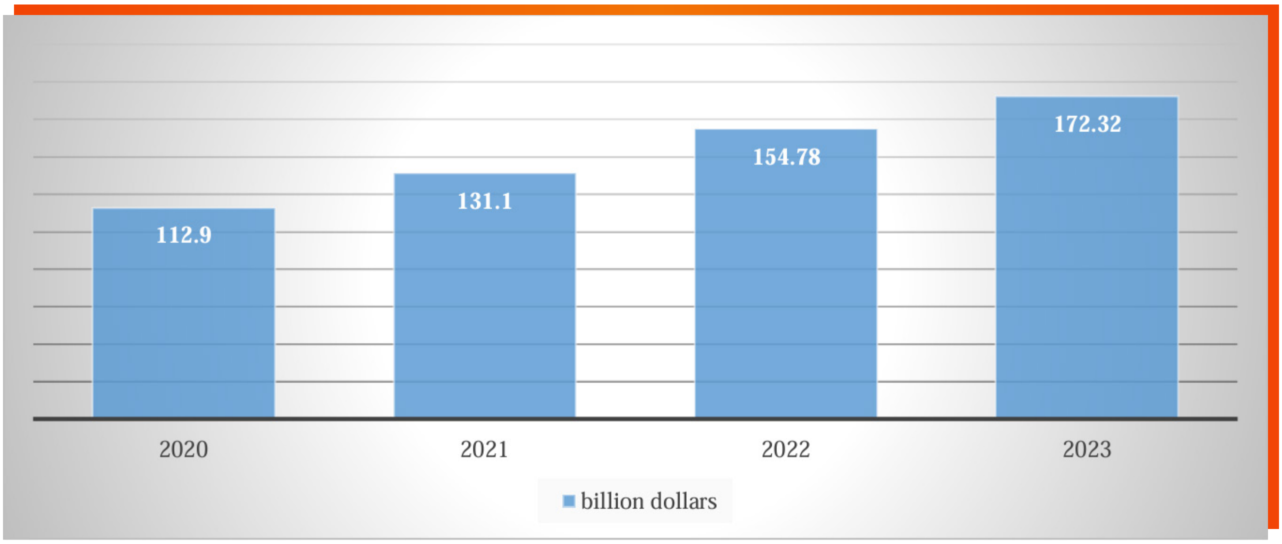

Figure 3 – Growth dynamics of the global cybersecurity market from 2020 to 2022 [13,14,15]

Real-time attacks and threats can lead to various negative consequences, ranging from failures in computer networks, telephone lines or technological systems to power outages, leaks of classified data, and as a result, threats to national security and failures of weapons and military equipment.

In addition, cyber-attacks lead to hidden data or identity theft, such as leaking user credentials, medical records, or financial data. Given the above dynamics, the relevance of end-to-end big data analysis to minimize threats and anomalies in real time is becoming particularly relevant.

Discussions

End-to-end big data analysis (also known as ‹‹end-to-end technology››), in its most general sense, is a concept and methodology that allows data to be processed 112.9 131.1 154.78 172.32 2020 2021 2022 2023 billion dollarsfrom the beginning to the end of its full lifecycle. Unlike traditional approaches where data is processed in different systems with different technologies, end-to-end big data technology combines all stages of data processing into one continuous process [9, 11, 12].

At the same time, if we are talking about data processing within a single continuous process, then when developing an optimal approach, it is necessary to take into account common scenarios for the interaction of various threat and attack situations. As noted earlier, currently the most popular technologies in the field of end-to-end big data analysis for the purpose of detecting threats and anomalies in the network are called high-performance computing, as well as controlled neural networks, which have both advantages and disadvantages, which have already been emphasized in this study.

At the same time, of the above-mentioned technologies in the field of end-toend analysis of big data for the purpose of detecting threats and anomalies in the network in real time, the most interesting are the refinement of technologies related to the use of artificial intelligence and training of neural networks. As you know, the main disadvantage of using supervised deep learning to detect threats and attacks is the inability to account for a separate type of attack - zero-day attacks that cannot be embedded in a training dataset for neural networks cannot be tracked by a neural network in a timely manner, as well as the inability to control unknown anomalies and threats.

