Methodology of Information Security Risk Assessment of Electronic Resources under Unauthorized Access Threats

Komil Kerimov
Department of System and Applied Programming
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
kamil@kerimov.uz

Zarina Azizova
Department of Information Security
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
z.i.azizova18@gmail.com

Abstract. **The article proposes a methodology for assessing the risk of information security of a computer network based on the results of the analysis of vulnerability attributes and protection attributes of information system elements, as well as security attributes of information system elements. According to the results of the research the space of information protection signs is formed. The results of the analysis of possible variants of threats of unauthorized access to electronic resources of the computer network, as well as solutions to reduce the risks of information security are given. Quantitative indicators of the results of the application of the proposed methodology to assess the risk of threats of unauthorized access to electronic resources of the computer network confirm the effectiveness of the proposed methodology, which can be used to improve the level of protection of electronic resources in organizations**

Keywords: computer network, vulnerability, risks, information security, artifacts, testing

I. Introduction.

Rapid growth rates of information technologies contribute to the expansion of business relations of a person in all spheres of his activity through the Internet. With the development of means of communication, such as computer networks, WEB sites, problems of protection of information (business, scientific) electronic resources of systems from encroachment on it by individuals have arisen.

Information security (IS) risk in the general sense is a certain probability of occurrence of an adverse event leading to some damage or loss in relation to the assets of the organization.

Information security risk of electronic resources (ER) on the Internet remains high if they are not adequately protected from unauthorized access. In this regard, the development of effective means of protecting ER information from unauthorized access remains relevant. Unauthorized access to a computer network, as a rule, is carried out through vulnerabilities in the ER, therefore, to reduce the risk of penetration to the system information, effective methods of vulnerability detection, their assessment and their exclusion are required. Nowadays the internet has become an integral part of our daily lives, with web applications serving as the backbone of various online services. However, this increased reliance on web applications has also made them attractive targets for malicious actors seeking to exploit vulnerabilities and compromise user data. Among the various attack vectors, Cross-Site Scripting (XSS) attacks have emerged as a significant security concern.

The analysis of scientific works of researchers dealing with this problem has shown that a significant part of the applied methods of risk assessment from threats of unauthorized access to the organization's assets are aimed at qualitative assessment of the threat under study. The risk arises when there is insufficient information about the consequences when making a decision, or in its absence in general. The complexity of the IS risk assessment process also depends on it. J.Bhattacharjee, A.Sengupta and K.Mazumdar proposed a formal risk assessment methodology that considers asset dependency and vulnerability dependency during risk calculation while determining the factors that affect the risk [1]. It should also be noted that in [2] the authors propose a new taxonomy of approaches to risk assessment based on qualitative, quantitative and hybrid (semi-quantitative) criteria. In

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8043

quantitative assessment of IS risks, the degree of influence of each individual scenario is considered from the point of view of the expected damage from the impact on assets of this scenario. Qualitative assessment of IS risks takes into account the measure of vulnerability and the measure of threat probability, expressed on a scale from one to five. This simplifies the stage of calculating the probability and impact of scenarios, but due to the fact that the input data are mostly the knowledge of experts, it leads to possible inaccuracies and subjectivity of the assessment. In turn, the authors [3] point out ways of applying fuzzy theory in order to reduce subjectivity.

It should be taken into account that the IS of a computer network depends largely on the competent implementation of a number of organizational and design works [4], and a significant problem for modern corporate networks are data leaks [5] - [9], which occur as a result of unauthorized influence of intruders. The proposed methodology of IS risk assessment on the example of an organization's computer network is based on the identification of threats to the security of ES and is aimed at obtaining quantitative results in the assessment of IS risks.

II. Methodology of Information Security Risk Assessment of Electronic Resources.

The most important requirements for a computer network design to meet modern information security include:

1) *Selection of the required computer network architecture.* The logical structure of the network should not depend on the physical structure. That is, the topology of the network at the link layer is built independently of the geographical location of the organizational structure network components;
2) *Effective password protection of switches, routers and servers,* providing computer network monitoring for prompt diagnostics and troubleshooting;
3) *Development of the system of notification of various events and incidents,* related to unauthorized access.

