UDC 004.492

The Best Scenario of Cyber Attack Selecting on the Information and Communication System Based on the Logical and Probabilistic Method

Lesia Alekseichuk[1], Oleksii Novikov[1], Andrii Rodionov[1], Dmytro Yakobchuk[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,*
37, Prosp. Beresteyskyi, Kyiv, 03056, Ukraine

Abstract

The task of analyzing and selecting the best scenario of a cyberattack on information and communication system is considered as a component of the task of analyzing systems security. A method and corresponding algorithm for finding the best scenario of an attack on information and communication system using a logical and probabilistic model is proposed. The model describes the development of adverse events that arise in the information and communication system from the implementation of possible attacks on the security system from cyberspace. Analysis of cyber attack scenarios allows predicting the development of possible adverse cyber security events from the implementation of multiple threats to the system. The developed method and corresponding algorithm for analyzing attack scenarios can be used to analyze the security of information and communication systems, as well as in automation systems for designing information security systems or designing attacks on such systems.

Keywords: Scenarios of cyberattacks on information and communication systems, Logical and probabilistic model of cyber security.

Introduction

Information and communication systems (further, ICS) remain the preferred targets of cybercriminals. Most often, the goal of these attacks is the organization of interruptions in the work of these systems and accidents in the work of enterprises or the suspension of key technological processes. The success of such cyberattacks is facilitated by the obsolescence and defects in the protection of ICS and their components, the growth in the skills of cybercriminals, a significant increase in the market for malicious software, and other factors.

The issue of security analysis of ICS remains relevant and attracts the attention of many researchers. In works [1] - [4], the main threats aimed at these objects are considered, the classification and methodology of countermeasures against threats are provided.

The level of cyber security of ICS is largely determined by the ability of specialists to predict the sequence of actions of attackers, possible trajectories and characteristics of attacks. Therefore, a lot of research is devoted to the issue of analyzing attack scenarios. In works [5]- [7], scenarios of attacks on ICS are analyzed, various approaches to the implementation of such attacks are considered. When analyzing scenarios, it is important to choose a methodology for describing attacks on information systems, in particular methods for describing trajectories and quantifying the effectiveness of attacks. Among the methods of describing attacks, the most famous are the method of attack trees, fault trees, risk trees [8], [9], attack graphs [10] - [15] and others.

An effective addition to the methods of describing attacks is the use of the list of known vulnerabilities and security defects of software CVE (CommonVulnerabilities and Exposures)

[16], the list of known techniques, techniques and tactics used by attackers for attacks ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) of the American company MITRE [17] and information from the American database of NVD vulnerabilities (National Vulnerability Database) [18].

Most methods of describing attacks do not operate and do not provide a quantitative assessment of attack effectiveness, so they are often supplemented with additional methods or procedures for such assessment. Among them is the logical and probabilistic method [19], which allows you to calculate the probability of a successful attack, the standard for calculating quantitative assessments of computer system security vulnerabilities CVSS (Common Vulnerability Scoring System) [20], methodology of factor analysis of information risks FAIR (Factor Analysis of Information Risk) [21] and others.

Analysis of attack scenarios in many cases allows not only to evaluate the effectiveness of cyber attacks, but also to develop countermeasures to increase the level of cyber defense of the ICS. The works [22 - 24] are devoted to the solution of such problems. In works [25 - 27], based on the analysis of ICS threats, methods of building a security information system network topology and optimal placement of information protection mechanisms are proposed.

Given the importance of the problem of analyzing scenarios of cyberattacks on ICS and their insufficient development, further scientific research is currently necessary. In particular, the task of developing methods for quantitative analysis of the consequences of cyber attacks on information systems, determining the level of their effectiveness and selecting the best attack scenario is urgent.

The aim of the study. For ICS with fixed physical, logical structures and the structure of the information security system, propose an approach to choose the best scenario of an attack on the ICS, which would provide the maximum quantitative criterion for the success of the attack using the logical and probabilistic method.

