One of the leading areas of cybersecurity of communication networks is considered – the introduction of preventive mechanisms, among which the most promising are the methods of active security analysis. These methods allow, in addition to timely detection of vulnerabilities of the target system (analyzed system), to confirm the possibility of their implementation, that is, to validate vulnerabilities by simulating the real actions of a potential attacker. The urgent need to validate vulnerabilities out of the many identified is caused by the fact that some of them can only be theoretical, while others are exploited using malicious scripts (exploits). At the same time, the process of validating vulnerabilities is practically not studied. That is why the work carried out an experimental study of the functioning of modern tools for exploiting vulnerabilities. Based on the observations, general quantitative characteristics of the vulnerability validation process were identified. A mathematical model for the analysis of the above characteristics based on Bernstein polynomials has been developed. It is the polynomial representation of the procedure for confirming the possibility of implementing the identified vulnerabilities that makes it possible to describe the dynamics of this process, taking into account the complex and volatile nature of the environment. Analytical dependencies are obtained for the number of cases of successful and negative confirmation of vulnerabilities. In particular, negative validation cases include simply failed attempts to validate vulnerabilities, as well as attempts that resulted in critical errors on the target system during the rational cycle of validating the identified vulnerabilities. The proposed dependencies make it possible to construct the probability distribution laws for the above characteristics of the vulnerability testing process

Keywords: active security analysis, exploitation of vulnerabilities, target system, corporate network security

UDC 004.056
DOI: 10.15587/1729-4061.2022.253530

DEVELOPMENT OF A METHOD FOR CHECKING VULNERABILITIES OF A CORPORATE NETWORK USING BERNSTEIN TRANSFORMATIONS

Roman Kyrychok
PhD
Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Hrinchenko Kyiv University
Bulvarno-Kudriavska str., 18/2, Kyiv, Ukraine, 04053
Oleksandr Laptiev
Corresponding author
Doctor of Technical Sciences, Associate Professor, Senior Researcher
Department of Cyber Security and Information Protection*
E-mail: alaptev64@ukr.net
Rostyslav Lisnevskyi
PhD, Associate Professor
Information Department System and Technologies*
Valerii Kozlovskyi
Doctor of Technical Sciences, Professor, Head of Department**
Vitaliy Klobukov
PhD, Assistant**
*Taras Shevchenko National University of Kyiv
Volodymyrskastr., 60, Kyiv, 01033
**Department of Information Security
National Aviation University
Liubomyra Huzara ave., 1, Kyiv, Ukraine, 03058

Received date 08.12.2021
Accepted date 21.02.2022
Published date 28.02.2022

How to Cite: *Kyrychok, R., Laptiev, O., Lisnevskyi, R., Kozlovskyi, V., Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. Eastern-European Journal of Enterprise Technologies, 1 (9 (115)), 93–101. doi: https://doi.org/10.15587/1729-4061.2022.253530*

1. Introduction

Based on the latest published data regarding the cybersecurity of companies, it is possible to determine how effective measures are taken by companies to protect their corporate networks. A report [1], released in November 2021 by Accenture, states that 55 % of companies (with an annual income of more than 1 billion USD) do not effectively prevent cyber attacks, they are too slow to identify and fix vulnerabilities.

One of the leading directions in ensuring the cybersecurity of communication networks of enterprises and institutions is the introduction of not only mechanisms for detecting cyber attacks, but also the introduction of preventive mechanisms. Among them, the most promising are the methods of active analysis of the security of corporate networks. These methods allow, in addition to the timely detection of vulnerabilities of the target system (the analyzed system), also to check them, that is, to confirm the possibility of implementing specific vulnerabilities by simulating the real actions of a potential attacker. It is the verification of identified vulnerabilities that is a key element of active security analysis, since some vulnerabilities are purely theoretical in nature, while others can be implemented using known exploits. It should be noted that on the Internet there can be both internal threats from inexperienced users, and external ones with the possibility of cyber attacks. Depending on their goals, attackers can implement entire attack strategies that consist of multi-stage attack chains. Therefore, the improvement of

technologies for the timely detection and closing of vulnerabilities in corporate networks that allow minimizing the risk of a cyber attack is an urgent issue [2, 3].

2. Literature review and problem statement

Based on the experience gained, it can be argued that cyberspace, de facto and de jure, has become a new theater of war.

For example, article [4] discusses theories and practices of cybersecurity. The analysis presented in the work showed that in order to disable the critical information infrastructure of the state. An attacker or an opposing party carries out cyber attacks using special samples of malicious software – cyber weapons. Cyber-weapons, such as Stuxnet, Gauss, Duqu, Wiper, Flame, miniFlame, Uroburos (Snake), etc. But there are no clear actions, methods and techniques to counter these threats.

Article [5] shows that attacks are designed exclusively for a specific computer network and are aimed at its most vulnerable components. Typically, such malware samples target a zero-day vulnerability. However, the methodology for checking attacks and real threats to computer networks is not considered and is not given.

