CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2019.7.1.184326
UDC 004.056.53

SERHII TOLIUPA,
VOLODYMYR NAKONECHNYI,
OLEKSANDR USPENSKYI

SIGNATURE AND STATISTICAL ANALYZERS IN THE CYBER ATTACK DETECTION SYSTEM

The globalization of information exchange and the widespread introduction of information technologies in all spheres of society's life created the problem of protecting information processed in information systems from challenges and threats in the cybernetic space. The presence of important information in the functioning of the systems and critical national infrastructures objects enables its usage by the negatively-minded elements and groupings for the implementation of unlawful actions in the cyberspace by violating the integrity, availability, and confidentiality of information, and inflicting damage on information resources and information systems. In this case, the possibility of using information technologies in the cybernetic space in the interests of carrying out military-political and power confrontation, terrorism, and hacking cyber attacks are of particular concern. Today, intrusion detection and attack systems are usually software or hardware-software solutions that automate the process of monitoring events occurring in the information system or network, and independently analyze these events in search of security issues signs. An analysis of modern approaches to the development of such systems shows that it is the signature analysis of network traffic provides effective results in the development of protection modules of cyber systems. In addition, for the reliable protection of information systems, it is not only necessary to develop separate mechanisms of protection, but also to implement a systematic approach that includes a set of interrelated measures. The purpose of the article is to develop a system for recognizing cyber threats based on signature analysis, which would reduce the time of an attack detection of a cyber defense system while the number and complexity of cyber attacks are increasing.

Keywords: cyberspace; cyber attack; signature analyzer; decision-making system; cyber intrusion.

Introduction. One of the main problems, which under the condition of globalization information exchange and wide implementation of information technologies in all spheres of society's life support came up in all states of the world, is the problem of protecting information processed in information systems from challenges and threats in the cybernetic space. Cyberspace possibilities, rapid development and implementation of leading-edge information and telecommunication technologies provide unprecedented opportunities for accumulation of data and its usage. The presence of important information in the systems functioning and objects of critical national infrastructures enable its usage by the negatively-minded elements and groupings for the implementation unlawful actions in the cyberspace by violating the integrity, availability, and confidentiality of information, and inflicting damage on information resources and information systems. In this case, the possibility of using information technologies in the cybernetic space in the interests of carrying out military-political and power confrontation, terrorism and hacking cyber attacks is of particular concern.

Analysis of recent researches and publications. As the world experience has shown, the most effective methodological approach for constructing innovative intellectual cyber attack

monitoring systems is the way to create a hierarchical multilevel structure of cyber attack detection at the beginning of their implementation. Furthermore, a hierarchical approach allows solving difficult problems of the information protection process managing from cyber attacks in the distributed information systems (IS) as a sequence of local tasks, coordinated with each other.

The threats estimation of critically important systems involves two aspects: situational analysis and threats detection [1], [6], [7], [9]. The situational analysis is a detailed analysis of software settings functioning of the IS. While carrying out such an analysis it is necessary to organize similar data and estimate it separately according to each group. There is an example of such analysis, presented in fig. 1.

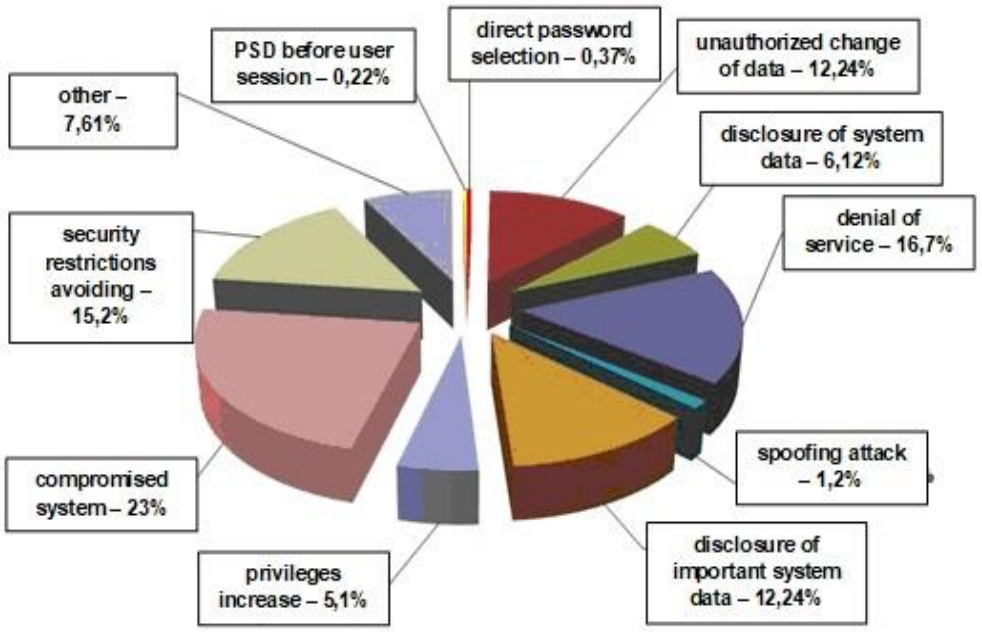

Figure 1 – Threat type diagram [1]