Description of the ICS model. To describe the logical structure of ICS, we use an oriented graph $G(V,E)$, where $v_i \in V$ is the set of system objects/ information resources/ services, $E=(e_1,..., e_L)$, $e_k=(v_i,v_j)$ is the presence or absence of ties between them, $E \subseteq V \times V$ and $e_i \in E$.

Such a description allows taking into account the network structure and connections between system objects. The network structure will depend on the switching connections and the corresponding network settings. While building the logical structure of the ICS, possible information flows should be taken into account, to build attack scenarios more accurately in the future.

If several services are located on one physical server, which can be objects, sources of threats or attack scenarios can pass through them, then we will separate them into separate objects v_i. We will present the resulting graph $G(V,E)$ in the form of an adjacency matrix, which is called an object accessibility matrix. The graph will be oriented because some objects can initiate connections only in one-way order.

The concept of an attack scenario on ICS. Attack on ICS is an unauthorized informational influence on the system both through network channels and, directly, on the elements of the system. We will consider the attack scenario as a sequence of actions of the attacker, which he needs to perform in order to successfully attack a specified object of the system - the target of the attack. Such actions of the attacker will consist of successive capture of objects that are connected by information flows with the specified object, starting with the object to which he has, or is able to gain access. When capturing the object (service, resource) we will understand the attacker's ability to attack and capture the target of the attack. Under the analysis of attack scenarios, we will understand the analysis of the ways in which these attacks can be carried out and the conditions for their implementation. A successful attack on the ICS means a violation of the information security policy and (or) causing significant damage to one of the system's critical objects [28].

Thus, to build an attack scenario, it is necessary to know the sources of threats, the connection (topology) of ICS services with each other, as well as the targets (objects) of attacks. That is, in fact, it is necessary to have a comprehensive model of threats on ICS.

Description of the comprehensive ICS threat model. To build a complex threat model on ICS, among the ICS objects $V=\{v_1,...,v_N\}$, a set of critical objects, which are considered attack objects $O = (o_1, \dots, o_M) \subset V$, is selected, and the set of objects that are considered sources of threats $A = (a_1, \dots, a_K) \subset V$. A condition for the success of an attack on ICS is a successful attack on at least one of its critical objects $O = (o_1, \dots, o_M) \subset V$. The number of attack objects can include services and servers that are critical from the point of view of security and functioning ICS, and among the sources of threats are users' computers, services connected to the Internet and external networks. The set of attack objects (critical objects) of the system can consist of services, servers, network equipment and other critical components of the ICS.

The tuple $G(V, E, A, O)$, which includes the network graph $G(V, E)$, attack objects $O \subset V$ and threat sources $A \subset V$, is called an attack graph. The set of paths from the sources of threats $A = (a_1, \dots, a_K)$ to the selected attack object o_t will contain the set of all possible ways of penetration of the attacker - attack scenarios:

$$(A; o_t) = \tag{1}$$
$$= \{\{(a_1; o_t)\}, \{(a_2; o_t)\}, \dots, \{(a_K; o_t)\}\}.$$

The attacker's ability to capture intermediate objects and successfully attack the target is defined as the estimated values of the probabilities $P = \{P_1, \dots, P_N\}$ for each object $V = \{v_1, \dots, v_N\}$ of the information system. Data on the probability of capturing objects are independent and are a relevant characteristic of ICS objects.

Thus, the complex model of threats will be defined by the tuple $G(V, E, A, O, P)$, where $G(V, E)$ is the topology of the ICS network, $A \subset V$ are the sources of threats, $O \subset V$ is the set of attack objects, $P = \{P_1, \dots, P_N\}$ are the probabilities of capture of ICS objects. This tuple is called an attack graph.

