ANTIVIRUS SYSTEM BASED ON ARTIFICIAL INTELLIGENCE CROSS-LEARNING TECHNOLOGY

Aleksandr V. Zhilnikov,
Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia,
og.alexander.saint@gmail.com

Alexander A. Krasilnikov,
Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia, **jvmaster55@gmail.com**

Ildar R. Mardgalimov,
Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia, **SilverCold@gmail.com**

Vladimir A. Osanov,
Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia, **osanov97v@mail.ru**

DOI: 10.36724/2072-8735-2022-16-11-50-56

Manuscript received 24 September 2022;
Accepted 18 October 2022

Keywords: *antivirus systems, information systems security, cybersecurity, computer virus, cyber threat, artificial intelligence, neural networks, machine learning, databases, mathematical methods*

The work is devoted to the priority task in the field of digital transformation, namely, ensuring the protection of information systems and technologies. Artificial intelligence has become one of the key tools in solving this problem. The paper considers an anti-virus system based on artificial intelligence cross-training technology. It presents statistical data confirming the need to implement the technology described in the paper due to a sharp increase in the number of infections of information systems and cyber attacks in recent years. The purpose of this development is to increase the efficiency and reliability of anti-virus systems, providing adaptability to the appearance of new types of cyberthreats. Based on a review of existing analogues for implementing artificial intelligence in cybersecurity, the main drawbacks of using this technology were identified, which were taken into account when developing an antivirus system based on artificial intelligence cross-training technology. The working principle of the proposed solution and the expected benefits from its use are formulated. Two main components of the system – the operation algorithm and the database – are considered in detail. The structural scheme of interaction between the elements in the cross-learning method is presented. The constituent elements of this scheme are described and the purpose of each of them is dissected. The structures of the proposed neural networks are considered. The fundamental logic of the used algorithms and types of mathematical methods is given. All databases necessary to provide the functionality of the described learning algorithm, and their purpose are disassembled. The choice of tools to implement cross-learning technology is justified. In conclusion, a conclusion is made about the possibilities of application of the antivirus system described in the work and about the main difficulties of its implementation.

Information about authors:

Aleksandr V. Zhilnikov, *student, Povolzhskiy State University of Telecommunications and Informatics (PSUTI), department of software engineering, student scientific society PSUTI, Samara, Russia*

Alexander A. Krasilnikov, *student, Povolzhskiy State University of Telecommunications and Informatics (PSUTI), department of software engineering, student scientific society PSUTI, Samara, Russia*

Ildar R. Mardgalimov, *student, Povolzhskiy State University of Telecommunications and Informatics (PSUTI), department of software engineering, student scientific society PSUTI, Samara, Russia*

Vladimir A. Osanov, *senior lecturer, Povolzhskiy State University of Telecommunications and Informatics (PSUTI), department of technical systems management, Samara, Russia*

Для цитирования:
Жильников А.В., Красильников А.А., Мардгалимов И.Р., Осанов В.А. Антивирусная система на основе технологии перекрестного обучения искусственных интеллектов // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №11. С. 50-56.

For citation:
Zhilnikov A.V., Krasilnikov A.A., Mardgalimov I.R., Osanov V.A. (2022). Antivirus system based on artificial intelligence cross-learning technology. *T-Comm*, vol. 16, no.11, pp. 50-56. (*in Russian*)

Introduction

In the last decade, the application of artificial intelligence technologies in Cyber Security (CS) has been the hottest topic in IT, due to the need to increase data privacy. With the development of information technology, cyber threats also evolve, which pose a threat to the storage and protection of users' personal data. This information is confirmed by cybersecurity statistics prepared by various organizations:

1. According to Cisco, Distributed Denial of Service (DDoS) attacks will grow to 15.4 million by 2023, more than double the 7.9 million in 2018 [1].
2. Verizon DBIR's 2020 study found that 45% of hacks were hacked, 17% were malware, and 22% were phishing or social engineering [1].
3. The Kaspersky ICS CERT report states that in the first half of 2021, the proportion of ACS computers on which malicious objects were blocked was 33.8% globally and 39.4% in Russia, an increase of 4.8 subparts over the previous half-year, putting Russia in 5th place among the world regions by this indicator. Much of the growth is due to an increase in the number of attacks using spyware and malicious scripts [2].