Article [6] deals with threats to computer systems and military networks. Examples are given that the implementation of such and other potentially dangerous cyber attacks is unacceptable, since the failure of control processes in such systems will lead to their failure to fulfill their tasks. Thus, the study of world experience has shown that the number of cyber attacks on computer systems and networks of critical infrastructure is constantly increasing. At the same time, their technological complexity increases, which, in turn, makes it impossible or difficult for information security systems to detect such cyber attacks. The information security systems currently used to detect cyber attacks are not fully capable of detecting potentially dangerous cyber attacks, as evidenced by the facts that have taken place in the world.

Article [7] provides a general analysis of cyberattacks. It is shown that, last but not least, the attacks are based mainly on signature-based approaches to the construction of cyber-attack templates, which are characterized by the presence of a «delay effect» in the development of the necessary signature. Therefore, other, alternative approaches are needed, focused on the detection of new, potentially dangerous cyber attacks.

The article [8] justifies and proves that the scientific task of providing the necessary level of protection of computer systems and networks from potentially dangerous cyber attacks requires the development of a new and effective method for constructing their templates. It is shown that the methodology for constructing patterns of potentially dangerous cyberattacks is rather complicated. The need to ensure high reliability of detection entails the need to take into account many informative characteristics or signs of a potentially dangerous cyber attack. Due to the different representation of the formats of characteristics of cyber attacks, which are defined differently by different vendors of information security systems, in practice there is an imbalance in their reduction to one metric system. As a result, it becomes impossible to use the characteristics of potentially dangerous cyberattacks to create their templates.

The article [9] considers the reasons for the violation of information security of computer networks. In particular, such main reasons are cited as: vulnerabilities in operating systems and applications, the presence of vulnerable or easily attacked services and malicious software, etc. It also mentions the danger of incorrect configuration of hardware and software, errors made when setting up access control. Using combinations of existing vulnerabilities and flaws in the network configuration and applied security policy, attackers (both external and internal), depending on their goals, can implement a variety of attack strategies. However, the methodology for checking attacks and real threats to computer networks is not considered and is not given.

The article [10] provides data that any company in its activities uses the wide opportunities that the Internet provides. However, along with the opportunities, the World Wide Web brings many threats to information security. The implementation of these threats can lead to significant material and reputational damage to the business. The types of network attacks and ways of their implementation are considered. However, the methodology for identifying vulnerabilities in software and hardware platforms for automated active analysis of the security of target corporate networks is not given.

At the same time, despite a significant number of publications on addressing various aspects of improving security and methods for identifying vulnerabilities, it becomes clear that the vulnerability analysis process remains ineffective [11–15]. There is no clearly described practical implementation of the rapid detection of vulnerabilities in enterprise computer networks. That is, there is a contradiction between the need for prompt (real-time), high-quality detection and verification of vulnerabilities in enterprise communication networks and the capabilities of existing methods for automating the process of actively analyzing their security.

3. The aim and objectives of research

The aim of this research is to develop an effective method for checking the vulnerabilities of software and hardware platforms for automated active analysis of the security of target corporate networks. This will make it possible to minimize the risks of cyber incidents associated with the presence of vulnerabilities in the target systems of the organization's information infrastructure. In addition, it allows to bypass the lack of highly qualified specialists in conducting an active analysis of the security of corporate networks.

To achieve the aim, the following objectives were set:

– conduct an experimental and practical study of the process of checking the vulnerabilities of information systems using special plug-ins to automate this process in a modern tool for exploiting vulnerabilities;

– develop a mathematical model for analyzing the quantitative characteristics of the vulnerability testing process, taking into account the complex and volatile nature of the environment;

– simulate the analysis of the quantitative characteristics of the vulnerability testing process and obtain analytical dependencies for the number of cases of successful and negative confirmation of vulnerabilities;

– perform a theoretical substantiation of the adequacy of the obtained analytical dependencies.

4. Materials and methods of research

The idea of preventive mechanisms for ensuring the information security of communication networks of enterprises

and institutions is to identify weaknesses before the attack by intruders. At the same time, the protection of weaknesses in this study is understood not as architectural (admitted at the design stage), but primarily as «operational gaps» (vulnerabilities). Such problems often arise during the operation of networks as a result of administrative errors or untimely software updates on individual information systems of such networks. What's more, by putting yourself in the shoes of a potential attacker, it is possible to determine the methods of hacking, the problems that an attacker might encounter, and the specific resources and materials that can be accessed [16–20].

Based on this, let's understand network security as a certain state of the network that makes it possible to resist any cyber attacks or the possible implementation of certain threats to information security. Preserving the confidentiality, integrity and availability of data and network components. Security analysis is the process of checking the network infrastructure for possible vulnerabilities and vulnerabilities in the network perimeter, including errors in configuration, software, and application source code.

To develop a method for checking the vulnerabilities of networks of enterprises and institutions using Bernstein transformations, the necessary experiments were carried out [21–27].

All experiments were performed on a machine running Windows 10 Pro x64 v1803, Intel Core i5-3210M CPU 2.50 GHz and 12 GB RAM using the VMware Workstation 12 Pro v12.5.9 build-7535481 virtualization platform on which a special test bench was deployed. A schematic representation of this stand is shown in Fig. 1.