Nowadays, for information systems protection, it is necessary not only to develop private mechanisms protection but also to implement a system approach, which involves a complex of connected actions. Any information safety-related system aims to prevent them from cyber attacks, protect the legal interests of a business entity from information security incidents, prevent from financial looting, dissemination, diseconomy, misrepresentation, and destruction of information.

For today, systems of cyber intrusion and cyber attacks detection usually present program or machine-program solutions, which help automate actions control process taking place in the information system or a network, and also analyze these actions directly to detect some cybersecurity warnings [4],[5]. As the number of different types and ways of organization network hacking has increased for the recent years, cyber attack detection system (CADS) became a necessary component of the security infrastructure of most organizations [2], [3].

In general, modern systems of intrusion and cyber attacks detection are far from ergonomic and effective solutions, according to security. But the improvement of efficiency should be considered not only in the detection sphere of improper activities on the infrastructure of secure information objects but also according to everyday exploitation of these measures and saving of computing power and information resources of a security system owner.

If to talk straight about modules of data-processing, it should be remembered that every cyber attack signature in the system of information processing concerning a cyber attack is a basic element for detecting of most general actions – cyber attack phase detecting (the stage of its implementation). The definition of a signature itself is generalized to a final rule. On the contrary,

each cyber attack is developed for the phase number of its development. The easier cyber attack is, the simpler it can be detected and there are more opportunities to analyze it.

The purpose of the article is to develop a system for recognizing cyber threats based on signature analysis, which would reduce the time of an attack detection of a cyber defense system while the number and complexity of cyber attacks are increasing.

To compass this purpose, the following problems should be solved:

- to create a detection system of the aberrant behavior which is built upon the capability of the cyber attack detecting system to have a knowledge of some characteristics which describe the correct (or permissive) behavior of the object of observation;
- to develop a signature analyzer model which enables a cyber attack or cyber intrusion detection for critically important information structures;
- to develop a statistical analyzer on basis of the average-case analysis model and the root-mean-square deviation of network traffic settings.

The main material research. The cyber attack scenario is a transition diagram which transits to an analogical diagram of the final determined automated device. Cyber attack phases can be described in the following way: ports testing; identification of program and machine tools; banner gathering; exploits usage; disorganization of network functioning with help of attacks for a customer service refusal; managing through backdoors; Trojans set searching; web proxies searching, presence signs removing and so on (in appropriate cases – with different level of detail).

The benefits of such an approach are obvious - in the case, separate processing of various stages of cyber attacks, it is possible to recognize a cyber threat in the process of its preparation and formation, and not at the stage of its implementation, as in the existing systems. At the same time, the elemental basis for recognition can be a signature search, detection of anomalies, the use of expert methods and systems, trust relationships and other information methods to assess what is happening in the information environment. A general approach to analysis allows us to determine distributed (in all senses) cyber threats, both in logical and physical space. The general scheme of event handling also allows searching for distributed cyber attacks by further data aggregating from different sources and constructing metadata about known incidents.

The cyber attack detection systems, like most modern software products, must meet some requirements [10], [11]. These are modern development technologies, orientation on the features of modern information networks and compatibility with other programs. To understand how to use CADS correctly, you need to identify how they work and what their vulnerabilities are. If we do not take into account various non-essential innovations in the field of detection of cyber attacks, then we can safely assert that there are two main technologies of constructing the CADS.

The most widespread cyber threats to information resources can be considered as potentially possible cases of natural, technical or human-induced nature, which may lead to unwanted effects on the information system, as well as on the information stored therein. The emergence of a cyber threat, that is finding the source of actualization of certain events in the threat, is characterized by such an element as vulnerability. By integrating a variety of approaches, as well as suggestions for solving this issue, we believe that the following kinds of cyber threats to information security can be identified: disclosure of information resources; violation of their integrity; failure of the equipment itself.

Traditionally, CADS are classified according to two characteristics: the method of detection and the level of the system on which the protection is carried out. Although these two classification features are most important in the selection of systems for detecting cyber attacks, there are still other characteristics that play an equally important role in the design of the CADS. After all, the safest solution can not be achieved by considering one or two aspects of taxonomy. All developers of attack detection systems and organizations that use CADS should understand and study their classification to choose the best solutions for information security systems. In the study of various aspects of taxonomy and the application of various options, we can achieve a higher level of information systems security.

The systems for detecting abnormal behavior are based on the fact that CADS has some features that characterize the correct or permissible behavior of the object of observation. The block diagram of the cyber security of the information system is presented in fig. 2.

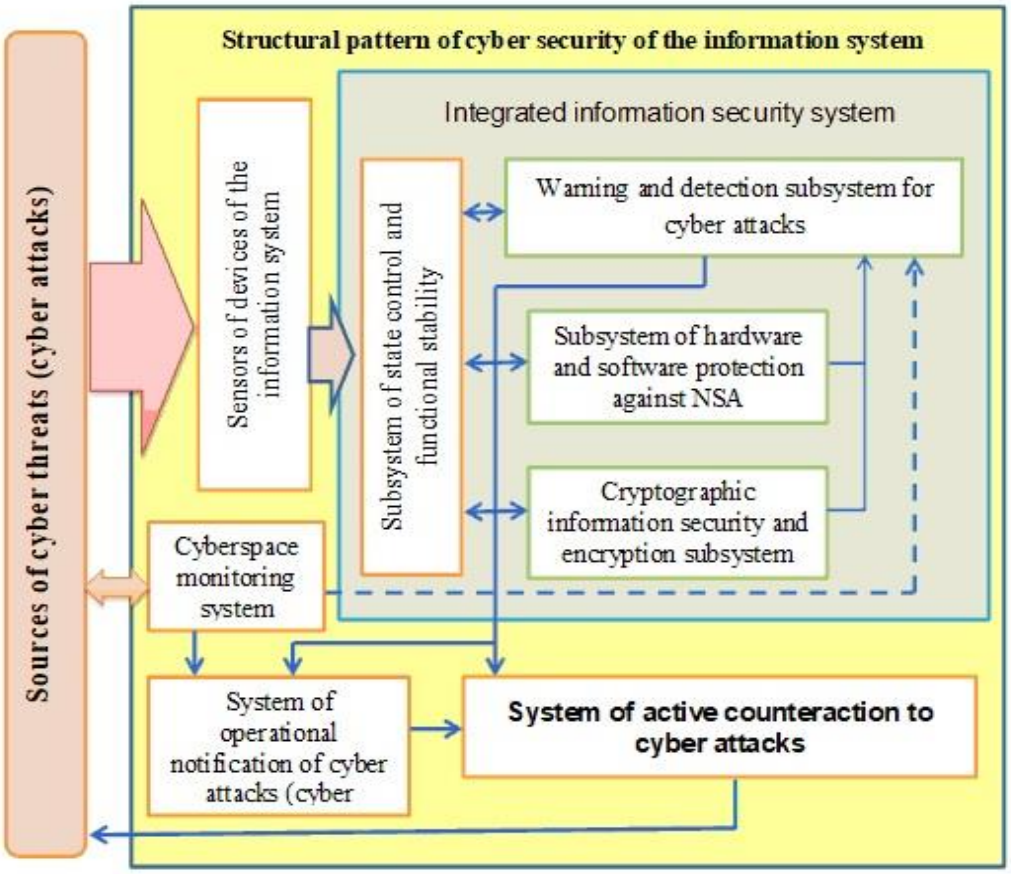

Figure 2 – Structural pattern of the cyber security of the information system

Sensors of cyber intrusion devices identify unusual behavior, anomalies in the operation of a single object. The difficulties of their application in practice are associated with the instability of the objects themselves, which are protected, and with external objects interacting with them. The object of observation can be the network as a whole, a separate computer, network service, user, etc. Sensors operate on the condition that the intruder violates the normal functioning of the information system.

The measures and methods traditionally used to detect abnormalities include the following:

– threshold values: the observation of an object is expressed in the form of numerical intervals; exceeding these intervals is considered to be an abnormal behavior; thresholds can be static and dynamic;

– statistical measures: the decision on the availability of a cyber attack is taken based on a large number of data collected through their statistical pre-processing;

– parametric: for the detection of a cyber attack a special “normal system profile” is constructed based on templates (some policy which this object must usually follow);

– nonparametric: the profile is built on observation of the object during the training period;

– measures based on rules (signatures): they are very similar to nonparametric statistical measures; in the period of training an idea of the normal behavior of the object is being formed, which is written in the form of special “rules”;

– other measures: neural networks, genetic algorithms, which allow classifying some set of known sensor-indicator signs; in modern CADS the first two methods are mainly used.

Usually, abnormal activity detection systems use logging books and current user activity as a data source for analysis. The *advantages* of cyber attack detection systems based on the technology of detecting abnormal behavior can be estimated as follows:

- anomaly detection systems are capable of detecting new types of cyber attacks, the signatures for which have not yet been developed;
- they do not require renewal of signatures and rules of cyber attacks detection;
- detection of anomalies generates information that can be used in criminal detection systems.

The *disadvantages* of systems based on the technology of detecting abnormal behavior are:

- systems require long and qualitative training;
- systems generate many mistakes of the second kind;
- systems are usually too slow at work and require a large number of computing resources.

Let's consider one of the effective methods for detecting intrusions and cyber attacks, which is based on the signature approach. Signatory methods allow you to describe a cyber attack with a set of rules or using a formal model, which can be used as a character string, semantic expression in a special language, etc. The essence of this method is to use a specialized database of cyber attacks templates (signatures) to find actions which fall under the definition of "cyber attack".

The signature method can protect from a viral or hacker cyber attack when its signature is already known (for example, the unchanged fragment of the virus body) and it is included in the database of CADS. If the network is experiencing the first attack from the outside, the first infection is still unknown, and the database simply lacks the signature for its search - the signature method CADS will not be able to signal the danger because it considers the attacking activity to be legitimate.

Most of the existing software products which claim to use the signature method, in fact, realize the most primitive way of signature recognition. In such systems, the signature method is implemented as an algorithm that examines only the dynamics of cyberattack development. And it is based on a state machine to assess the scenario of the developing attack. According to the plan, this approach should allow tracking the dynamics of the development of cyber attacks by the actions of the intruder, while as the module for data collection even the systems for detecting cyber attacks can be used.

Signature analyzer model. Thus, the effectiveness of the signature CADS is determined by three main factors: the efficiency of refinement of the signature base, its completeness from the point of view of the determination of the cyber attack signature, as well as the presence of intelligent algorithms for reducing the attacking party's actions to some basic steps, within which there is a comparison with the signatures.

To implement the chosen method of determination and identification CADS, models of the signature and statistical analyzers of network traffic are offered, and the fuzzy intellectual system is used to determine the sources of cyber-media and the choice of solutions for their elimination. The structure of the universal signature parser flow packets of network traffic is presented in fig. 3.

The mechanism of signature analyzer functioning includes two stages: filtering and collecting fragments of packages, recognition of cyber-criminals by signatures.

The work of the analyzer is described by the following model. Denote the network traffic coming from the packet capture module, as a flow in the form of a set $S = \{s_i\}_1^n$, where n is the total number of packets. The base of signatures can be represented as a set of $B(1)$, which combines signature type clusters $B_j = \{b_{jk}\}_1^K$, $j = \overline{1,m}$:

$$B = B_1 \cup B_2 \cup ... \cup B_m = \cup_{j=1}^m B_j \quad (1)$$

where m – the number of clusters of signatures;

j – cluster, which is a set of identical signatures;

K – total number of signatures in the j-cluster.

The input of the response module receives a signal only if $S \subseteq B$.

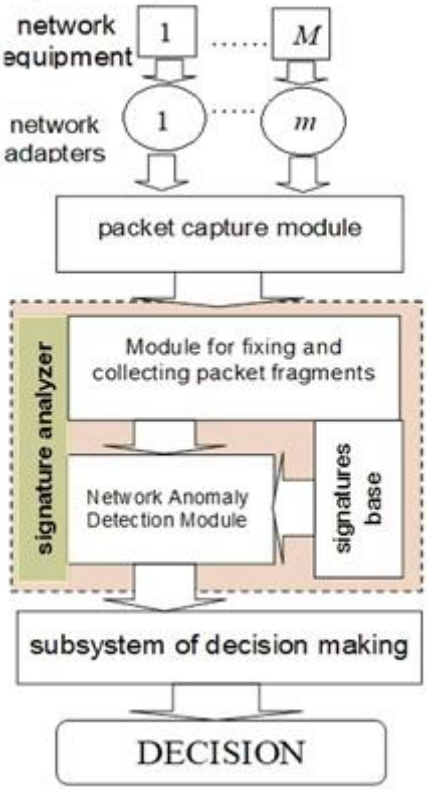

Figure 3 – The structure of the universal signature parser flow packets of network traffic