Figure 1 shows a computer network of an organizational structure in which its two subnets are geographically separated but connected by the same logical topology.

Notation: gw - gate way, dsw - distribution switch, asw - access switch.

The network is configured with six local virtual networks of Vlan type [6]:

- vlan 2 (switches for device management: dsw1,asw1,asw1,asw2, asw3, asw 4)
- vlan 3 (servers: web, file, mail);
- vlan 4 (computers of production and technical department (PTD)) ;
- vlan 5 (computers of financial and economic department (FEO));
- vlan 6 (computers of accounting department (AD));
- vlan 7 (computers - other users (U)).

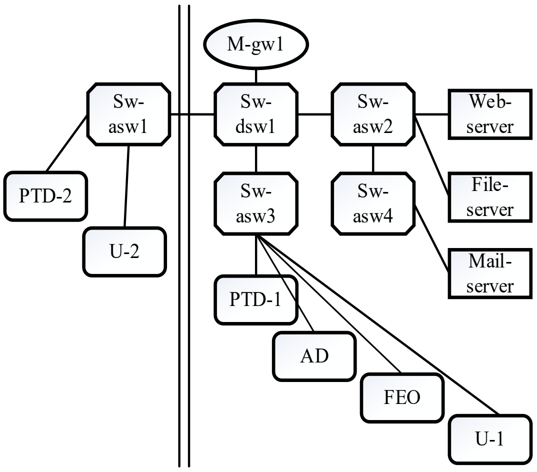

Fig. 1. Simplified diagram of the organization's computer network.

Vlans form a group of network nodes in which all traffic of a Vlan, including broadcast traffic, is completely isolated from other Vlans. Frame transmission between nodes of one Vlan occurs at the second (link) layer. Vlans communicate with each other through a router at the third (network) layer.

The computer network included:

- router *M-gw1-* for transferring data from one Vlan to another Vlan;
- switch *Sw-dsw1* for the distribution layer, where all subnets are aggregated into a common trunk;
- switches *Sw-asw1, Sw-asw2, Sw-asw3, Sw-asw4* are used as access devices. End-user computers and servers connected to them.

To assess risk, the following steps should be performed:

a) *Form the space of protection and vulnerability attributes of the project;*
b) *Build a table of project artifacts with protection and vulnerability attributes;*
c) *Develop a database of vulnerabilities;*
d) *Build a scheme of threat detection in case of unauthorized access to the project objects by protection and vulnerability attributes;*
e) *Prepare data for assessment of information security risks of the ER;*
f) *Assess IS risks in case of unauthorized access using this methodology.*

III. Formation of the Space of Information Protection Attributes

Let's represent the attributes of the computer network project as artifacts of the information security risk management process of the object with the corresponding attributes of protection and vulnerability (Tables 1-3).

TABLE 1 ARTIFACTS OF CONTROL WITH APPROPRIATE SIGNS OF PROTECTION AND SIGNS OF VULNERABILITY

№	Control artifacts	Protection feature code	Vulnerability code
1	Web server	X1	Y1
2	File server	X2	Y2
3	Mail server	X3	Y3
4	Router M-gw1	X4	Y4
5	Switch Sw-dsw1	X5	Y5
6	Switch Sw-asw1	X6	Y6
7	Switch Sw-asw2	X7	Y7
8	Switch Sw-asw3	X8	Y8
9	Switch Sw- asw4	X9	Y9
10	Computer PTD-1	X10	Y10
11	Computer PTD-2	X11	Y11
12	Computer FEO	X12	Y12
13	Computer AD	X13	Y13
14	Computer U-1	X14	Y14
15	Computer U-2	X15	Y15