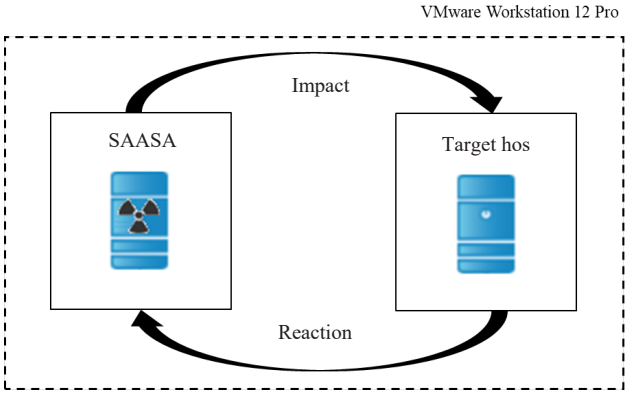

Fig. 1. Diagram of the test stand

As an active system of automatic active security analysis (SAASA), virtual machines running Kali GNU/Linux Rolling 2019.3 are used. Virtual machines with the following Metasploit framework automation tools installed and configured:

– metasploit-autopwn;

– armitage.

The target host is several virtual machines with different platforms installed and the corresponding standard set of software: MS Windows XP SP2 and SP3, MS Windows 7, MS Windows 8.1, MS Windows 10, MS Windows Server 2008 R2; MS Windows Server 2016; Mac OS X 10.13 and 10.14; Metasploitable 2 and Metasploitable 3 (United States). It should be noted that this sample of platforms was formed taking into account statistical data from Netmarketshare and Statcounter on the prevalence of specific operating systems in the world [28, 29]. According to the data presented, about 20 % of respondents in the business environment continue to use outdated versions and even more in government institutions.

All experiments are a series of automatic security analyzes of the same target hosts using the above exploits, and subsequent analysis of the results of their work.

At the same time, to conduct these experiments, a special technique was developed, which provides for the following system of actions:

1. After deploying the test bench and setting up all target hosts, create snapshots (VMware snapshots) of the virtual machine data to preserve its original (initial) state. A virtual machine snapshot is a copy of a virtual machine disk file (VMDK) at a specific point in time that allows to restore the saved state of the virtual machine.

2. Analyze the security of the next host using the Armitage graphical cyber attack management tool using the Hail Mary exploit mode, save the results and restore the VMware image to the original state of the target host under investigation.

3. Analyze the security of the next host using the db_autopwn automation and cyber attack plugin, save the results, and restore the VMware image to the original state of the target host under investigation.

4. In case of a critical error in steps 2 and 3, during the active security analysis, restore the original state of the investigated target host and reanalyze it, excluding from the list of exploits that led to this error.

5. Arrange the results of the experiments in the form of a table.

5. Results of research on the development of an effective method for checking the vulnerabilities of software and hardware platforms of target corporate networks

5. 1. Experimental and practical study of the process of checking the vulnerabilities of information systems using the vulnerability exploitation toolkit

Using the system of actions presented above, a number of observations of the functioning of automated means of exploiting the discovered vulnerabilities were carried out. As a result, it was found that the process of validating the vulnerabilities of hosts of the target corporate network can be represented by a vector (q_s, q_f, q_c) of a three-dimensional vector space. The abscissa q_s determines the number of successfully tested vulnerabilities of the target system, the ordinate q_f determines the number of unsuccessful vulnerability checks. At the same time, the q_c applicate determines the number of vulnerability validation cases that led to a critical error in the target system and subsequent loss of communication.

The obtained statistical data of the results of experimental and practical research are given in Table 1.

In Table 1 £ – the total number of attempts to exploit the identified vulnerabilities of an individual host of the target corporate network; t – the total time for checking the identified vulnerabilities of an individual host of the target corporate network, expressed in seconds.

After analyzing the data in Table 1, it follows that each of the coordinates of the vector (q_s, q_f, q_c) is constantly changing in time, during which an active analysis of the security of the corporate network is being carried out. At the same time, all three coordinates are connected by some functional dependence.

Table 1

Vulnerability check results with armitage and autopwn

Platform (Software)	Armitage					Metasploit-autopwn				
	£	q_s	q_f	q_c	t	£	q_s	q_f	q_c	t
Windows XP SP2	312	3	306	3	345	63	3	58	2	244
Windows XP SP3	98	3	93	2	86	58	3	53	2	286
Windows 7	85	2	80	3	65	63	3	60	2	369
Windows 8.1	83	1	81	1	58	65	0	64	1	281
Windows 10	84	0	83	1	154	1255	0	1255	0	1523
Windows Server 2008 R2	96	2	92	2	82	84	1	82	1	363
Windows Server 2016	39	0	39	0	71	32	0	32	0	43
Mac OS X 10.13	63	1	61	1	115	59	1	58	0	249
Mac OS X 10.14	46	1	45	0	83	41	1	40	0	58
Metasploitable 2	765	3	762	0	293	1445	3	1442	0	1462
Metasploitable 3	780	3	777	0	330	1911	3	1908	0	1933

5. 2. Development of a mathematical model for analyzing the quantitative characteristics of the vulnerability testing process

Unlike deterministic dynamic systems, which can be described by differential equations based on the nature of the system, the task of vulnerability testing is not unique.