Statistical analyzer. When developing a statistical analyzer, a model based on the analysis of the mean value and the mean square deviation of the network traffic parameters is proposed. This method is based on comparing the local (current) characteristics Y_b of the flow of packets with averaged over some time (global) characteristics Y_b. As a statistical characteristic of the flow of packets, a sample average ξ, a sample variance d^2 and a consent criterion χ^2 are used. If the local characteristics are significantly different from global ones, then an abnormal behavior of the packet stream and the likely failure of hardware, software or security policy violations are concluded. The structure of a statistical analyzer that implements this method of detecting cyber attacks is shown in fig. 4**.**

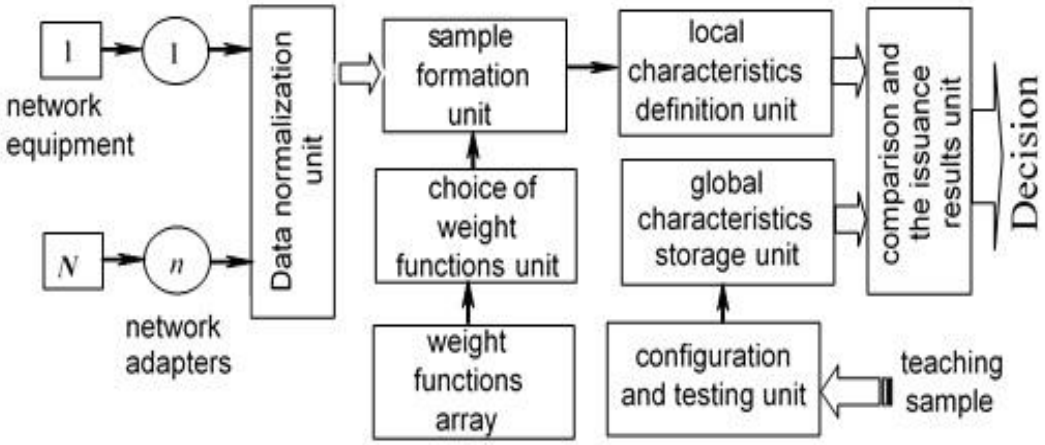

Figure 4 – The statistical analyzer structure

The work of the statistical analyzer is described by the following model. The numeric value $X_i\{x_{\min} \le X_i \le x_{\max}\}$ is a certain event in the flow of network events at a time $t_i, i = \overline{1,n}$. The set of values is characterized by the mean value $\bar{x}$ and variance σ_x of the value X. To determine the local characteristics, the average value $\bar{x}$ is calculated not for the whole stream of N events, but only for the last n events. For this purpose we use the weight function $F(z)$ and the local characteristics can be calculated using the following formula:

$$W(N) = \sum_{i=1}^{N} F(t_N - t_i) f(X_i) \tag{2}$$

As a weight function $F(z)$ the function of the form for finding $W(N)$ was chosen:

$$F_S(z) = \frac{1}{k_S} \sum_{j=1}^{S} \frac{(z/t)^j}{j!} \exp(-z/t) \tag{3}$$

where t – is the time interval on which local characteristics are calculated;

k_S – rationing factor.

To determine the local characteristics, the range of possible values X is divided into B intervals: $[x_{\min}, x_{\max}] \to [x_0, x_1]...[x_{B-1}, x_B]$ and the hit frequencies in the corresponding intervals are calculated not for the whole stream, but for the *n* most recent events. Local characteristics are calculated by (2) and (3).

When designing an intellectual (expert) system, was chosen the fuzzy logic model [8]. This is because a significant amount of information on the causes and source of cyber attacks (CA) can only be obtained expertly or in the form of heuristic descriptions of processes. To determine the sources of CA security system should be represented by the model of the information network on which it is oriented. Such a model divides the process of the information moving between computers across the network environment to several levels. Thus, the primary security problem can be represented by the decomposition of security tasks at individual levels of the network.

Represent a separate level of security in the form of a nonlinear object with a plurality of input variables $\{x_i\}, i = \overline{1,n}$ and one output variable y:

$$y = f_y(x_1, x_2, ..., x_n) \tag{4}$$

As input variables, we will select signs of CA sources. The output variable *y* is a network status indicator.

The model uses the following assumptions and limitations:

- input variables $\{x_i\}$ within one level are independent;
- separate network functions are isolated on each of the network levels.

Integrated Intelligent Decision-making Support System (IIDmSS) for identifying intruders contains a set of functional components which allow you to automate control actions as much as possible when changing the security situation. The structure of the decision-making information system for determining cyber intrusions is presented in fig. 5.

Conclusion. The current state of the systems for detecting cyber attacks on information systems is full of weaknesses and vulnerabilities, which, unfortunately, allow harmful influences to successfully destroy information security systems. This situation is a result of the rapid development of technologies and methods which are used by cybercriminals to achieve their goals. The attacking side will always have an advantage due to the factors of unexpectedness and unpredictability of its actions. Therefore, intrusion detection systems are needed to quickly detect and prevent security breaches (especially caused by previously unknown cyber attacks) which are characterized by unclear criteria.

From this perspective, the following tasks were solved in the work:

- the system for detecting an abnormal behavior that takes into account the multiplicity of monitoring parameters is developed;

– the signature analyzer model for detecting anomalies during the cyber attack is proposed;
– the model of the statistical analyzer, which task is to minimize the probability of making a false decision by the cyber attack detection system is designed.

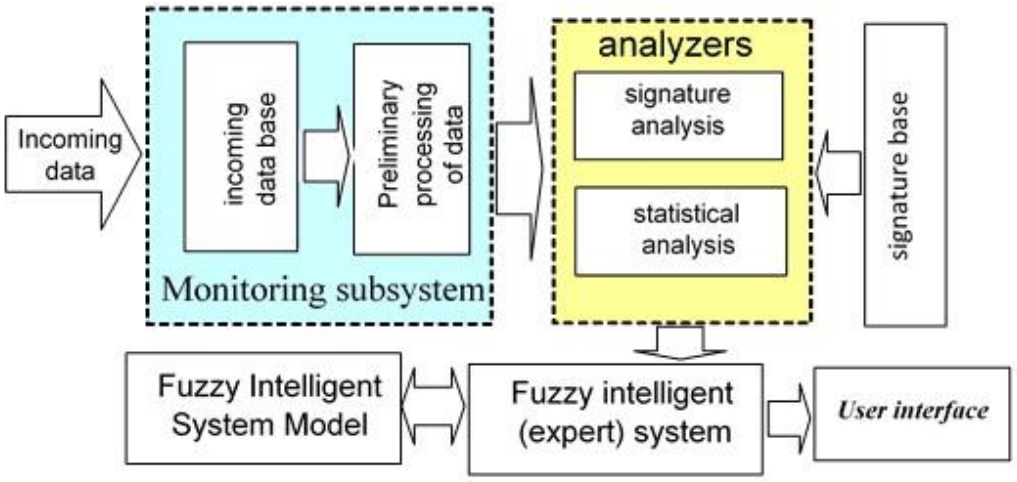

Figure 5 – The structure of the decision-making information system

In general, when new threats and anomalies arise from attacking actions with unidentified or unclearly defined properties, these tools do not always remain effective, they require long time resources for being adapted. That is why intrusion detection systems should be continuously investigated and refined to ensure continuity in their effective functioning. Today, for information protection, not just the development of private security mechanisms is required, but also the implementation of a systematic approach that contains a set of interrelated measures. The main objective of any information security system should be the creation of conditions for the safe operation of the enterprise, cyber threats prevention, protection of enterprise legitimate interests from illegal encroachments, prevention of theft financial means, disclosure, loss, leakage, distortion, and destruction of the official information.

REFERENCE

[1] U. Drejs, M. Movchan, "Analiz neganivnih naslidkiv kiberatak na informacijni resursi objektiv kritichnoji infrastrukturi derjavi", in *Proc. Third International Scientific and Practical Conference Topical issues of cyber security and information security*, Kyiv: European University, 2017, pp. 71-74.
[2] M.I. Masyuk, "NSD: teoriya i praktika", *Spetsialnaya Tehnika*, no. 3, pp. 128-140, 2003.
[3] A. A. Malyuk, S. V. Pazizin, N. S. Pogozhin, *Vvedenie v zaschitu informatsii v avtomatizirovannyih sistemah*. Moscow, Russia: Goryachaya liniya-Telekom, 2001.
[4] L. V. Astahova, V. I. Tcimbol, "Primenenie samoobuchauschejsy sistemy koreljacii sobitiy informacionnoy bezopasnosty na osnove nechotkoy logiki pri avtomatizacii sistem menedjmenta informacionnoy bezopasnosty", *Vestnik JUUrGU, series Computer technologies, management, radio electronics*, vol. 16, no. 1, pp. 165-169, 2015.
[5] "TOP-10 vredonosnih program v Ukraine". [Online]. Available: https://eset.ua/ru/news/view/572/index0/-10-2018. Accessed on: Sept. 10, 2018.
[6] O. U. Cherednichenko, V. V. Fesjoha, U. O. Procjuk, and T. V. Bondarenko, "Analiz isnujuchih pidhodiv protidiji najposhirenishim kibernitichnim vtruchanjam v informatcijno-telekomunikatcijny mereji", *Modern Information Technologies in the Sphere of Security and Defence*, № 2 (32), pp. 13-16, 2018.
[7] P. Kabiri, and A. Ghorbani, "Research on Intrusion Detection and Response: A Survey", *International Journal of Network Security*, vol. 1, no. 2, pp. 84-102, Sept. 2005.

[8] H. Sh. Mondal, T. Hasan, B. Hossain, E. Rahaman, and R. Hasan, "Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic", in *Proc. Third International Conference on Electrical Information and Communication Technology*, New Jersey, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8275211. Accessed on: Dec. 17, 2018.
doi: 10.1109/EICT.2017.8275211.

[9] S. Douzi, I. Benchaji, and B. ElOuahidi, "Hybrid Approach for Intrusion Detection Using Fuzzy Association Rules", in *Proc. Second syber security in networking conference (CSNet)*, Paris, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8602882. Accessed on: Dec. 17, 2018.
doi: 10.1109/CSNET.2018.8602882.

[10] G. Manasi, "Taxonomy of Anomaly Based Intrusion Detection System: A Review", *International Journal of Scientific and Research Publications*, vol. 2, iss. 12, Dec. 2012. [Online]. Available: http://www.ijsrp.org/research-paper-1212.php?rp=P12460. Accessed on: Dec. 17, 2018.

[11] L. K. Babenko, O. B. Makarevich, and O. Yu. Peskova, "Razrabotka kompleksnoy sistemyi obnaruzheniya atak", in *Proc. Fifth International Scientific and Practical Conference Information Security*, Taganrog, 2003, pp. 235-239.

The article was received 10.03.2019.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ю. Дрейс, та М. Мовчан, "Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави", на *3 Міжнародній науково.-практичній конференції Актуальні питання забезпечення кібербезпеки та захисту інформації*, Київ, 2017, с. 71-74.

[2] М. И. Масюк, "НСД: теория и практика", *Специальная Техника*, № 3, с. 128-140, 2003.

[3] А. А. Малюк, С. В. Пазизин, Н. С. Погожин, *Введение в защиту информации в автоматизированных системах*. Москва, Российская Федерация: Горячая линия-Телеком, 2001.

[4] Л. В. Астахова, В. И. Цимбол, "Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности", *Вестник ЮУрГУ, серия Компьютерные технологии, управление, радиоэлектроника*, т. 16, № 1, с. 165-169, 2015.

[5] "ТОП-10 вредоносных программ в Украине". [Электронный ресурс]. Доступно: https://eset.ua/ru/news/view/572/index0/-10-2018. Дата обращения: Сент. 10, 2018.

[6] О.Ю. Чередниченко, В.В. Фесьоха, Ю.О. Процюк, та Т.В. Бондаренко, "Аналіз існуючих підходів протидії найпоширенішим кібернетичним втручанням в інформаційно–телекомунікаційні мережы", *Modern Information Technologies in the Sphere of Security and Defence*, № 2 (32), с. 13-16, 2018.

[7] P. Kabiri, and A. Ghorbani, "Research on Intrusion Detection and Response: A Survey", *International Journal of Network Security*, vol. 1, no. 2, pp. 84-102, Sept. 2005.

[8] H. Sh. Mondal, T. Hasan, B. Hossain, E. Rahaman, and R. Hasan, "Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic", in *Proc. Third International Conference on Electrical Information and Communication Technology*, New Jersey, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8275211. Accessed on: Dec. 17, 2018.
doi: 10.1109/EICT.2017.8275211.

[9] S. Douzi, I. Benchaji, and B. ElOuahidi, "Hybrid Approach for Intrusion Detection Using Fuzzy Association Rules", in *Proc. Second syber security in networking conference (CSNet)*, Paris, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8602882. Accessed on: Dec. 17, 2018.
doi: 10.1109/CSNET.2018.8602882.

[10] G. Manasi, “Taxonomy of Anomaly Based Intrusion Detection System: A Review”, *International Journal of Scientific and Research Publications*, vol. 2, iss. 12, Dec. 2012. [Online]. Available: http://www.ijsrp.org/research-paper-1212.php?rp=P12460. Accessed on: Dec. 17, 2018.

[11] Л. К. Бабенко, О. Б. Макаревич, и О. Ю. Пескова, “Разработка комплексной системы обнаружения атак”, на *V международной научно-практической конференции по Инфлрмационной безопасности*, Таганрог, 2003, с. 235-239.