TABLE 2 EQUIPMENT PROTECTION CHARACTERISTICS

№	Protection characteristic and description	Protection code index
	Characteristics of server protection	
1.	Digest Authentication program that allows you to encrypt the username and password in a request.	1
2.	HTTPS protocol, which allows encryption of all data transmitted between the browser and the server, not just usernames and passwords.	2
3.	Authentication and authorization via RADIUS server protocol. Verification of user credentials (including encrypted credentials) at the request of the served system.	3
	Switch protection characteristics	
4.	A network screen in the form of a hardware and software module filters routed and/or broadcast packets	4
5.	Packet-type firewall. Packet filters function at the network layer and control the passage of traffic based on the information contained in the packet header.	5
6.	Port security. The switch function is used to prevent unauthorized change of the MAC address of a network device.	6
7.	Port security is used to prevent overflow attacks.	7
8.	DHCP snooping. Switch function to protect against server attacks on the network or DHCP spoofing attacks.	8
9.	Dynamic ARP Inspection (Protection) - A switch feature to protect against attacks using the ARP protocol.	9
	Characteristics of computer protection	
10.	Personal firewall - software that controls the computer's network activity and filters traffic. It is installed directly on the protected computer.	10
11.	MAC authentication. An authentication method that grants access to a network by authenticating the computer rather than the user.	11
12.	Web Authentication provides access to the network by authenticating the user through a web interface. An effective method of combating IP spoofing.	12
13.	Cryptographic two-factor authentication using one-time passwords. An effective method of combating IP spoofing.	13

TABLE 3 CHARACTERISTICS OF EQUIPMENT VULNERABILITIES

№	Vulnerability characteristic and description	Vulnerability code index
	Characteristics of server vulnerability	
1.	The username and password in the request are not encrypted, (Digest Authentication is not configured).	1
2.	Data transmitted between the browser and the server and usernames and passwords are not encrypted (HTTPS protocol does not work).	2
3.	User credentials (including encrypted credentials) are not verified at the request of the served system, (RADIUS server protocol is not implemented).	3
4.	Insecure password recovery. A vulnerability occurs when a Web server allows an attacker to unauthorized obtain, modify, or recover other users' passwords.	4
5.	Inadequate authentication. A Web server allows an attacker to access sensitive information or server functions without proper authentication.	5
6.	Insufficient authorization. With insufficient authorization, the Web server allows an attacker to access sensitive information or features that should be restricted.	6
	Characteristics of switch and router vulnerabilities	
7.	Network shield in the form of a hardware and software module is not installed (or configured). Routed and/or broadcast packets are not filtered.	7
8.	Packet-type firewall is not installed (or configured). The network layer does not filter and control traffic flow based on packet header information.	8
9.	The switch's Port security feature is not configured. The MAC address on the switch's network card has changed, causing packets to be sent to the port to which the attacker is connected.	9
10.	The switch's Port security feature is not configured. The switching table is full. After the table is full, the switch does not learn new MAC addresses and starts working as a network hub, sending traffic to all ports.	10
11.	DHCP Snooping server is not used. An attack involving the spoofing of a DHCP server on a network or a DHCP starvation attack forces the DHCP server to give out all existing addresses on the server to the attacker.	11
12.	Dynamic ARP Inspection (Protection) - The switch feature to protect against attacks using the ARP protocol is not used.	12
	Characteristics of computer vulnerabilities	
13.	The computer's network activity is not monitored and traffic is not filtered according to the specified rules. Personal firewall is not installed directly on the protected computer.	13
14.	MAC authentication is not properly configured. Unauthorized access to the computer's network is open while connected to the switch.	14
15.	Unauthorized access to the network is opened during user authentication via the Web interface (Web authentication is not properly configured).	15
16.	Weak authentication.	16

IV. DATABASE FOR INFORMATION SECURITY RISK ASSESSMENT.

The database project includes the following data sets:

1) *Artifacts of security feature codes.*
2) *Artifacts of vulnerability feature codes.*

3) *Characteristics of server security features.*
4) *Characteristics of router security features.*
5) *Characteristics of switch security features.*
6) *Characteristics of signs of vulnerability of servers.*
7) *Characteristics of signs of vulnerability of the router.*
8) *Characteristics of switch vulnerability signs.*
9) *Characteristics of computer vulnerability indicators.*
10) *Temporal array about the operational state of the computer's ER.*
11) *Temporary array of artifacts, with corresponding codes of protection and vulnerability attributes.*

Formation of stages of information security risk assessment of a computer network. IS risk assessment carried out according to the following stages:

a) *Readings on the operating state of the protection elements are taken (array 10).*
b) *Using arrays 1, 2, and 10, an array of artifacts is generated, with corresponding threat and vulnerability feature codes (array 11).*
c) *Using arrays 3,4,5,6 and 11, the presence of a threat to the computer network ER is determined.*
d) *Information security risk assessment is performed.*
e) *A decision is made to reduce information security risks.*

V. Risk Assessment of Unauthorized Access Threats to Electronic Resources of a Computer Network

Let the testing of defence elements result in an array of 10 (Table 4).

Note: In Table 4, the value of the protection code index in the third column of Tables 2-3 corresponds to the protection or vulnerability characteristic of the artifact. For example, X10 (protection code index), U11 (vulnerability code index).

TABLE 4 RESULTS OF TESTING THE ELEMENTS OF PROTECTION

№	Control artifacts	State of the protection element
1.	Web server	Y1(4)
2.	File server	X2(3)
3.	Mail server	X3(2), X3(3)
4.	Router M-gw1	X4(1), X4(2)
5.	Switch Sw-dsw1	X5(1), X(2)
6.	Switch Sw-asw1	X6(5), X6(6), Y6(9), X6(7)
7.	Switch Sw-asw2	X7(5), X7(6), X7(7), X7(9)
8.	Switch Sw-asw3	X8(5), X8(6), X8(7), X8(9)
9.	Switch Sw- asw4	X7(5), X7(6), X7(7), X7(9)
10.	Computer PTD-1	X10(13), X10(14), X10(15), X10(16)
11.	Computer PTD-2	X11(13), Y11(14), У11(15), У11(16)
12.	Computer FEO	X12(13), X12(24), X12(15), X12(16), X12(17)
13.	Computer AD	X13(13), X13(24), X13(15), X13(16), X13(17)
14.	Computer U-1	X14(13), X14(24), X14(15), X14(16), X14(17)
15.	Computer U-2	X15(13), X15(24), X15(15), X15(16), X15(17)

With the help of arrays 1,2,10, array 11 - an array of artifacts with the corresponding codes of threat and vulnerability features (Table 5) formed.

TABLE 5 RESULTS OF TESTING FOR THE FORMATION OF AN ARRAY OF ARTIFACTS

№	Control artifacts	State of the protection element
1.	Web server	Y1(4)
2.	File server	Y1
3.	Mail server	x2
4.	Router M-gw1	x3
5.	Switch Sw-dsw1	x4
6.	Switch Sw-asw1	Y5
7.	Switch Sw-asw2	Y6
8.	Switch Sw-asw3	x7
9.	Switch Sw- asw4	x8
10.	Computer PTD-1	x9
11.	Computer PTD-2	x10
12.	Computer FEO	Y11
13.	Computer AD	x12
14.	Computer U-1	x13
15.	Computer U-2	x14

VI. Analysis of Possible Variants of Unauthorized Access Threats to Electronic Resources of a Computer Network.

The results of data analysis, using arrays 3, 4, 5, 6 and 11, summarized in Table 6.

Let's consider possible variants of threats of unauthorized access to the computer network ER, according to the results of testing to form an array of artifacts:

A. "Insecure Password Recovery" vulnerability, where the Web server allows an attacker to unauthorized obtain, modify, or recover the password of a PTD-2 computer user.

Possible Threats:

- Denial of Service (DoS - attack) - an attack on some system resource to bring it to failure.

B. Switch Sw-asw1 Vulnerability "The switch Port security feature is not configured correctly".

Possible Threats:

- MAC-spoofing attack, which changes the MAC address on a switch's network card, causing packets to be sent to the port to which the attacker is connected.

C. PTD-2 Computer vulnerability "MAC authentication not properly configured" opens unauthorized access to the network when it connects to the switch.

Possible Threats:

- Man in the middle (MitM) - The attacker is between two victims, either listening to the traffic that is passed between them or intercepting it and spoofing it. At the same time, for the victims of the attack, there are no visible signs of the attack;
- Denial of Service (DoS attack) - an attack on a system resource to bring it to failure.

TABLE 6 RESULTS OF TESTING FOR THE FORMATION OF AN ARRAY OF ARTIFACTS

№	**Control artifacts**	**Vulnerable electronic resources**			**Possible attacks on vulnerabilities of electronic resources**
		Y1(4)	*Y6(9)*	*Y11(14)*	
1.	M-gw1				
2.	Web server	yes			“Denial of service”, attack on Y1(4)
3.	File server				
4.	Mail-server				
5.	Sw-dsw1				
6.	Sw-asw1		yes		“MAC spoofing” attack on Y6(9)
7.	Sw-asw2				
8.	Sw-asw3				
9.	Sw-asw4				
10.	PTD-1				
11.	PTD-2			yes	“Man in the middle” attack on Y11(14) “Denial of service” attack on Y11(14)
12.	FEO				
13.	AD				
14.	U-1				
15.	U-2				

VII. INFORMATION SECURITY RISK ASSESSMENT IN CASE OF UNAUTHORIZED ACCESS

Assessment of IS risk from unauthorized access threats is based on the data in Table 7. Let us introduce notations for the following parameters [4]:

- Pg – threat attribute of one ER vulnerability;
- Dt– threat characteristic of an ER threat as a sum of threat attributes;
- Uj – characteristic of the set of ER threats on the path with index j. The line of information interaction between the end user of one Vlan and the end user of another Vlan taken as the path with index j.
- Vj – IS risk of the path with index j from one end-user to another end-user;
- V – IS risk of the computer network

To estimate Dt, we index Pg by the index t (t= 1,2,...,15). In this case, the sign Pgt at the intersection of the vulnerability column g and row t of the ER of Table 7 takes the value 1 if vulnerability occurs, otherwise 0. The value of Dt is determined by the following expression:

$$Dt = \begin{cases} 0, & \sum_{g=1}^{4} Pgt = 0 \\ \sum_{g=1}^{4} Pgt, & \sum_{g=1}^{4} Pgt > 0 \end{cases},$$

According to the results of calculations, the following values for threat characteristics Dt, $(t = 1,2,\dots,15)$ are obtained:

M-gw1	D1=0
Web-server	D2=1
File-server	D3=0
Mail-server	D4=0
sw-dsw1	D5=0
sw-asw1	D6=0
sw-asw2	D7=0
sw-asw3	D8=0
sw- asw4	D9=0
PTD-1	D10=0
PTD-2	D11=1
FEO	D12=0
AD	D13=0
U-1	D14=0
U-2	D15=0

The threat characteristic Uj is defined as the sum of the characteristics [10] of the ER threats on the interaction path of two end-users.

Let us index the parameter Dt by index j (1,2,...,m). We define Uj using the data for threat characteristics from the following expression:

$$j = \begin{cases} \sum_{1}^{q} Dq, & 0 < \sum_{1}^{q} Dq < Lj \\ 0, & \sum_{1}^{q} Dq = 0 \end{cases},$$

where the index q, is defined by the number of vulnerable ERs on the path with index j. The results of the Uj calculations summarized in Table 7.

TABLE 7 RESULTS OF THE DATA ANALYSIS

№	**Information paths in the graph of a computer network**							Uj	Uj
1	a1	a10	a8	a5	a7	a2		1	1
2	a1	a10	a8	a5	a7	a3		0	0
3	a1	a10	a8	a5	a7	a4		0	0
4	a1	a12	a8	a5	a7	a2		1	1
5	a1	a12	a8	a5	a7	a3		0	0
6	a1	a12	a8	a5	a7	a9	a4	0	0
7	a1	a13	a8	a5	a7	a2		1	1
8	a1	a13	a8	a5	a7	a3		0	0
9	a1	a13	a8	a5	a7	a9	a4	0	0
10	a1	a14	a8	a5	a7	a2		1	1
11	a1	a14	a8	a5	a7	a3		0	0
12	a1	a14	a8	a5	a7	a9	a4	0	0
13	a1	a11	a6	a7		a2		3	1
14	a1	a11	a6	a5	a7	a3		2	1
15	a1	a11	a6	a5	a7	a9	a4	2	1
16	a1	a15	a6	a5	a7	a2		2	1
17	a1	a15	a6	a5	a7	a3		1	1
18	a1,	a15	a6,	a5	a7	a9	a4	1	1
19	a1	a11	a6	a5	a8	a12		2	1
20	a1	a11	a6	a5	a8	a13		2	1
21	a1	a11	a6	a5	a8	a14		2	1
22	a1	a15	a6	a5	a8	a1		1	1
23	a1	a15	a6	a5	a8	a12		1	1
24	a1	a15	a6	a5	a8	a13		1	1
25	a15	a6	a5	a8	a14			1	1
26	a11	a6	a5	a8	a10			2	1

The IS risk of end-user ER information interaction on the path Vj , (j= 1,2,...,15) is determined from the expression:

$$V_j = \begin{cases} 1, & 0 < Uj \\ 0, & Uj = 0 \end{cases}$$

The results of IS risk on the path Vj are summarized in Table 7. The vertices of the graph are identified with the corresponding ERs of the network and labeled with symbols ak, $(k = 1,2,\ldots,15)$.

To assess the IS risk, let us represent the computer network (Figure 2) as a finite graph (Figure 3). In Figure 2, the shaded nodes of the graph simulate the vulnerabilities of the electronic resources of the computer network. With the help of the graph, using Table 7, it is possible to identify a subgraph of the part of the computer network exposed to IS risk (Figure 3), as well as the part not exposed to IS risk (Figure 4).

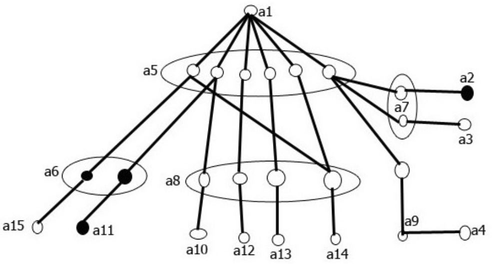

Fig. 2. Simplified diagram of the organization's computer network.

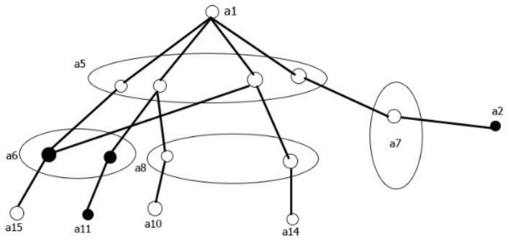

Fig. 3. Subgraph of the part of computer network exposed to information security risk.

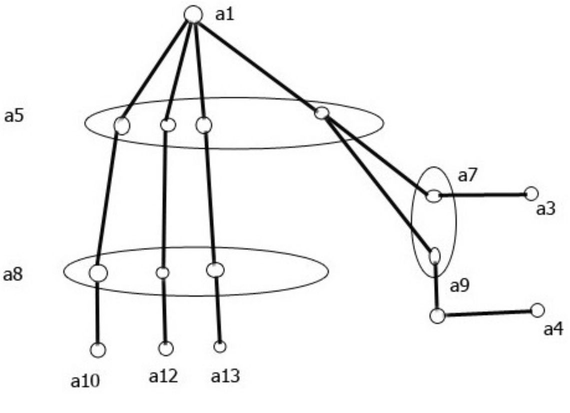

Fig. 4. Subgraph of the part of computer network not exposed to information security risk.