Therefore, to build the model, let's use an approach based on the use of a polynomial estimate based on the first Weierstrass theorem, as one of the main approaches to solving problems of nonparametric approximation. It consists in the following: if the function $f(x)$ is continuous on the segment $[a, b]$, then there is a sequence of polynomials $\{P_n(x)\}$ that converges uniformly on the segment $[a, b]$ to $f(x)$. Thus, for any $\varepsilon>0$, there is a polynomial $P_n(x)$ with number n that depends on ε, such that:

$$\left|P_n(x)-f(x)\right|<\varepsilon,$$

for all x on the segment $[a, b]$.

This theorem was proved in 1912 by a famous scientist [2]. The following polynomials $P_n(x)$ were used as approximating polynomials $P_n(x)$:

$$B_n(f;x)=B_n(x)=\sum_{k=0}^{n} f\left(\frac{k}{n}\right)b_{k,n}(x), \quad (1)$$

where

$$b_{k,n}(x)=C_n^k x^k(1-x)^{n-k},\ C_n^k=\frac{n!}{k!(n-k)!}.$$

The function $b_{k,n}(x)$ is called the basic Bernstein polynomial of degree n, the operators $B_n(f; x)$, respectively, are Bernstein polynomials of order n in the function $f(x)$, and the coefficients f(k/n) are called the Bernstein coefficients.

In [2], based on elementary results of probability theory, it is proved that the sequence of polynomials $\{B_n(f;x)\}$ converges $n\to\infty$ to $f(x)$ uniformly on [0, 1], i.e.:

$$\lim_{n\to\infty}\left\|f-B_n(f)\right\|=0.$$

In this case, the following theorem holds.

Theorem 1. For all $n\geq 2$ and $x\in[0, 1]$, the expression:

$$\left|B_n(f;x)-f(x)\right|\leq M\sqrt{\frac{x(1-x)}{n}}, \quad (2)$$

if the function $f(x)$ on the segment [0, 1] satisfies the Lipschitz condition [3] with constant M.

Thus, due to the impossibility of using differential equations, to build a mathematical model for analyzing the quantitative characteristics of the vulnerability testing process, it was decided to use Bernstein polynomials. These polynomials make it possible to successfully approximate analytical dependencies.

5. 3. Analysis of the quantitative characteristics of the process of checking vulnerabilities using the method of mathematical modeling

Based on the results of an experimental study of the operation of modern automated means of exploiting vulnerabilities (Table 1), a mathematical model for analyzing the quantitative characteristics of the process of checking the vulnerabilities of information systems using the regression analysis method was built. To do this, let's first evaluated the statistical relationship between the variables t and q_s, q_f, q_c in the study of the validation mechanism of the Armitage graphical cyber attack management tool using the correlation coefficient R.

According to the table 1, auxiliary values are calculated: sample mean ($\tilde{t}$, $\tilde{q}$), variance (D_t, D_q), and standard deviation (σ_t, σ_q).

The results are shown in Table 2.

From the data in Table 2 it follows that there is a linear relationship between the variables t and q_s, q_f, q_c, since none of the values of R is equal to zero.

It should be noted that the closest linear relationship is observed between the values of t and q_f. Accordingly, it can be argued that with an increase in one value, on average, the other also increases.

In addition, the correspondence of the sample value of the correlation coefficient R to the correlation value (ρ) between the general sets of values of t and q_s, q_f, q_c was checked using

the Student's distribution. The value of t_{calc} is determined according to the following expression:

$$t_{calc} = |R|\sqrt{\frac{n-2}{1-R^2}}. \quad (3)$$

The results of determining the values of t_{calc} are presented in Table 3.

Table 2

Estimated values of the correlation coefficient

Required values	Armitage		
	t, q_s	t, q_f	t, q_c
$\tilde{t}$	152.91	152.91	152.91
$\tilde{q}$	1.73	219.91	1.18
D_t	12716.09	12716.09	12716.09
D_q	1.42	79027.89	1.36
σ_t	112.77	112.77	112.77
σ_q	1.19	281.12	1.17
R	0.6	0.84	–0.07

Table 3

Criterion for the significance of the correlation coefficient

Calculated values	Armitage		
	t, q_s	t, q_f	t, q_c
t_{calc}	2.254	4.693	0.216

Comparison of the obtained values t_{calc} with the theoretical ones with the number of degrees of freedom $f=n-2=9$ and $\alpha=5$ %, there are the following results:

– for t, q_s – $t_{calc}>t_{table}$ let's obtain 2.254>2.096, this indicates a direct relationship between the time of checking the identified vulnerabilities and the number of successfully checked vulnerabilities;

– for for t, q_f – $t_{calc}>t_{table}$ let's obtain 4.693>2.096, this indicates a significant direct relationship between the time of checking the identified vulnerabilities and the number of unverified vulnerabilities;

– for for t, q_c – $t_{calc}>t_{table}$ let's obtain 0.216<2.096, which indicates a very weak relationship between the time of checking the identified vulnerabilities and the number of vulnerability checks that led to critical errors on the target host.