Timely detection of zero-day attacks, as well as anticipating unknown anomalies and threats and responding to them in a timely manner are difficult tasks. In solving complex problems, it is necessary to use such neural network learning algorithms that can simultaneously allow real-time learning based on information about past events that are not interconnected with each other.

Standard learning algorithms are not suitable for solving the above-mentioned and complex multi-purpose tasks, since they do not meet the needs of multi-purpose constraints. At the same time, it is known that the solution of complex multi-purpose tasks is possible using the genetic algorithm of non-dominant sorting (NSGA-II), developed back in 2000 by a group of scientists: Kalyanma Deb, Amrit Pratap and Samir Agarwal [6, 8] or the algorithm of deeply deterministic policy gradient (DDPG). If we consider the first algorithm (NSGA-II), then in recent studies in the field of solving complex optimization problems, it has been seriously criticized due to instability and insufficient efficiency in solving complex control problems requiring experience reproduction and asynchronous updating of artificial neural networks [7, 9].

In this regard, the deeply deterministic Policy gradient Algorithm (DDPG) is seen as one of the most promising algorithms for solving complex problems such as zero-day attacks or unpredictable threats and attacks. The algorithm of the deeply deterministic policy gradient (DDPG) simultaneously studies the Q function and politics, using data obtained outside politics and the Bellman equation to study the Q function, while the algorithm uses the Q function itself to study politics, therefore it is perfectly suitable for use in environments with continuous operation spaces (online mode of the Internet).

The Deeply Deterministic Policy Gradient Algorithm (DDPG) is an improved algorithm of the previously known actor-critic algorithm. In the Subject-Critic algorithm, the subject function generates an action based on the current state. The "critic" evaluates the function of the action value based on the output from the "Subject", as well as the current state. TD (temporal-difference) errors received from the critic lead to training in the critic's network, and then the network of "Subjects" is updated based on the policy gradient.

The Deep Deterministic Policy Gradient (DDPG) algorithm combines the advantages of the Subject-Critic and Deep Q-Learning algorithms. The Deep QLearning algorithm is a combination of, in fact, the deepest learning, as well as deep learning and learning with reinforcement learning to achieve an end-to-end algorithm based on the principle of "from perception to action". In other words, the algorithm of the deeply deterministic policy gradient (DDPG) from the concept of Deep Q-Learning. selects the target network and evaluation network for both the "Subject" and the "critic". Moreover, the policy of the deeply deterministic Policy Gradient algorithm (DDPG) is no longer stochastic, but deterministic. This means that the only real action is derived from the network of "Subjects" instead of reporting the probability of various actions. The critical network is updated based on an equation that can be written as follows:

$$L = \frac{1}{I}\Sigma_i^N (Q(s_t, a_t|\theta^Q) - y_i)^2 \qquad (1.1.)$$

In equation (1.1.)

$$y_i = r_i + \gamma^{Q'}\left(s_{t+1}, a_t\middle|\theta^{Q'}\right) \qquad (1.2.)$$

In equation (1.1.), the value of Q estimated by the target network, and I indicates the total number of mini-packets. The network of "Subjects" is updated using a gradient term represented by the following equation:

$$\nabla_{\theta^\mu} J = \frac{1}{I}\Sigma_i^N \nabla_a Q(s, a \mid \theta^Q) \mid_{s=s_i, a=\mu(s_i)} \nabla_{\theta^\mu}\mu(s \mid \theta^\mu) \mid_{s=s_i} \qquad (1.3.)$$

In the presented equation (1.3.) $Q(s, a \mid \theta^Q)$ating from the network is ‹‹criticism››.

It is important to note that the deeply deterministic policy gradient (DDPG) algorithm also solves the problem of continuous operation space (which is particularly relevant in those analysis systems that are associated with real-time work on the Internet) by reproducing experience and asynchronous updates.