Logical and probabilistic criterion for the probability of success of the attack scenario. To solve the problem of analyzing attack scenarios and determining the best one among them, consider an ICS with known fixed network topology $G(V, E)$ and a set of critical objects for attacks $O = (o_1, \dots, o_M) \subset V$. Let us consider $J(A) -$ the functional of the success of attack scenarios (success of attacks) on ICS. We will give the meaning of this functionality as the probability of the ICS reaching an undesirable state, which is introduced, developed and widely used in the logic and probabilistic theory of security of complex systems [19].

The fundamental concepts of logic and probabilistic theory of security are the concept of a dangerous state of the system. Provided there is a formal description of the dangerous state function, we will use it as a criterion for the success of the ICS attack scenario. Let's consider the methodology of constructing such a criterion.

According to the logic and probabilistic theory of security, attack scenarios constitute a conjunction of a sequence of events Z_i, none of which can be removed without violating the corresponding scenario. Let's write the following conjunction in the form of a function of the algebra of logic (FAL) as:

$$\varphi_l = \bigwedge_{i \in K_{\varphi_l}} Z_i \,,$$

where K_{φ_l} is the sequence of actions of the attacker in the ICS, which leads to the dangerous state of the specified object of the system, which corresponds to the l - th attack scenario.

Based on this, each real ICS can be represented in the form of a threat state function (TSF) - a finite set of attack scenarios (l =1, 2, …, d), and events Z_i, (where $i \in K_{\varphi_l}$):

$$y(Z_1,\ldots,Z_m) = \bigvee_{l=1}^{d} \varphi_l = \bigvee_{l=1}^{d} \left[\bigwedge_{i \in K_{\varphi_l}} Z_i \right]. \tag{2}$$

According to the logic and probability theory, the probability of the transition of the ICS to a dangerous state will be formulated as:

$$P\{y(Z_1,\ldots,Z_m) = 1\} = P\left\{ \bigvee_{l=1}^{d} \left[\bigwedge_{i \in K_{\varphi_l}} Z_i \right] = 1 \right\}. \tag{3}$$

$P\{y(Z_1, \dots, Z_m) = 1\}$ can be calculated using the known probability functions of each of the events Z_i. To do this, it is necessary to transform TSF (2) into one of the equivalent forms: orthogonal disjunctive normal form, perfect disjunctive normal form, or unique function in the basis of conjunction-negations [19]. For them, it is possible to directly replace the Boolean variables for them, it is possible to directly replace the Boolean variables with their probabilistic values $P\{Z_i = 1\} = P_i$ (relationship (3)).

Based on this methodology, it is possible to write a logical and probabilistic criterion for the probability of success of an attack scenario on ICS:

$$J(A) = P(G, A, O, P), \tag{4}$$

where all variables are defined above.

We note that in the future, when building a procedure and algorithm for analyzing ICS attack scenarios and determining the best among them, the network topology and the set of critical objects for attacks will be fixed, and function A - the finite set of possible attack scenarios - will be an independent variable.

Note that changes in parameters A will lead to a change in the structure of the ICS model, which will have an impact on the final value of the criterion for the probability of success of an attack $J(A)$ on ICS.

Analysis of success and selecting of the best scenario of attack on ICS. Let's formulate the problem of analyzing and selecting the best scenario of a cyberattack on ICS based on the known topology of the network $G(V,E)$ and the structure of the cyber security system $O=(o_1,\ldots,o_M)\subset V$ ICS. Among all possible scenarios of cyberattacks, find the following scenario (graph structure) that provides the maximum of the functional $J(A)$:

$$\begin{cases} A^* = \arg\max_{A\in V} J(A) \\ A=(a_1,a_2,\ldots,a_K\}\subset V \end{cases}, \qquad (5)$$

where $A=(a_1,\ldots,a_K)\subset V$ - finite set of possible attack scenarios, A* - the best attack scenario that gives the functional $J(A)$ the maximum value.

As mentioned above, the functional $J(A)$ should determine the quantitative measure of the success of the attack, in addition, it should depend on the main parameters of the ICS model and the complex threat model, such as topology, descriptions of the placement of critical objects for attacks, attack scenarios, etc.