From the data in Table 1 it is possible to show that the time for a rational vulnerability check cycle, in the case of the Armitage tool, is 345 seconds. Therefore, it is possible to first normalize the time interval as follows:

$$t_n = \frac{t_i}{T}, \quad (4)$$

where t_n – normalized time; T – target host vulnerability check time in seconds (rational cycle time); t_i – time during which the corresponding characteristics (q_s, q_f, q_c) took their values within the rational cycle.

The results of normalization of the time interval are presented in Table 4.

Then the values of the variables $q_s(t_n)$, $q_f(t_n)$, $q_c(t_n)$, as a function of the normalized time, are presented in Table 5.

Then, using the data in Table 5 and expressions (1), let's finally obtain the initial analytical dependencies for the number of successfully tested vulnerabilities $q_s=q_s(t_n)$:

$$\begin{aligned} q_s(t_n) &= q_s(0)b_{0.11}(t_n) + q_s(0{,}168)b_{1.11}(t_n) + \\ &+ q_s(0{,}188)b_{2.11}(t_n) + q_s(0{,}206)b_{3.11}(t_n) + \\ &+ q_s(0{,}238)b_{4.11}(t_n) + q_s(0{,}241)b_{5.11}(t_n) + \\ &+ q_s(0{,}249)b_{6.11}(t_n) + q_s(0{,}333)b_{7.11}(t_n) + \\ &+ q_s(0{,}446)b_{8.11}(t_n) + q_s(0{,}849)b_{9.11}(t_n) + \\ &+ q_s(0{,}957)b_{10.11}(t_n) + q_s(1)b_{11.11}(t_n). \end{aligned}$$

After substituting the corresponding values from Table 5, simplifying the expression:

$$\begin{aligned} q_s(t_n) &= b_{1.11}(t_n) + 2b_{2.11}(t_n) + 2b_{4.11}(t_n) + b_{5.11}(t_n) + \\ &+ 3b_{6.11}(t_n) + b_{7.11}(t_n) + 3b_{9.11}(t_n) + 3b_{10.11}(t_n) + 3b_{11.11}(t_n). \end{aligned} \quad (5)$$

From the Table 6 it is shown that the values of $b_{k,11}(t_n)$, for $k=\overline{0...11}$.

Similarly, using (1) and the data in Table 5, let's obtain the initial analytical dependencies for the number of untested vulnerabilities $q_f=q_f(t_n)$, (6) and the number of vulnerability testing cases that led to critical errors $q_c=q_c(t_n)$, (7):

$$\begin{aligned} q_f(t_n) &= 81b_{1.11}(t_n) + 80b_{2.11}(t_n) + 39b_{3.11}(t_n) + 92b_{4.11}(t_n) + \\ &+ 45b_{5.11}(t_n) + 93b_{6.11}(t_n) + 61b_{7.11}(t_n) + 83b_{8.11}(t_n) + \\ &+ 762b_{9.11}(t_n) + 777b_{10.11}(t_n) + 306b_{11.11}(t_n). \end{aligned} \quad (6)$$

$$\begin{aligned} q_c(t_n) &= b_{1.11}(t_n) + 3b_{2.11}(t_n) + 2b_{4.11}(t_n) + \\ &+ 2b_{6.11}(t_n) + b_{7.11}(t_n) + b_{8.11}(t_n) + 3b_{11.11}(t_n). \end{aligned} \quad (7)$$

Table 4

Normalization of the rational cycle time

Real time – t	0	58	65	71	82	83	86	115	154	293	330	345	0
normalized time – t_n	0	0.168	0.188	0.206	0.238	0.241	0.249	0.333	0.446	0.849	0.957	1	0

Table 5

Normalized time function

t_n	0	0.168	0.188	0.206	0.238	0.241	0.249	0.333	0.446	0.849	0.957	1
$q_s(t_n)$	0	1	2	0	2	1	3	1	0	3	3	3
$q_f(t_n)$	0	81	80	39	92	45	93	61	83	762	777	306
$q_c(t_n)$	0	1	3	0	2	0	2	1	1	0	0	3

Table 6

Polynomial values $b_{k,11}(t_n)$

k	$b_{k,11}(t_n)$
0	$(1-t)^{11}$
1	$11t(1-t)^{10}$
2	$55t^2(1-t)^9$
3	$165t^3(1-t)^8$
4	$330t^4(1-t)^7$
5	$462t^5(1-t)^6$
6	$462t^6(1-t)^5$
7	$330t^7(1-t)^4$
8	$165t^8(1-t)^3$
9	$55t^9(1-t)^2$
10	$11t^{10}(1-t)$
11	t^{11}

Thus, as a result, the following analytical dependencies were obtained:

$$q_s(t_n)=\sum_{i=0}^{n} q_s\left(t_n^{(i)}\right)b_{k,n}(t_n),$$

$$q_f(t_n)=\sum_{i=0}^{n} q_f\left(t_n^{(i)}\right)b_{k,n}(t_n),$$

$$q_c(t_n)=\sum_{i=0}^{n} q_c\left(t_n^{(i)}\right)b_{k,n}(t_n), \quad (8)$$

these are the final expressions for the studied characteristics of the information systems vulnerability validation process. It is the polynomial representation of the procedure for confirming the possibility of implementing the identified vulnerabilities that makes it possible to describe the dynamics of the vulnerability validation process, taking into account the complex and volatile nature of the environment.