Under the above specified conditions, updating the networks of the target ‹‹critic›› and the target ‹‹Subject›› will have the following form:

$$\theta^{Q'} \leftarrow \tau\theta^{Q} + (1-\tau)\theta^{Q'} \qquad \text{(1.4.)}$$

As already noted, the Deeply Deterministic Policy Gradient Algorithm (DDPG) is an algorithm outside politics. In other words, the playback buffer may contain old events, even if they could have been received using an outdated policy. The reason is that the Bellman equation does not care which transition features are used, or how the actions were chosen, or what happens after the transition, because the optimal Q-function must satisfy the Bellman equation for all possible transitions.

Thus, any transitions that have ever been experienced in training a neural network are possible when trying to match the Q-function approximator by minimizing the Bellman mean square error.

Q-learning algorithms for function approximators such as Deep Q-Learning (and all its variants) and the Deeply deterministic Policy gradient algorithm (DDPG) are largely based on minimizing this loss function of the Bellman mean square error. At the same time, with regard to the deeply deterministic policy gradient (DPG) algorithm, there is one main point regarding calculating the maximum over actions in the goal.

Usually calculating the maximum over actions in a target is a problem in continuous action spaces. The Deeply Deterministic Policy Gradient (DDP) algorithm solves this problem by using a policy target network to calculate actions that can be maximized $Q_{\phi_{targ}}$.

The target policy network is determined in the same way as the target Q function: by averaging policy parameters during training:

$$L\,(\phi,\mathcal{D}) = \underset{(s,a,r,s',d)\,\sim\,\mathcal{D}}{E}\left[(Q_\phi(s,a) - (r + \gamma(1-d)Q_{\phi_{targ}}\left(s', \mu_{\theta_{targ}}(s')\right)))^2\right] \qquad \text{(1.5.)}$$

In the presented equation $\mu_{\theta_{targ}}$ – target policy.

The Deeply Deterministic Policy Gradient (DPG) algorithm trains the deterministic policy of a neural network outside politics. Since the policy is deterministic, there is a risk that not all the wide range of actions can be used to find useful training signals. In order to better study politics, various obstacles (noises) are added when using the deeply deterministic Policy Gradient (DPG) algorithm during the training. An example is uncorrelated Gaussian noise of mean zero. To make it easier to obtain better training data, it is allowed to reduce the noise scale during training.

During testing, no noise is added to the actions to see how well the neural network uses what it has learned in the learning process.

Studying politics in a deeply deterministic Policy Gradient (DPG) algorithm is quite simple. If it is necessary to study a deterministic policy, μ_θ(s) gives an action that maximizes $Q_\phi(s,a)$. Since the action space is continuous, it is assumed that the Q-function is differentiable with respect to the action, one can simply perform a gradient ascent (only with respect to policy parameters) to solve the following equation:

$$\max_{\theta} \underset{(s \sim \mathcal{D}}{E}\left[(Q_\phi(s,\mu_\theta(s))\right] \quad (1.6.)$$

The algorithm described above once again proves the fact that multitasking decision-making models with a deeply deterministic policy gradient (DDPG) algorithm are more stable and effective, since this algorithm combines the advantages of the Subject-Critic and Deep Q-Learning algorithms, choosing the best of them, which allows us to draw an unambiguous conclusion about the possibility of adapting the algorithm a deeply deterministic policy gradient (DDPG) for use in models aimed at solving complex multi-purpose tasks, such as end-to-end analysis of big data in real time to detect anomalies and threats in order to ensure cybersecurity.

At the same time, it is quite obvious that the basis of the problem outlined in this study lies in the inability to develop an optimally complete list of cases of anomalies and threats, as well as the anticipation of zero-day attacks. Given the fact that modern capabilities, although they allow the training of neural networks, it is problematic to foresee all possible problems of end-to-end analysis of big data in order to detect anomalies in real time. Based on this, it is necessary to develop a neural network training model that will allow networks to learn in real time, tactically building attack and threat scenarios in real time.