Table 7 shows that the total number of end-user ER interaction paths is 26 and the number of exposed paths is 18. The IS risk value of a computer network is calculated by the following expression:

$$V = f(x) = \begin{cases} \sum_{1}^{n} Vj, & \sum_{1}^{n} Vj > 0 \\ 0, & \sum_{1}^{n} Vj = 0 \end{cases},$$

where $n = 26$ is the total number of end-user interaction paths. Calculating the risk of IS, computer network, by the above expression, show that the percentage of V is: $V = (18/26) \times 100 = 70$ %.

The risk of information security of a computer network with identified vulnerabilities is high. Mitigation measures are required.

Information Security Risk Mitigation Solutions. The following actions are required to reduce IS risk in case of threats that disrupt the computer network:

- selection of the optimal mode of secure operation of the information system for the current situation;
- selection of the optimal service discipline for local and remote users communicating with the information system;
- switching on the reserve ERs of the system in case of their overloaded state;
- blocking of some nodes of the computer network for some time or until a new situation occurs;
- blocking of service requests for a certain category of information system users;
- blocking of some modes of operation of the information system, etc.

Depending on the situation, the minimum IS risk is achieved by performing one or more of the above actions.

VIII. Conclusion

Information security risk assessment is an important part of a comprehensive approach to information security. In this regard, a prerequisite for protecting electronic resources is the process of analyzing and then assessing IS risks for their subsequent identification as a possible threat and taking appropriate countermeasures to manage them.

In the paper we proposed the principles of IS risk assessment in case of threats of unauthorized access to the computer network ER, and developed a methodology for determining the IS risk, which is based on the recognition of signs of threats of unauthorized access to ER. The effectiveness of the proposed methodology is considered on a specific example of application of the methodology of IS risk assessment at possible threats of unauthorized access to the computer network ER. The study has shown that to assess the IS risk to the network requires information about vulnerabilities that open unauthorized access to its ER, as well as knowledge about the ways of interaction of end users of the network.

References

[1] J. Bhattacharjee, A. Sengupta and C. Mazumdar, "A formal methodology for Enterprise Information Security risk assessment," presented at 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS), La Rochelle, France, 2013.

[2] A. Shameli-Sendi, R. Aghababaei-Barzegar and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," Computers & Security, vol. 57, pp. 14-30, 2016.

[3] Y. Ye, W. Lin, S. Deng and T. Zhang, "A Practical Solution to the Information Security Risk Evaluation Problems in Power Systems," presented at 2014 International Conference on Future Computer and Communication Engineering, Tianjin, China, 2014.

[4] R. Khamdamov, K. Kerimov and J. Ibrahimov, "Method of Developing a Web-Application Firewall", Journal of Automation and Information Sciences, vol. 51, pp. 61-65, 2019.

[5] S. Bezzateev, T. Elina, V. Mylnikov and I. Livshits, "Methodology of information systems risk assessment based on the analysis of user behavior and information security incidents," Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics, vol. 21, pp. 553-561, 2021.

[6] F. Krachten , Introduction to Rational Unified Process - 2.ed.: Williams, 2002.

[7] A. Astakhov, The Art of Information Risk Management. M: DMK Press, 2010.

[8] P. Khorev, Methods and means of information protection in computer systems. M: Helios, 2006.

[9] S. Zapechnikov, Information security of open systems. In 2 vol. Vol. 1 Threats, vulnerabilities, attacks and approaches to defense. M: GLT, 2017.

[10] V. Opanasenko, S. Kryvyi, "Synthesis of Adaptive Logical Networks on the Basis of Zhegalkin Polynomials", Cybernetics and Systems Analysis, vol. 51, pp. 969–977, 2015.