All of the above information indicates the relevance of developing new and high-quality systems to repel hacker attacks. Increasing the level of cybersecurity of information systems and computer networks solves one of the main problems of their development, as the factors that slow down this process are eliminated. Consequently, the demand for the development of this direction increases [3].

With the advent of information technology, the topic of information privacy immediately became one of the most important and urgent. It was then that the first methods of protecting information appeared, as well as methods of storing it on various media. Previously, cybersecurity actions were performed manually, but now it is mainly with the help of computers and software. Cybersecurity is based on three processes:

- cyber threat prevention;
- cyber threat detection;
- response.

Today the following types of attacks are widespread: backdoor, DDoS attacks, direct access attacks, eavesdropping, data spoofing, phishing, clickjacking, etc.

Modern operating systems are equipped with various algorithms for checking and scanning for possible cyber threats. The main preventive measure at the moment is the use of firewalls, so-called firewalls, which filter incoming packets. An important security measure is the use of cryptography to protect files, i.e. the authentication procedure for data access. The simplest example of this method is password entry or biometric verification.

Over time, experts came up with a method of implementing a separate program to protect the system and its data – antivirus, which monitors the status and performance of the system, helps detect and eliminate a cyber threat in advance if it is present. Gradually, antiviruses have grown to include more and more features and methods of detecting cyber threats as well as ways to counter them. However, the program is unable to analyze a huge amount of information in a small amount of time, due to the high demand on system resources, which leads to its slowdown.

Analogues

Given the demand for Artificial Intelligence (AI) and Machine Learning (ML), specialists began to actively use these technologies to develop system security techniques. AI, with its enormous computing power, can provide real-time system protection by deeply analyzing the actions of services and processes.

The first classification can look at the characteristics of the data to decide if it is malicious. Some methods involve detecting anomalies in real-time data processing, where traffic information is processed using an algorithm capable of tracking process behavior and classifying it as a cyber threat or safe object. Another method is probabilistic programming. A set of computer languages that can distribute probabilities through analysis. A whole tree of malware can be compiled so that the history of these computer viruses can be tracked.

Neural networks and machine learning algorithms can quickly and efficiently process large amounts of data and recognize its specifics. These functions can then be used to determine if the data is malicious. Using the accumulated database, they can learn and keep errors to a minimum. However, a problem arises, when AI is used in cybersecurity, the speed and scalability of the system increases.

Speaking of the various methods of working with AI, which are currently used in the field of cybersecurity, it is worth separately considering several methods of application of neural networks proposed by experts:

1. Harini M Rajan, Dharani S have proposed a system using neural network techniques, expert systems and intelligent agents. Expert systems basically consist of two parts based on knowledge and inference mechanism. Neural networks identify malicious codes that can cause malware (software) to be installed on a user's system. Intelligent agents use sensors and actuators to prevent DDOS attacks [5].
2. Swapnil Ramesh Kumbar presented a system that uses fuzzy system techniques - pattern recognition, image recognition, processing techniques and data mining. Phishing and fake auctions can be prevented with Data Mining. Pattern matching is used in many systems: fingerprints, facial recognition, voice recognition as protection [6].
3. Mohana, K.V.K. Venugopal, Sathwik H.N. use a chaotic neural network and genetic algorithms to protect the data. Random numbers are generated using a universal algorithm and passed as a parameter used in the processing of the neural network. After the neural network is processed, a key is created which is used for encryption. It is not easy to decrypt the data without the key, which increases security [7].