Algorithm for selecting of the best scenario of attack on ICS. Let's formulate an algorithm for building the probability function of the best scenario of attack on ICS in the following form:

1. To define the set of objects/ resources/services in ICS $V=\{v_1,\ldots,v_N\}$;
2. To present the logical topology of the ICS network in the form of a graph $G(V,E)$;
3. To determine the categories of intruders and the multitude of sources of threats $A=(a_1,\ldots,a_K)\subset V$, as well as a variety of attack targets $O=(o_1,\ldots,o_M)\subset V$;
4. To determine the probabilities of capturing objects $P=\{P_1,\ldots,P_N\}$, included in the attack scenarios and build a comprehensive threat model $G(V,E,A,O,P)$;
5. To define a set of attack paths for each of the identified attack objects:

$$\begin{cases} (A;o_1)=\{\{(a_1;o_1)\},\{(a_2;o_2)\},\ldots,\{(a_K;o_1)\}\} \\ (A;o_2)=\{\{(a_1;o_2)\},\{(a_2;o_2)\},\ldots,\{(a_K;o_2)\}\} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ (A;o_M)=\{\{(a_1;o_M)\},\{(a_2;o_M)\},\ldots,\{(a_K;o_M)\}\} \end{cases}$$

6. For each of the attack objects $o_i\in O$, based on the attack graph, write the attack paths (A,o_i) in the form of a logic algebra function (2);
7. Write down the function of the dangerous state in the form (3);
8. To convert the dangerous state function to the orthogonal disjunctive normal form (ODNF) to construct the success probability functions of the attack scenario;
9. To construct the function of the probability of success of the attack scenario $J(A)$ for ICS in the form (4);
10. Based on the values of the object capture probabilities $P=\{P_1,\ldots,P_N\}$ to calculate the set of criteria for the probability of success of attack scenarios on ICS $J_1(a_1)$, $J_2(a_2)$, …, $J_K(a_K)$ ((ratio (4)) for each of the possible attacks $A=(a_1,\ldots,a_K)\subset V$;
11. Determine the maximum functional $J_{max}(A)$ of the finite number of arguments $A=(a_1,\ldots,a_K)\subset V$ and the corresponding best attack scenario A^* (relation (5)).

In order to determine the efficiency of the developed method and algorithm for selecting the best scenario of attack on ICS, we will consider an example.

An example of using the algorithm for selecting of the best scenario of attack on a local network connected to the Internet.

Consider the ICS, which is a local network connected to the Internet [26].

The network contains web and mail servers connected to a database server. In addition, users use the application server, which also communicates with the database server. In addition, the network has an automatic workplace (AWP) of a user and an administrator's AWP, which has access to all servers of the system (Figure 1).

Consider the case when an attacker wants to gain access to a critical attack object - a database server $O_{serv}\subset V$.

To solve the problem, use the proposed algorithm, according to which:

1. Let's build an access matrix of hosts among themselves (Figure 2), as well as a logical diagram of a local network (Figure 3).

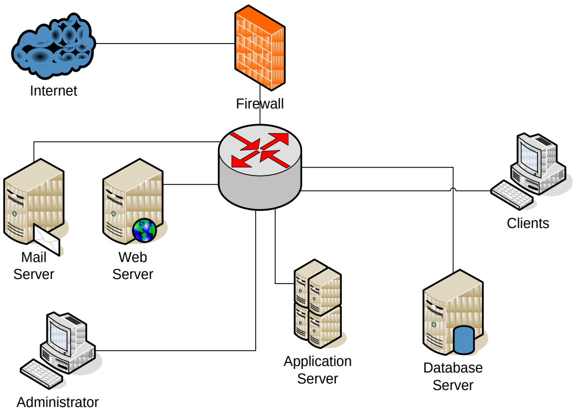

Figure 1: Physical structure of the local network

The matrix shows the connection of network hosts to each other. If the connection is present, then the cell at column and row is set to 1 for corresponding serial number of the host. If there is no connection - 0.