СЕРГІЙ ТОЛЮПА,
ВОЛОДИМИР НАКОНЕЧНИЙ,
ОЛЕКСАНДР УСПЕНСЬКИЙ

СИГНАТУРНІ ТА СТАТИСТИЧНІ АНАЛІЗАТОРИ В СИСТЕМІ ВИЯВЛЕННЯ КІБЕРАТАК

Глобалізація інформаційного обміну та широке впровадження інформаційних технологій в усі сфери життя суспільства створили проблему захисту інформації, що обробляється в інформаційних системах, від викликів і загроз в кібернетичному просторі. Наявність важливої інформації у функціонуванні систем і об’єктів критичних національних інфраструктур дозволяє використовувати її негативно налаштованими елементами і угрупованнями для здійснення протиправних дій в кіберпросторі шляхом порушення цілісності, доступності та конфіденційності інформації, нанесення шкоди інформаційним ресурсам та інформаційним системам. Можливості кібернетичного простору, лавиноподібний процес розвитку та впровадження новітніх інформаційних і телекомунікаційних технологій забезпечують безпрецедентні умови для накопичення і використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки, екологічного захисту, безпеки стратегічних ресурсів держави. При цьому особливу занепокоєність викликає можливість використання інформаційних технологій в кібернетичному просторі в інтересах здійснення військово-політичного та силового протистояння, тероризму і хакерських кібератак. На сьогоднішній день системами виявлення вторгнень і атак зазвичай є програмно-апаратні рішення, які автоматизують процес моніторингу подій, що відбуваються в інформаційній системі або мережі, і самостійно аналізують ці події в пошуках ознак проблем безпеки. Аналіз сучасних методів та підходів до розробки таких систем показує, що саме сигнатурний аналіз мережевого трафіку забезпечує ефективні результати при розробці модулів захисту киберсистем. Крім того, для надійного захисту інформаційних систем необхідно не тільки розробити окремі механізми захисту, але й реалізувати системний підхід, що включає в себе комплекс взаємопов’язаних заходів. Метою статті є розробка системи розпізнавання кіберзагроз на основі аналізу сигнатур, яка дозволила б скоротити час виявлення атак на системи кібероборони при збільшенні кількості і складності кібератак.

Ключові слова: кіберпростір; кібератака; сигнатурний аналізатор; система прийняття рішення; кібервторгнення.

Toliupa Serhii, doctor of technical sciences, professor, professor at the cybersecurity and information protection academic department, Faculty Information Technologies of the Taras Shevchenko Kyiv National University, Kyiv, Ukraine,
ORCID: 0000-0002-1919-9174,
E-mail: tolupa@i.ua

Nakonechnyi Volodymyr, doctor of technical sciences, senior research fellow, professor at the cybersecurity and information protection academic department, Faculty Information Technologies of the Taras Shevchenko Kyiv National University, Kyiv, Ukraine.
ORCID: 0000-0002-0247-5400.
E-mail: nvc2006@i.ua

Uspenskyi Oleksandr, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
ORCID: 0000-0001-6953-421X.
E-mail: uspensky@ukr.net.

Толюпа Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

Наконечний Володимир Сергійович, доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

Успенський Олександр Анатолійович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

DOI 10.20535/2411-1031.2019.7.1.184327
УДК 004 [056.5 + 85]

АНДРІЙ ШЕВЧЕНКО,
ГЕРМАН ЗАСТЕЛО,
ЄВГЕН ШПАЧИНСЬКИЙ

АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Проаналізовано застосування методів машинного навчання на основі штучних нейронних мереж у прикладних задачах виявлення та класифікації кіберзагроз. Актуальність тематики статі обумовлена значними обсягами впровадження технологій машинного навчання в системі захисту інформації та забезпечення кібербезпеки. Розкривається взаємозалежність між поняттями „штучний інтелект", „машинне навчання" і „глибоке навчання". За результатами аналізу інформаційних джерел, виділено основні методи машинного навчання, які знайшли застосування в галузі кібербезпеки, а саме: мережі Байєса, штучні нейронні мережі, метод опорних векторів, нечітка логіка. Проведено аналіз методів виявлення кіберзагроз, зокрема, статистичні, сигнатурні, евристичні та методи виявлення аномальній. Надано загальну характеристику й виділено переваги та завдання, які вирішують методи машинного навчання для виявлення аномальних подій у сфері кібербезпеки. Розглядаються основні типи штучних нейронних мереж, які застосовуються в задачах виявлення кіберзагроз. Підґрунтям для розгляду загального застосування методів машинного навчання є штучні нейроні мережі на основі багатошарового персептрона зі зворотнім