5. 4. Justification of the adequacy of the obtained analytical dependences

Table 7 presents the comparative values of the results of the calculation and the data of the Table 5.

Table 7

Comparative values for $q_s(t_n)$

t_n – normalized time	Empirical values $q_s^e(t_n)$	Calculated values $q_s^p(t_n)$	Deviation $\Theta=\left\|q_s^e(t_n)-q_s^p(t_n)\right\|$
0	0	0	0
0.168	1	1.065446	0.065446
0.188	2	1.100162	0.899838
0.206	0	1.126111	1.126111
0.238	2	1.167208	0.832792
0.241	1	1.171013	0.171013
0.249	3	1.181262	1.818738
0.333	1	1.309026	0.309026
0.446	0	1.494756	1.494756
0.849	3	2.425641	0.574359
0.957	3	2.970647	0.029353
1	3	3	0

From the data given in Table 7, it can be seen that the function $q_s=q_s(t_n)$ of a successful vulnerability check satisfies the Lipschitz condition [3], i.e. $t_n^{(1)}, t_n^{(2)} \in [0; 1]$ for $K>0$ let's obtain the inequality:

$$\left|q_s\left(t_n^{(1)}\right)-q_s\left(t_n^{(2)}\right)\right| \le K\left|t_n^{(1)}-t_n^{(2)}\right|. \quad (9)$$

It follows from condition (9) that there is a rectangular area outside of which the graph of the function $q_s=q_s(t_n)$ is not defined. This makes it possible in the future to build probability distribution laws for the number of successfully tested vulnerabilities. In addition, when condition (9) is satisfied, estimate (2) is valid, i.e.,

$$\left|B_n(q_s,t_n)-q_s(t_n)\right| \le K\sqrt{\frac{t_n(1-t_n)}{n}}. \quad (10)$$

It follows from inequality (2) that there exists a positive number K for which:

$$\theta=\left|q_s^e(t_n)-q_s^p(t_n)\right|=K\sqrt{\frac{t_n(1-t_n)}{n}}. \quad (11)$$

Dependence (11) allows to set the appropriate accuracy of determining the degree of the Bernstein polynomial.

Thus, using the data in Table 7 and dependence (11), the maximum value for $q_s=q_s(t_n)$ is defined as:

$$\max(K_i)=13.949121,$$

where $i \in [1; 11]$.

Also, generalized data were obtained by similarly modeling the analysis of other quantitative characteristics of the vulnerability testing process. In particular, data were obtained on the number of failed vulnerability checks and the number of vulnerability checks that led to critical errors during the rational cycle of checking for identified vulnerabilities. The results of the corresponding comparisons are presented in Table 8, 9.

Table 8

Comparative values for $q_f(t_n)$

t_n – normalized time	Empirical values $q_f^e(t_n)$	Calculated values $q_f^p(t_n)$	Deviation $\Theta=\left\|q_f^e(t_n)-q_f^p(t_n)\right\|$
0	0	0	0
0.168	81	62.547827	18.45217
0.188	80	63.809242	16.19076
0.206	39	64.596778	25.596778
0.238	92	65.508850	26.49115
0.241	45	65.575300	20.5753
0.249	93	65.743882	27.256118
0.333	61	67.844585	6.844585
0.446	83	78.745219	4.254781
0.849	762	538.115125	223.884875
0.957	777	478.499059	298.500941
1	306	306	0

Table 9

Comparative values for $q_c(t_n)$

t_n – normalized time	Empirical values $q_c^e(t_n)$	Calculated values $q_c^p(t_n)$	Deviation $\Theta=\left\|q_c^e(t_n)-q_c^p(t_n)\right\|$
0	0	0	0
0.168	1	1.337389	0.337389
0.188	3	1.360285	1.639715
0.206	0	1.364959	1.364959
0.238	2	1.346917	0.653083
0.241	0	1.343984	1.343984
0.249	2	1.335418	0.664582
0.333	1	1.221982	0.221982
0.446	1	1.125939	0.125939
0.849	0	0.731249	0.731249
0.957	0	1.860081	1.860081
1	3	3	0

In addition, using the data in Table 8, 9 and dependence (11), let's obtain the maximum values of K for $q_f=q_f(t_n)$:

$$\max(K_i)=4880.359905,$$

where $i\in[1;11)$ and $q_c=q_c(t_n)$;

$$\max(K_i)=30.411511,$$

where $i\in[1;11)$.