$$\begin{array}{c|ccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & - & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & - & 0 & 0 & 0 & 0 & 1 \\ 3 & 1 & 0 & - & 0 & 0 & 0 & 1 \\ 4 & 1 & 1 & 1 & - & 1 & 1 & 1 \\ 5 & 0 & 0 & 0 & 0 & - & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 1 & - & 1 \\ 7 & 0 & 0 & 0 & 0 & 0 & 1 & - \end{array}$$

Figure 2: Host access matrix, where 1 – Firewall, 2 – MailServer, 3 – Web Server, 4 Administrator, 5 – Clients

2. Define categories of intruders, multiple sources of threats $A = (a_1, \dots, a_K) \subset V$ and a critical object for an attack $O_{serv} \subset V$ - the cyber security system of the database management server.

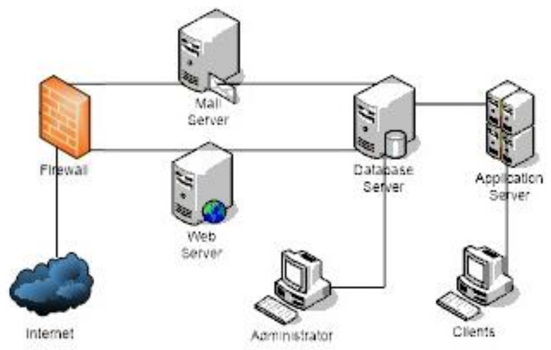

Figure 3: Logical structure of the local network

We will consider two categories of intruders: external (from the Internet) and internal (from the local network). In this way, the entry points to the system will be: the firewall, the administrator's AWP, and the user's AWP.

The attack scenario can be considered successful if the attacker gains access to the servers that have direct access to the database management server: web server, mail server, application server, and the administrator's AWP. Figure 4 shows the sources and paths of the attacks on the database management server.

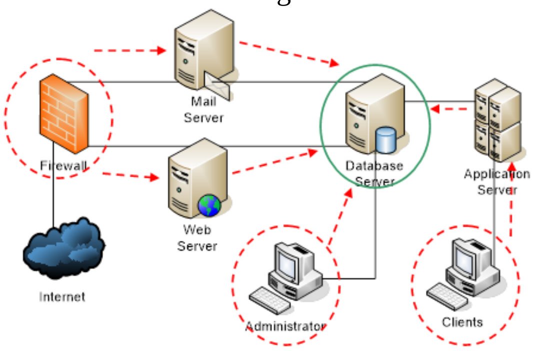

Figure 4: Sources and paths of attacks on the database management server

3. Based on the access matrix of hosts and logical circuits of the local network, we automatically form a scenario of attack development. In Figure 5, we present the scenario of an attack on a database server in the form of a graph.

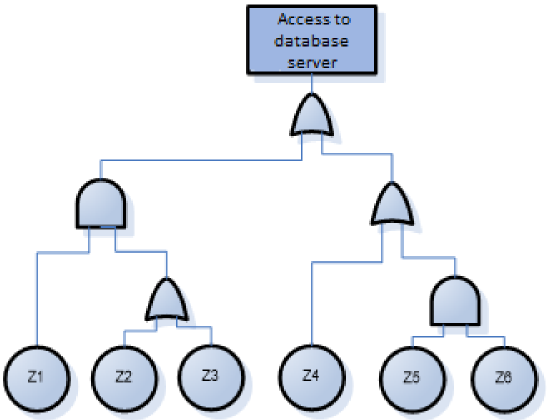

Figure 5: Attack scenarios in the form of a graph, where Z1 – Capture Firewall, Z2 – Capture Mail Server, Z3 – Capture Web Server, Z4 – Capture Administrator, Z5–Capture Clients, Z6 – Capture Application Server