As can be seen from the above, neural networks are used to analyze and detect malicious elements, as well as to encrypt user data to make it harder for third parties to access. Nowadays, some systems use Generative adversarial network (GAN) algorithm to train AI, when two intelligences with opposite goals are combined into one system. However, this paper will consider a cross-learning method, which is similar to the GAN algorithm, but has specific differences that will be described later. This method has been proposed as a way to improve the efficiency of application of AI in the field of CS [4].

Artificial Intelligence technology automates the process of information security. The use of this branch of the IT sphere helps both to automate the process itself without the participation of CS personnel and to ensure the proper safety of user data. AI has several goals, such as detecting anomalies in system operation, solving classification and prediction tasks. The work is based on algorithms written in various programming languages [8].

However, the system using AI in its work has disadvantages. For example, a large amount of time and data required to train a neural network, the possible presence of errors of the first kind (rejection of a correct hypothesis) and the second kind (acceptance of a false hypothesis), difficult interpretability of the results for a person.

While it is still possible to deal with possible errors and the processing of the results obtained, there are difficulties with the time required and the data required. Training artificial intelligence always takes a large amount of time, as well as testing its effectiveness. For this test requires a specialist who will analyze a large volume of obtained results of actions, during training. That's why the technology of cross-training was proposed, in which a large part of the data is processed by another artificial intelligence, and then it directs the trainee in the right direction. This will reduce the load on the specialist, as well as facilitate the training of the system and the overall effectiveness of the method [9].

System operation principle

The technology itself is a system of two interconnected artificial intelligences that will work with each other. The general algorithm of antivirus operation is shown in Figure 1. Let's examine its two key components using the "FourEyes Smart Antivirus" project as an example:

- work algorithm;
- database (DB).

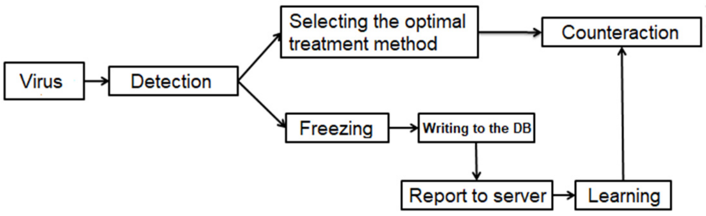

Fig. 1. Algorithm of FourEyes antivirus based on cross-learning technology

The principle of the system of two AIs is considered in the format of an "attack-defense" cycle, in which the "attacking" AI, which generates new modifications of cyber threats, tries to introduce a computer virus into the system, and the "defending" AI picks the best option to counter the attack. The result of the cycle, if any, is recorded and processed by the program, subsequently entering them into the database. After that, the next cycle is started. Through this interaction, the two AIs learn and replenish the databases associated with them. In the program code is prescribed logic of their interaction, in which the results are entered into a database, from which they will be displayed in the console for the developer or analyst to understand.

The resulting algorithms for detecting computer viruses of the second AI are then directly transferred to the device or set of devices, allowing them to work more efficiently and stably. Due to this cyclic interaction, it is possible to achieve effective training of the antivirus system as a whole, as well as reduce the time for self-learning. Moreover, it is possible to predict the emergence of new computer virus archetypes that may appear in the future.

System elements and their purpose

The work of each element is interconnected through a set of databases, which are used in the further process of learning and operation of the antivirus, as shown in Figure 2 [10]. AI in this scheme refers to the algorithms that are directly connected to the neural networks that ensure the operation of the entire network, through the use of mathematical methods. A1 is the algorithm responsible for the work of the attacking AI. It is associated with H1 – a neural network trained to cluster cyberthreats (M1 – clustering method).

That is, N1 divides the input data by certain attributes and enters them into B1, a database containing cyber threats. N2, a neural network trained to modify cyber threats, uses B1 to create new variations of computer viruses using M2, the "gluing" method. N2 then enters the results into B2, a database containing the modified cyberthreats. The resulting computer virus variations then complement the groups of preceding computer viruses, i.e., B1 clusters, using M3, the association method. Unstructured, abnormal or fundamentally new data, in this case, modifications of cyberthreats, are sent to BC – a database containing abnormal situations, from which a report is generated to the server administration (S – server, RD – report to developers), where software staff works with the arising problem.

Then certain data from B1 goes through the NF, an auxiliary filtering neural network, which uses M4, a method of detecting anomalies, and then go to B3 – the database containing the filtered modified cyber-threats and is a temporary. A2 is the algorithm responsible for the operation of the protecting AI. It in turn is linked to N3, a neural network trained to select treatments using M3, which uses the previously mentioned B3. The results are entered into B4, a database containing treatment methods, and abnormal situations similar to modified cyberthreats are sent to BC. B1 and B4 are directly linked to the ES, the expert system that processes the final data and makes the necessary decisions.

The result of ES work in update mode is constantly transmitted to the antivirus, which is a computer application or their complex. For a functional and intuitive interaction with such software the following blocks of the antivirus are supposed to be basic:

- minimalistic interface;
- personal cabinet;
- helpdesk;
- secure cloud storage;
- privacy protection;
- program control;
- vulnerability tracking system;
- cleaning and partial optimization of your computer;
- network monitoring;
- reporting of antivirus work.

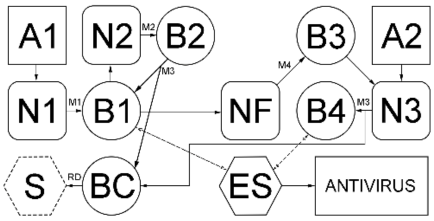

Fig. 2. The structural scheme of interaction of elements in the method of cross-training

Database

To implement such a scheme, it is necessary to think through the logical component of each database, its purpose and structure. Analytical DBMS AWS Redshift, based on PosrtreSQL, will manage the created databases. It is a cloud data storage of large size, with multi-threaded parallel processing of queries [11]. Amazon Redshift DBMS was chosen to work with the database for the following reasons:

- data compression;
- management of accesses, rights and resources;
- maintaining performance at peak loads with segmentation;
- fine-tune the operation of the program;
- the use of datalake technology;
- good optimization when dealing with huge amounts of data, up to several petabytes.

These factors make it relatively easy to work with the data to train the system and reduce the time it takes to process queries in the database. Each database will contain the data required for AI training.

B1 is a document-oriented database in which computer viruses in byte format will act as data. Using logically designed methods, the data from it will flow to N1 for sorting and to N2 for creating new variations of cyberthreats. B2 is essentially similar to B1 in structure, but it will only store various new computer virus modifications based on the cyberthreats from B1. Computer viruses that fit the description of any subtype of existing computer viruses from B1 are sent to it as an addition to the existing data. Computer viruses that do not fit any description are sent to BC. B3 is a temporary database that stores a specific batch of initial and generated cyber viruses to work with them through the N3 neural network.

This DB is used to facilitate the process of collecting the necessary data from B1 and B2. B4 is a document-oriented database in which the data are byte sequences to treat or freeze system-defined cyberthreats. At the end of the cycle, the final data from B1 and B4 goes into the ES database, on the basis of which the main, protective module of the antivirus will operate.

As input data in the scheme of work are the above described databases with the initial set of cyber threats and their treatment. Learning takes place using a system of 3 main and 1 auxiliary neural networks. The basis of the complex is similar to the generative-adversarial model of the two main neural networks N2 and N3, but this scheme mainly differs from GAN [12] in the absence of a separate discriminator that would check the authenticity of the generated computer virus, since the FourEyes system primarily considers the protection against cyber threats and hence it does not care about the computer virus subtype, but only its operability. The absence of a discriminator is primarily due to the fact that each element of the sample, in the form of cyber threats or their elements, must be compared with all the available elements of the database to provide full control modifications and minimize the number of misses. Neural network N2 is a multilayer neural network generator, the layers of which represent independent characteristic features of individual computer viruses.

As inputs come in random variables, one by one, in the form of computer viruses from the database B1, which, passing through the distributing layer, fall into the hidden, where neurons are those or other features of cyberthreat with certain weights. At the output the system receives a combined computer virus, which goes to B2. The N3 neural network has several classification layers to identify the computer virus by the patterns of actions in the system on its side and one layer to select a treatment method based on the association.

Each neuron of the network has its own weight, which is increased if there is a match with a computer virus received as input. Treatment selection is chosen by enumerating the options in descending order of neuron weight of the previous layers. If the "heaviest" by weight method does not fit as a final option, the option lower in the list of weights arrives for checking. N1 is a clustering neural network with layers in the form of certain, initially defined criteria. Its structure is similar to N3, but much simpler in terms of structural grid of neurons, due to the fact that this neural network does not need to select a specific model, but just cluster input data into available groups.

NF is a filtering neural network whose main purpose is to detect anomalies from a number of computer viruses in the form of input data updated base B1. By anomalies we mean certain modifications of computer viruses, clearly different from the previously known ones. After the completion of the N3 neural network cycle, B1 and B4 bases are connected to the ES. The functionality of the anti-virus is just in the ES, which is the core of the anti-virus, and with the help of the knowledge base in the form of the above mentioned B1 and B4, performs activities to protect the system from cyberthreats.

Neural networks

Each neural network is designed to maximize the efficiency of its methods. N1 uses the clustering method, dividing the input data into certain groups according to the specified attributes. The clustering method consists in performing a collection of data about objects and arranging them into a homogeneous group to facilitate further interaction with them. For the correct operation of the described method, the initial input data was reduced to a single template with the necessary characteristics. Different characteristics of the system when affected by a computer virus became the feature space.

These could include, for example, system load, resource coverage, process activity, peak and minimum process load on the system. One of the clustering tasks is the detection of novelty of input data, i.e. the detection of new subtypes of computer viruses that cannot be assigned to any existing cluster. Another task is to recognize the smallest differences between different types of computer viruses (clusters) with similar characteristics, which further increases the probability of effective treatment. On a fundamental level, the method works on the basis of a fuzzy clustering algorithm, more precisely the *c-means* algorithm, that is grouping of elements using fuzzy partitioning. This algorithm uses a fuzzy error criterion, which is based on the formula:

$$E^2(X,U) = \sum_{i=1}^{N}\sum_{k=1}^{K} U_{ik} \,||\, x_i^{(k)} - c_k \,||^2 +, \qquad (1)$$

where *U* is the membership matrix, c_k is the "center of mass" of fuzzy cluster *k:* $c_k = \sum_{i=1}^{N} U_k x_i$.

The M2 gluing method based on generative modeling is currently under development as part of the FourEyes project. The choice came between two specific models – generative and discriminative [13]. It is assumed that the N2 neural network will use this method to go through the database B1, and by combining or modifying independent elements of existing cyberthreats, produce new variants of computer viruses. Consequently, after examining all sides of the two methods, it was decided to use the generative modeling method. The choice was made because of the differences in the performance of the methods. The discriminative model evaluates the probability of correlation of label *x* with a certain dataset *y*, while the generative model does not evaluate certain labels, comparing each generated element with the entire dataset.

The M3 association method used is based on the Hopfield neural network. This network is recurrent, in which signals take values from -1 to 1. Its training is mainly aimed at remembering certain images with the help of weights:

$$X_i = W\,X_i, \qquad (2)$$

where X_i is memorized image, W is the weight of the interaction matrix.

Such training allows you to calculate network parameters with one formula and see the influence of neurons on each other:

$$\omega_{ji} = \frac{1}{N}\sum_{k=1,,m} x_{ik}x_{jk}\,, \qquad (3)$$

where w_{ji} is a certain element of the matrix of weights, *m* is the number of memorized images.

This method will help correctly supplement the database B1 with new modifications of computer viruses obtained using the M2 method, and correctly correlate them with the available groups of cyberthreats. In turn, in the N3 neural network, the M3 method is needed to correctly correlate the treatment methods of the B4 database with the cyberthreat variants.

The H3 neural network requires a certain database with computer viruses and cyberthreats, which will be used in further work, to work effectively and properly. Base B3 is temporary and is created by sampling base B1 passing through the filtering neural network NF, which uses the M4 method, i.e. the anomaly detection method.

This method is necessary to look through the whole data sample and identify certain elements that are clearly out of the average of the whole sample. The method is based on a "sliding windows" algorithm, which divides a series of data into certain windows, which makes it possible to identify the anomaly of the series not only in one particular moment, but also in similar moments and their subspaces. The most generalized description takes the training time series S_i , *p* windows s^k_i are extracted from each , similarly *r* windows t^l_j are extracted from the test time series T_j . The anomaly of the test window t^l_j is estimated based on its similarity to the training windows.

Development tools

The implementation of such a software complex is possible only with the use of properly selected tools. Within the framework of this project its basis is the Python programming language [14] and the library designed for deep machine learning and neural network creation Tensorflow [15]. The use of Python language is due to the large number of libraries and frameworks, as well as strong corporate and public support.

It is very easy to use, which in turn is important for concentrating the attention on the development of algorithms for machine learning, rather than on the technical nuances of the language and complex syntax. Tensorflow library stands out among its counterparts, which are PyTorch, Keras and Scikit-learn, due to the abstractions that allow to focus on the general logic of the application, rather than the small details of implementation, among other advantages are the following:

- a large amount of documentation;
- powerful tools for monitoring the learning process of models and visualization (Tensorboard);
- support from a large community of developers and technical companies;
- ensuring the maintenance of models;
- support for distributed learning.

Conclusion

In conclusion, it is worth noting that new circumvention and hacking techniques are being developed every day to steal user and corporate data. As a result, AI is increasingly being used to automate the detection of system vulnerabilities, hacking software systems, and bypassing anti-virus and firewall protections.

Consequently, it is necessary to improve and automate methods of information protection, which in turn will enable the most efficient development of systems and various networks. Building on the previously described benefits and opportunities for preventing cyber threats that may be developed by attackers in the future, such an improvement could be the introduction of AI cross-learning.

This technology, being both an automated learning system and an anti-virus complex, allows to reduce the time cost of providing the required level of performance and efficiency, greatly reducing the entropy of input data in case of unexpected changes in the system. Most importantly, the proposed system has the ability to predict the emergence of new modifications of existing computer viruses or cardinally new elements of cyber threats, which will provide increased reliability of information storage and full-fledged operation of information systems.

However, this anti-virus system is extremely costly to develop, due to the creation of several complex, relative to the structure, neural networks for the correct operation of algorithms, as well as ensuring the competent work of heavy mathematical methods. Full implementation of such a project will allow to reach a new level of counteraction to information and computer threats.

References

1. Fortinet (2022), “Cybersecurity: Statistics, facts and figures for 2021”, available at: https://www.fortinet.com/en/resources/cyberglossary/cybersecurity-statistics (Accessed 30.03.2022).

2. Kaspersky ICS-CERT (2021), “Threat Landscape for Industrial Automation Systems. First half of 2021”, available at: https://ics-cert.kaspersky.ru/publications/reports/2021/09/09/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2021 (Accessed 30.03.2022).

3. RBC (2022), “The demand for cybersecurity experts in Russia has increased one and a half times. The first half of 2022”, available at: https://rbc-ru.turbopages.org/rbc.ru/s/technology_and_media/26/01/2022/61effbfe9a79479830c8c236 (Accessed 30.03.2022).

4. Zhilnikov A.V., Krasilnikov A.A., Mardgalimov I.R. (2022) “Development of antiviral system "FourEyes" based on artificial intelligence cross-training technology”, *VIII International scientific and practical full-time conference "Problems and prospects of introduction of innovative telecommunications technologies",* Orenburg, 25 March 2022, pp. 271-280.

5. Harini M.R. (2017) “Artificial Intelligence in Cyber Security-An Investigation”, *International Research Journal of Computer Science*, vol. 9, no. 4, pp. 28-30.