Conclusions

To summarize, it should be noted that the importance of detecting threats and anomalies of network security in real time in an increasingly complex digital landscape cannot be overestimated. At the same time, in this regard, a proactive protection mechanism is important, which will focus on the fastest possible detection of violations in data flows or behavior of the security system, identifying potential threats and anomalies in real time before they develop into serious security violations. Detecting anomalies in real time in connection with the above is a key task. At the same time, special requirements must be placed on the threat and anomaly detection system in real time, in terms of the need for constant modernization in an ever-changing landscape of cyber threats and anomalies.

At the same time, to solve the problem of building an optimal threat and anomaly detection system, it is not enough to simply develop a system model, since it is impossible to develop an optimally complete list of cases of anomalies and threats, as well as to anticipate zero-day attacks.

Given the above, this study proposes end-to-end data-driven big data analysis based on a deeply deterministic policy gradient (DDPG) algorithm. The above algorithm simultaneously studies the Q-function and the policy. It uses data outside politics and the Bellman equation to study the Q-function and uses the Q-function to study politics and is perfectly suitable for use in environments with continuous action spaces (real-time on the Internet).

References

1. Bae C., Yeh W.-C., Shukran M.A. M., chung, Y.Y. and Hsieh T.-J., ‹‹A novel anomaly-network intrusion detection system using ABC algorithms››, International Journal of Innovative Computing, Information and Control, vol. 8, no. 12, pp. 8231-8248, 2012.

2. Bhange A., Syad, A. and Singh S. Thakur, ‹‹DDoS attacks impact on network traffic and its detection approach››, International Journal of Computer Applications, vol. 40, no. 11, pp. 36-40, 2012.

3. Fu X, Lu X, Peltsverger B, Chen S, Qian K, Tao L. A static analysis framework for detecting sql injection vulnerabilities. In: Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International. IEEE: 2007. p. 87-96.

4. Khor K.-C., Ting C.-Y., and Phon-Amnuaisuk S., ‹‹A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection››, Applied Intelligence, vol. 36, no. 2, pp. 320-329, 2012.

5. Liu, G. Yi, Z. and Yang, S. ‹‹A hierarchical intrusion detection model based on the PCA neural networks››, Neurocomputing, vol. 70, no. 7-9, pp. 15611568, 2007.

6. McCulloch U.S., Pitts V. Logical calculus of ideas related to nervous activity // In the collection: ‹‹Automata›› edited by K.E. Shannon and J. McCarthy, pp. 115-133, 1943

7. Nguyen H. V. and Choi Y., ‹‹Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework››, World Academy of Science, Engineering and Technology, International Science Index, vol. 4, no. 3, pp. 247-252, 2010.

8. Pan, Y., Sun, F., Teng, Z. et al. Detecting web attacks with end-to-end deep learning. J Internet Serv Appl 10, 16 (2019).

https://doi.org/10.1186/s13174019-0115-x

9. Patcha A. and Park J.-M., ‹‹An overview of anomaly detection techniques: existing solutions and latest technological trends››, Computer Networks, vol. 51, no. 12, pp. 3448-3470, 2007.

10. Prasenna P., Raghav Ramana A. V. T., Krishna Kumar R., and Devanbu A., ‹‹Network programming and mining classifier for intrusion detection using probability classification››, in Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME '12), pp. 204-209, IEEE, Salem, Tamilnadu, March 2012.

11. Vincent P, Larochelle H, Lajoie I, Bengio Y, Manzagol P-A. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. J Mach Learn Res. 2010; 11(Dec):3371-408.

12. Electronic resource. Access mode:
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930878
(accessed 05.12.2023).

13. Electronic resource. Access mode:
https://explodingtopics.com/blog/cybersecurity-stats (accessed 05.12.2023).

14. Electronic resource. Access mode:
https://www.statista.com/statistics/680953/global-malware-volume/
(accessed 05.12.2023)
15. Electronic resource. Access mode:
https://www.statista.com/topics/8338/malware/#topicOverview
(date of application 05.12.2023).