Analysis of data in the Table 7–9 shows that there is a certain deviation due to the fact that a small number of terms were taken during the study, but such a deviation is acceptable.

6. Discussion of the results on the development of an effective method for checking the vulnerabilities of software and hardware platforms of target corporate networks

In the course of an experimental study of the functioning of modern means of exploiting vulnerabilities, generalized characteristics of the vulnerability verification process were identified. In particular, this is the number of successfully tested vulnerabilities of the target system – q_s, as well as the number of negative confirmations of vulnerabilities. The latter include the number of failed vulnerability checks – q_f and the number of cases of vulnerability validation that led to a critical error in the target system and subsequent loss of communication – q_c.

In the course of modeling the analysis of the above quantitative characteristics of the vulnerability testing process, analytical dependencies (8) were derived, which fully reflect the dynamics of this process.

Comparison of empirical data obtained during the study of the process of checking the vulnerabilities of information systems using vulnerability exploitation tools with the calculated values shows an acceptable deviation (Tables 7–9). It should be noted that as the number of values increases, these deviations become smaller and smaller. At the same time, for further research related to erroneous attempts to validate vulnerabilities and cases of validation that led to critical errors, this difference is not significant.

Thus, the proposed analytical dependencies make it possible to construct the laws of probability distribution of the above characteristics of the vulnerability validation process. This is a distinctive feature of the developed method.

However, it should be noted that the vulnerability validation process involves checking vulnerabilities using only known exploits. This approach is somewhat limited due to the fact that checks for the possibility of implementing previously unknown vulnerabilities, for example, zero-day vulnerabilities, remain unaccounted for, and requires further development.

The disadvantage of the developed method is an increase in the time for calculating vulnerabilities, but this disadvantage is not critical with the modern rapid development of computer technology. The direction of further research can be considered the improvement of the method by taking into account additional factors for the analysis of vulnerabilities that fell outside the scope of consideration during the development of this method.

7. Conclusions

1. In the course of an experimental study of the functioning of modern means of exploiting vulnerabilities, generalized characteristics of the vulnerability verification process have been identified. In particular, this is the number of successfully tested vulnerabilities of the target system, the number of unsuccessful checks, as well as the number of cases of vulnerability validation that led to a critical error in the target system and subsequent loss of communication. These characteristics take into account the complex and changing nature of the environment, as well as the risk of a critical error in the functioning of the target system when exploiting vulnerabilities.

2. A mathematical model has been developed to analyze the quantitative characteristics of the vulnerability testing process, taking into account the complex and volatile nature of the environment. A feature of the developed model is the use of Bernstein polynomial transformations.

3. In the course of modeling the analysis of the generalized quantitative characteristics of the vulnerability testing process, their analytical dependencies have been derived, which fully reflect the dynamics of this process.

4. In the course of comparing the empirical data obtained during the study of the process of checking the vulnerabilities of information systems, carried out by full-scale modeling, with the calculated values, it has been found that the deviation cannot exceed 20 %. The error of the results obtained in identifying critical vulnerabilities was no more than 17 %, which confirms the adequacy of the developed model.

References

1. State of Cybersecurity Resilience 2021: How aligning security and the business creates cyber resilience. Accenture. Available at: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
2. Bernshteyn, S. (1952). Dokazatel'stvo teoremy Veyershtrassa, osnovannoe na teorii veroyatnostey. Sobranie sochineniy. Vol. 1. Moscow: AN SSSR.