4.Based on the defined graph (Fig. 5) and relation (2), we will construct the function of the dangerous state y

$$y(Z_1,\dots,Z_6) = Z_1(Z_2 \vee Z_3) \vee (Z_4 \vee Z_5Z_6) =$$

$$= Z_1Z_2 \vee Z_1Z_3 \vee Z_4 \vee Z_5Z_6 \; . \qquad (6)$$

5. To move to the probabilistic form (3), let's write (6) in the form

$$\begin{aligned} y(Z_1,\dots,Z_6) &= Z_1(Z_2 \vee Z_3) \vee (Z_4 \vee Z_5Z_6) = \\ &= Z_1(Z_2'Z_3')' \vee (Z_4'(Z_5Z_6)')' = \\ &= [(Z_1(Z_2'Z_3')')'((Z_4'(Z_5Z_6)')')']' = \\ &= [(Z_1(Z_2'Z_3')')'(Z_4'(Z_5Z_6)')].' \qquad (7) \end{aligned}$$

6. Let's write $P\{y(Z_1,\dots,Z_6) = 1\}$ by replacing Z$_i$ in (7) with $P\{Z_i = 1\} = P_i$ and get the function of the probability of success of the attack scenario $J(A)$:

$$\begin{aligned} J(A) \; &= \; P\{y(Z_1,\dots,Z_6) = 1\} = \\ &= P\{[(Z_1(Z_2'Z_3')')'(Z_4'(Z_5Z_6)')]' = 1\} = \\ &= 1 - \left[1 - P_1\left(1 - (1 - P_2)(1 - P_3)\right)\right] \\ &\quad [(1 - P_4)(1 - P_5P_6)]. \qquad (8) \end{aligned}$$

7. Based on relation (8) and the known probabilities of capturing objects $P = \{P_1,\dots,P_N\}$, we will calculate a set of criteria for the probability of success of network attack scenarios $J(a_1)$, $J(a_2)$, …, $J(a_K)$ for each of possible attacks $A = (a_1,\dots,a_K) \subset V$;

8. We determine the maximum functional $J_{max}(A)$ of the finite number of arguments $A = (a_1,\dots,a_K) \subset V$ and the corresponding best attack scenario A^* (relation (5)).

In order to determine the efficiency and main quantitative characteristics of the developed method and algorithm for selecting of the best scenario of attack on the Database Server of a local network connected to the Internet, we will conduct a computational experiment.

Analysis of the results of the computational experiment. We will obtain and analyze the quantitative characteristics of the algorithm for selecting of the best scenario of attack on the Database Server of a local network connected to the Internet. To do this, we will place the main input and output data of the experiment in Table 1.

In the columns of Table 1, the values of the probabilities of the realization of the capture conditions are given Firewall - P_1, Mail Server - P_2, Web Server - P_3, AWP Administrator – P_4, AWP Clients - P_5, Application Server P_6. The rows contain the probable conditions for several attacks $A(a_1,\dots,a_{13})$ on Database Server. The last column shows the values of the criteria for the probability of success of the attack scenarios $J(a_1)$, $J(a_2)$, …, $J(a_{13})$ on the Database Server.

Table 1. Probable values of P_j, $j=1,..,6$ and success results of $J(A)$ attacks $A(a_1,\dots,a_{13})$ on Database Server

	P_1	P_2	P_3	P_4	P_5	P_6	$J(A)$
a_1	1.0	X	1.0	X	X	X	1.0
a_2	1.0	1.0	X	X	X	X	1.0
a_3	1.0	1.0	1.0	X	X	X	1.0
a_4	X	X	X	1.0	X	X	1.0
a_5	X	X	X	X	1.0	1.0	1.0
a_6	0,6	0,2	0,4	0,7	0,1	0,5	0,8039
a_7	0	0,2	0,4	0,7	0,1	0,5	0,715
a_8	0,6	0	0,4	0,7	0,1	0,5	0,7834
a_9	0,6	0,2	0	0,7	0,1	0,5	0,7492
a_{10}	0,6	0,2	0,4	0	0,1	0,5	0,3464
a_{11}	0,6	0,2	0,4	0,7	0	0,5	0,7936
a_{12}	0,6	0,2	0,4	0,7	0,1	0	0,7936
a_{13}	0,5	0,5	0,5	0,5	0,5	0,5	0,7656