6. Kumbar S.R. (2014) "An Overview on Use of Artificial Intelligence Techniques in Effective Security Management", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, pp. 5893-5898.

7. Mohana K., Venugopal V. K. and Sathwik, H.N. (2014) "Data Security using Genetic Algorithm and Artificial Neural Network", *International Journal of Scientific & Engineering Research*, vol. 5, no. 2, pp. 543-548.

8. Arockia Panimalar, S., Giri Pai, U., Khan, S. (2018) “Artificial Intelligence Techniques for Cyber Security”, *International Research Journal of Engineering and Technology*, vol. 5, no. 3, pp. 122-124.

9. Vyugin V.V. (2013) *Mathematical Bases of the Theory of Machine Learning and Forecasting*, Moscow Center for Continuous Mathematical Education, Moscow, Russia.

10. Zhilnikov A.V., Mardgalimov, I.R., Krasilnikov, A.A. (2022) “Application of artificial intelligence cross-training technology in cybersecurity”, *XVI International Industrial Scientific and Technical Conference "Information Society Technologies"*, Moscow, 2-3 February 2022, pp. 110-112.

11. Bauer S. (2013) *Getting Started with Amazon Redshift*, Packt Publishing Ltd, Birmingham, UK.

12. Langr J. and Bok, V. (2019) *GANs in Action*, Manning Publications, New York, USA.

13. Foster D. (2019) *Generative Deep Learning*, O'Reilly Media, Sebastopol, California.

14. Andreas C. Müller (2016) *Introduction to machine learning with python: a guide for data scientists,* O'Reilly Media, Sebastopol, California.

15. Raschka S. (2017) *Python machine learning: machine learning and deep learning with python, scikit-learn, and tensorflow 2,* Packt Publishing Ltd, Birmingham, UK.

АНТИВИРУСНАЯ СИСТЕМА НА ОСНОВЕ ТЕХНОЛОГИИ ПЕРЕКРЕСТНОГО ОБУЧЕНИЯ ИСКУССТВЕННЫХ ИНТЕЛЛЕКТОВ

Жильников Александр Владимирович, *Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), Самара, Россия,* **og.alexander.saint@gmail.com**

Красильников Александр Александрович, *Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), Самара, Россия,* **jvmaster55@gmail.com**

Мардгалимов Ильдар Раильевич, *Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), Самара, Россия,* **SilverCold@gmail.com**

Осанов Владимир Андреевич, *Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), Самара, Россия,* **osanov97v@mail.ru**

Аннотация

Работа посвящена приоритетной задаче в сфере цифровой трансформации, а именно обеспечению защиты информационных систем и технологий. Искусственный интеллект стал одним из ключевых инструментов в решении данной задачи. В статье рассмотрена антивирусная система на основе технологии перекрестного обучения искусственных интеллектов. Представлены статистические данные, подтверждающие потребность в реализации описываемой в работе технологии в связи с резким приростом количества заражений информационных систем и кибератак в последние годы. Целью данной разработки является повышение эффективности и надежности антивирусных систем, обеспечивающих адаптивность к появлению новых видов киберугроз. На основе обзора существующих аналогов реализации искусственного интеллекта в сфере кибербезопасности выявлены основные недостатки использования этой технологии, которые были учтены при разработки антивирусной системы на основе технологии перекрестного обучения искусственных интеллектов. Сформулирован принцип работы предлагаемого решения и предполагаемые преимущества от ее использования. Подробно рассмотрены две основные составляющие системы - алгоритм работы и база данных. Представлена структурная схема взаимодействия элементов в методе перекрестного обучения. Описаны составные элементы данной схемы и разобрано назначение каждого из них. Рассмотрены структуры предлагаемых нейронных сетей. Приведена фундаментальная логика используемых алгоритмов и видов математических методов. Разобраны все базы данных, необходимые для обеспечения функционала описываемого алгоритма обучения, и их назначение. Обоснован выбор инструментария для реализации технологии перекрестного обучения. В заключение сделан вывод о возможностях применения описанной в работе антивирусной системы и о основных трудностях ее реализации.

Ключевые слова: *антивирусные системы, безопасность информационных систем, кибербезопасность, компьютерный вирус, кибеугроза, искусственный интеллект, нейронные сети, машинное обучение, базы данных, математические методы.*

Литература

1. Fortinet. Кибербезопасность: статистика, факты и цифры за 2021 год. 2022. URL: https://www.fortinet.com/ru/resources/cyberglossary/cybersecurity-statistics (дата обращения: 30.03.2022)

2. Kaspersky ICS-CERT. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2021 года. 2021. URL: https://ics-cert.kaspersky.ru/publications/reports/2021/09/09/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2021 (дата обращения: 30.03.2022).

3. РБК Новости. В России в полтора раза вырос спрос на экспертов по кибербезопасности. 2022. URL: https://rbc-ru.turbopages.org/rbc.ru/s/technology_and_media/26/01/2022/61effbfe9a79479830c8c236 (дата обращения: 30.03.2022).

4. *Жильников А.В., Красильников А.А., Мардгалимов И.Р.* Разработка антивирусной системы "FourEyes" на основе технологии перекрестного обучения искусственных интеллектов // VIII Международная научно-практическая очно-заочная конференция "Проблемы и перспективы внедрения инновационных телекоммуникационных технологий": тр. конф. Оренбург, 25.03.2022. С. 271-280.

5. *Harini M.R., Dharani S.* Artificial Intelligence in Cyber Security-An Investigation // International Research Journal of Computer Science, 2017. Vol. 9, no. 4, pp. 28-30.

6. *Kumbar S.R.* An Overview on Use of Artificial Intelligence Techniques in Effective Security Management // International Journal of Innovative Research in Computer and Communication Engineering, 2014. Vol. 2, pp. 5893-5898.

7. *Mohana, K., Venugopal, V.K. and Sathwik, H.N.* Data Security using Genetic Algorithm and Artificial Neural Network // International Journal of Scientific & Engineering Research, 2014. Vol. 5, no. 2, pp. 543-548.

8. *Arockia Panimalar S., Giri Pai U., Khan S.* Artificial Intelligence Techniques for Cyber Security // International Research Journal of Engineering and Technology, 2018. Vol. 5, no. 3, pp. 122-124.

9. *Вьюгин В.В.* Математические основы теории машинного обучения и прогнозирования. М.: МЦНМО, 2013. 304 с.

10. Жильников А.В., Мардгалимов И.Р., Красильников А.А. Применение технологии перекрестного обучения искусственных интеллектов в кибербезопасности // XVI Международная отраслевая научно-техническая конференция "Технологии информационного общества": тр. конф. Москва, 02-03.03.2022. С. 110-112.

11. *Bauer S.* Getting Started with Amazon Redshift. Packt Publishing Ltd, 2013. 137 p.

12. *Langr J., Bok V.* GANs in Action. Manning Publications, 2019. 276 p.

13. *Foster D.* Generative Deep Learning. O'Reilly Media, 2019. 308 p.

14. *Andreas C. Muller.* Introduction to machine learning with python: a guide for data scientists. O'Reilly Media, 2016. 398 p.

15. *Raschka S.* Python machine learning: machine learning and deep learning with python, scikit-learn, and tensorflow 2. Packt Publishing Ltd, 2017. 622 p.

Информация об авторах:

Жильников Александр Владимирович, *студент, Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), кафедра программной инженерии, студенческое научное общество ПГУТИ, Самара, Россия*

Красильников Александр Александрович, *студент, Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), кафедра программной инженерии, студенческое научное общество ПГУТИ, Самара, Россия*

Мардгалимов Ильдар Раильевич, *студент, Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), кафедра программной инженерии, студенческое научное общество ПГУТИ, Самара, Россия*

Осанов Владимир Андреевич, *старший преподаватель, Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), кафедра управления в технических системах, Самара, Россия*