3. Malozemov, V. (2019). O mnogochlenakh Bernshteyna. Seminar «CNSA & NDO». Available at: http://apmath.spbu.ru/cnsa/pdf/2019/Malozemov_BernsteinPolynom_17sep2019.pdf
4. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O.et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: https://doi.org/10.15587/1729-4061.2019.175978
5. Barabash, O. (2020). The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research, 8 (8), 4133–4139. doi: https://doi.org/10.30534/ijeter/2020/17882020
6. Laptiev, O., Vitalii, S., Yevseiev, S., Haidur, H., Gakhov, S., Hohoniants, S. (2020). The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit50783.2020.9349322
7. Savchenko, V., Laptiev, O., Kolos, O., Lisnevskyi, R., Ivannikova, V., Ablazov, I. (2020). Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit50783.2020.9349304
8. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S. et.al. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies, 1 (2 (109)), 14–23. doi: https://doi.org/10.15587/1729-4061.2021.225346
9. Laptiev, O., Savchenko, V., Pravdyvyi, A., Ablazov, I., Lisnevskyi, R., Kolos, O., Hudyma, V. (2021). Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), 13 (1), 48–54. Available at: https://www.ijcnis.org/index.php/ijcnis/article/view/4902
10. Hryshchuk, R., Korobiichuk, I., Ivanchenk, S., Roma, O., Golishevsky, A. (2019). The Throughput of Technical Channels as an Indicator of Protection Discrete Sources from Information Leakage. Computer Modeling and Intelligent Systems, 2353, 523–532.
11. Mashkov, O. A., Sobchuk, V. V., Barabash, O. V., Dakhno, N. B. et. al. (2019). Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. Mathematical Modeling and Computing, 6 (2), 344–357. doi: https://doi.org/10.23939/mmc2019.02.344
12. Barabash, O., Dakhno, N., Shevchenko, H., Sobchuk, V. (2018). Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method. 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC). doi: https://doi.org/10.1109/msnmc.2018.8576310
13. Korotin, S., Kravchenko, Y., Starkova, O., Herasymenko, K., Mykolaichuk, R. (2019). Analytical Determination of the Parameters of the Self-Tuning Circuit of the Traffic Control System on the Limit of Vibrational Stability. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). doi: https://doi.org/10.1109/picst47496.2019.9061256
14. Rakushev, M., Permiakov, O., Lavrinchuk, O., Tarasenko, S., Kovbasiuk, S., Kravchenko, Y. (2019). Numerical Method of Integration on the Basis of Multidimensional Differential-Taylor Transformations. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). doi: https://doi.org/10.1109/picst47496.2019.9061339
15. Barabash, O., Lukova-Chuiko, N., Sobchuk, V., Musienko, A. (2018). Application of Petri Networks for Support of Functional Stability of Information Systems. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). doi: https://doi.org/10.1109/saic.2018.8516747
16. Kravchenko, Y., Leshchenko, O., Dakhno, N., Trush, O., Makhovych, O. (2019). Evaluating the Effectiveness of Cloud Services. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit49449.2019.9030430
17. Musienko, A. P., Serdyuk, A. S. (2013). Lebesgue-type inequalities for the de la Vallée-poussin sums on sets of entire functions. Ukrainian Mathematical Journal, 65(5), 709–722. doi: https://doi.org/10.1007/s11253-013-0808-4
18. Saiko, V., Nakonechnyi, V., Narytnyk, T., Brailovskyi, M., Lukova-Chuiko, N. (2020). Terahertz Range Interconnecting Line For LEO-System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). doi: https://doi.org/10.1109/tcset49122.2020.235468
19. Ruban, I., Martovytskyi, V., Lukova-Chuiko, N. (2018). Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System. Cybernetics and Systems Analysis, 54 (2), 302–309. doi: https://doi.org/10.1007/s10559-018-0032-1
20. Lakhno, V., Kozlovskii, V., Boiko, Y., Mishchenko, A., Opirskyy, I. (2017). Management of information protection based on the integrated implementation of decision support systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 36–42. doi: https://doi.org/10.15587/1729-4061.2017.111081
21. Kozlovskyi, V., Lakhno, V., Kasatkin, D., Boiko, Y., Kravchuk, P., Lishchynovska, N. (2019). A model and algorithm for detecting spyware in medical information systems. International Journal of Mechanical Engineering and Technology, 10 (1), 287–295. Available at: https://iaeme.com/MasterAdmin/Journal_uploads/IJMET/VOLUME_10_ISSUE_1/IJMET_10_01_029.pdf

22. Lakhno, V. A., Kasatkin, D. Y., Blozva, A. I., Kozlovskyi, V., Balanyuk, Y., Boiko, Y. (2020). The Development of a Model of the Formation of Cybersecurity Outlines Based on Multi Criteria Optimization and Game Theory. Advances in Intelligent Systems and Computing, 10–22. doi: https://doi.org/10.1007/978-3-030-63319-6_2
23. Barabash, O., Kopiika, O., Zamrii, I., Sobchuk, V., Musienko, A. (2018). Fraktal and Differential Properties of the Inversor of Digits of Q s-Representation of Real Number. Modern Mathematics and Mechanics, 79–95. doi: https://doi.org/10.1007/978-3-319-96755-4_5
24. Samoilenko, A. M., Samoilenko, V. G., Sobchuk, V. V. (1999). On periodic solutions of the equation of a nonlinear oscillator with pulse influence. Ukrainian Mathematical Journal, 51 (6), 926–933. doi: https://doi.org/10.1007/bf02591979
25. Sobchuk, V., Pichkur, V., Barabash, O., Laptiev, O., Igor, K., Zidan, A. (2020). Algorithm of Control of Functionally Stable Manufacturing Processes of Enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit50783.2020.9349332
26. Yudin, O., Sydorenko, V., Gnatyuk, S., Verkhovets, O. (2021). Model of the quantitative criterion calculation for security assessment of the information and telecommunications systems in the critical infrastructure of the state. Advanced Information Systems, 5 (4), 109–115. doi: https://doi.org/10.20998/2522-9052.2021.4.15
27. Semenov, S., Weilin, C., Zhang, L., Bulba, S. (2021). Automated penetration testing method using deep machine learning technology. Advanced Information Systems, 5 (3), 119–127. doi: https://doi.org/10.20998/2522-9052.2021.3.16
28. Operating System Market Share(11.2019-10.2020). Available at: https://netmarketshare.com/operating-system-market-share.aspx
29. Desktop Windows Version Market Share Worldwide (01.2021-01.2022). Available at: https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide