Алексеенко Ю.В., студент магистратуры
2 курс, факультет «Техника и технологии»
ИСОиП (филиал) ДГТУ
Россия, г. Шахты

Iuliia Alekseenko, graduate student
2 year, Faculty "Engineering and Technology"
Institute of Service and Business (Branch) DSTU
Russia, Shakhty

Авдеева Т.Г., студент магистратуры
2 курс, факультет «Техника и технологии»
ИСОиП (филиал) ДГТУ
Россия, г. Шахты

Tatyana Avdeeva, graduate student
2 year, Faculty "Engineering and Technology"
Institute of Service and Business (Branch) DSTU
Russia, Shakhty

THE APPLICATION OF NEURAL NETWORK FOR CYBERSECURITY

Abstract: Over the past few years, the number of cyber attacks has increased dramatically. Currently, not only government organizations and business companies are attacked by hackers, but many Internet users. Recent studies have shown that machine learning and analytics can predict potential attacks pretty accurate. This article contains the results of the analysis of attacks from 2017 to 2018. The authors also describe several ways of protection by using neural networks and machine learning algorithms as a promising solution to the problem.

Keywords: machine learning, neural networks, cybersecurity, artificial intelligence, cyber attacks.

The relevance of the problem aimed at preventing cyberattacks is determined by modern safety requirements. Firstly, the word “cyberattack”, is considered as the type of attacks. Cyberattack is any type of offensive acts performed by a person or a group of people aimed at breaking computer
systems, information, computer networks, infrastructures, and personal
electronic devices. There are two major types of cyberattacks: attacks where the
primary goal is to disable the target computer or knock it offline, or attacks where
the goal is to get access to the target computer's data and perhaps gain admin
privileges on it [1].

The round diagram below shows the motivation of cyberattacks in 2017-
2018. Cyber Crime has more than 64%. The second place takes Cyber
Espionage (around 22 %) which presents 1/4 of all analyzed attacks. Hacktivism
and Cyber Warfare take the third and fourth places respectively [2].

![Motivations of Attacks](image)

**Figure 1 – Motivations behind attacks**

Last few years there has been a significant increase in the amount of
information getting stolen as the result of successful cyberattacks every day.
Moreover, the total damage from various attacks is 5 billion. These costs are
supposed to be increased greatly over the next 5 years, while the spends on
cyber security measures will be1 trillion dollars in the next four years [3].

Thus, the development of new tools and systems to fight cyberattacks is
an urgent problem for many business companies and organizations to protect
their data and infrastructure. While the set of following steps are usually taken
as security measures: company security policy, special software and its constant updating, cloud services, cyber security specialists, many companies are likely to use such new approaches as data analysis and machine learning to insure a more reliable level of security. The Cyber Research Alliance (CRA) identified the application of Big Data Analytics to cyber security as one of the top six priorities for future cyber security research and development [4].

Systems working on these principles are able to detect two types of warnings: attack recognition and anomaly-based behavior in a system. The first type of systems provides a strong defense against familiar attacks; the other is primary focused on those attacks that are not yet encountered. To work correctly both types of systems collect some data to analyze: time when an attack or attempt of this attack happened, the sequence of events which might have led to this attack, differences in data received from various sources, statistical analysis and etc.

All successfully working security systems can be divided into two major classes: human-based and machine-based ones. Most of “analyses-driven solutions” rely on rules created by an expert and therefore miss any attacks that don’t match these rules. Meanwhile, today’s machine-learning approaches rely on “anomaly detection”, to trigger false positives creating distrust of the system and are to be investigated by humans.

For example, researchers from MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) and the machine-learning startup PatternEx demonstrate an artificial intelligence platform called AI2 that predicts cyber-attacks significantly better than existing systems by continuously incorporating input from human experts. The team showed that AI2 can detect 85 percent of attacks, which is roughly three times better than previous benchmarks, while also reducing the number of false positives by a factor of 5 [5].
The application of neural networks for solving information protection problems is primarily related to the intellectual analysis and prediction of time series (for example, the traffic dynamics of a protected local network), as well as the search for hidden correlations in arrays of primary data.

Also, neural networks can be used for solving encryption tasks, for example, changing an encryption algorithm or encryption key where this change will happen randomly at different time periods.

The real problem of using neural networks for cybersecurity is associated with great computing power needed to train this network. This process is time consuming and requires a big array of training data. Thus, sometimes the solutions based on neural networks are hard to use for a large corporate network if the main purpose is online detection.

To summarize, it can be said that using neural networks for cybersecurity problems is a promising solution, since such networks are more flexible if to compare them with pre-programmed detection algorithms.

References:
1 What is a cyber attack? Recent examples show disturbing trends // CSO. URL: https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html


4 Security Analytics: Using Deep Learning to Detect Cyber Attacks // UNF Digital Commons. URL: https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1783&context=etd