The first five rows of Table 1 show the values of the probability of the conditions that correspond to the scenarios of five successful attacks on the Database Server: a_1– capture of the Firewall and capture of the Web Server; a_2 – Firewall capture and Mail Server capture; a_3 – capture of Firewall with simultaneous capture of Mail Server and Web Server; a_4 - capture of the Administrator's AWP; a_5 – simultaneous capture of Clients and Application Server AWP. The first three scenarios are external attacks, and the fourth and fifth are internal attacks. All scenarios give the highest values 1.0 of the criterion $J(a_1)$, $J(a_2)$, …, $J(a_5)$. The X icon in the first five lines indicates the probabilities of implementing conditions, the values of which do not affect the success of attacks.

Lines 6 to 13 of Table 1 contain the conditions for conducting other attack scenarios with different effectiveness.

The maximum functional $J_{max}(A)$ will allow selecting A^* - the best (or bests) scenario of attack on a local network connected to the Internet.

Conclusions

The task of analyzing and selecting the best scenario of a cyberattack on an ICS is considered as a component of the task of analyzing the security of systems. A method and corresponding algorithm for selecting of the best scenario of attack on ICS using a logic and probability model is proposed. The model describes the development of adverse events that arise in the ICS from the implementation of possible attacks on the security system from cyberspace.

Analysis of cyber attack scenarios allows predicting the development of possible adverse cyber security events from the implementation of multiple threats to the system. The developed method and corresponding algorithm for analyzing attack scenarios can be used to analyze the security of ICS, as well as in automation systems for designing information security systems or designing attacks on such systems.

A computational experiment was conducted, the quantitative characteristics of the algorithm for selecting of the best scenario of attack on the Database Server of a local network connected to the Internet were obtained and analyzed. The analysis of the results confirmed the efficiency of the developed method and algorithm.

References

[1] Vipin Kumar, Jaideep Srivastava, Aleksandar Lazarevic (editors). Managing cyber threats: issues, approaches, and challenges. Springer Science+Business Media, Inc., 2005, 330 p. Access mode: https://link.springer.com/book/10.1007/b104908

[2] Rubio J.E., Román R., López J. Analysis of Cybersecurity Threatsin Industry 4.0: The Caseof Intrusion Detection; Proceedings of the CRITIS; Lucca, Italy. 8–13 October 2017. Access mode: https://www.researchgate.net/publication/327532675_Analysis_of_Cybersecurity_Threats_in_Industry_40

[3] Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, Manish Kumar. Review and in sighton the behavior aspects of cybersecurity. Cybersecurity, V. 3, No. 10, 2020. Access mode: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00050-w

[4] Konstantin M. Zuev, MichaelBeer, Reliability of Critical Infrastructure Networks: Challenges. Access mode: http://www.researchgate.net/publication/312043117

[5] Genge B., Kiss I., Haller P. A System Dynamics Approach for Assessing the Impact of Cyber Attacks on Critical Infrastructures. Int. J. Crit. Infrastruct. Prot. 2015;10:3–17.
Access mode: https://www.sciencedirect.com/science/article/abs/pii/S1874548215000244

[6] Syfert M., Kościelny J.M., Możaryn J., Ordys A., Wnuk P. Simulation Model and Scenarios for Testing Detectability of Cyberattacks in Industrial Control Systems. In: Kowalczuk Z., editor. Proceedings of the International Conference on Diagnostics of Processes and Systems DPS 2022; Chmielno, Poland. 5–7 September 2022; Cham, Switzerland: Springer International Publishing; 2023. pp. 73–84. Access mode: https://link.springer.com/chapter/10.1007/978-3-031-16159-97

[7] Sztyber-Betley, A., Syfert, M., Kościelny, J. M., & Górecka, Z. Controller Cyber-Attack Detectionand Isolation. Sensors (Basel, Switzerland), 223(5), 2778.
Access mode: https://doi.org/10.3390/s23052778

[8] Chris Salter, O. Sami Saydjari, Bruce Schneier, Jim Wallner, Toward a Secure System Engineering Methodology, Conference: Proceedings of the workshop on New security paradigms, 1998. Access mode:https://www.researchgate.net/publication/221067740_Toward_a_Secure_System_Engineering_Methodolgy

[9] Chee-Wooi Ten, Chen-Ching Liu, Manimaran Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. IEEE Conference: Power Engineering Society General Meeting, 2007. Access mode: https://www.researchgate.net/publication/224716761_Vulnerability_Assessment_of_Cybersecurity_for_SCADA_Systems_Using_Attack_Trees

[10] Qian Y. Information Assurance: Depend ability and Security in Networked Systems / Y. Qian, D. Tipper, P. Krishnamurthy, J. Joshi. – Morgan Kaufmann. – 2007. – 576 p. Access mode:https://www.researchgate.net/publication/216546027_Information_Assurance_Dependability_and_Security_in_Networked_Systems

[11] Jajodia S., Noel S., O'Berry B. Managing Cyber Threats: Issues, Approaches and Challenges, Chap. 5. Topological Analysis

of Network Attack Vulnerability, Kluwer Academic Publisher, 2003. Access mode: https://www.researchgate.net/publication/226860954_Topological_Analysis_of_Network_Attack_Vulnerability

[12] Jajodia S., Noel S., etal. Efficient Minimum-Cost Network Hardening Via Exploi Dependency Graphs. // In Proceedings of the 19th Annual Computer Security Applications Conference, LasVegas, NV, USA, December 2003. Access mode: https://www.researchgate.net/publication/221046627_Efficient_MinimumCost_Network_Hardening_Via_Exploit_Dependency_Graphs

[13] S. Noeland S. Jajodia, "Measuring Security Risk of Networks Using Attack Graphs," International Journal of Next Generation Computing, vol. 1, no. 1, 2010, pp. 135-147. Access mode: https://www.researchgate.net/publication/220202986_Measuring_Security_Risk_of_Networks_Using_Attack_Graphs

[14] Sheyner O. Automated Generation and Analysis of Attack Graphs / Sheyner O., Jha S., Wing J., Lippmann R., Haines J. // In 2002 IEEE Symposiumon Security and Privacy. – Oakland, California, - 2002.

[15] Sheyner O. Two Formal Analyses of Attack Graphs/Sheyner O., Jha S., Wing J. // IEEE Computer Security Foundations Workshop, CapeBrenton, Nova Scotia, Canada. – June 2002. – P. 49–63.

[16] Common Vulnerabilities and Exposures (CVE). Access mode: https://cve.mitre.org/

[17] Access mode: https://attack.mitre.org/

[18] National Institute of Standardsand Technology, “National Vulnerability Database, NVD”. Access mode: https://nvd.nist.gov/vuln-metrics.

[19] Ryabinin I.A. Logical-Probabilistic Calculus: A Tool for Studying the Reliability and Safety of Structurally Complex Systems. Automation and Remote Control vol. 64, 2003, P. 1177–1185; Access mode: https://link.Springer.com /article/ 10.1023/A:1024798521540#article-info

[20] CVSS “Common Vulnerability Scoring System (CVSS),” Forum of Incident Responseand Security Teams (FIRST). Access mode: http://www.f irst.org/cvss/

[21] Factor Analysis of Information Risk (FAIR). Access mode: https:// www.fairinstitute.org/

[22] S. Noeland S. Jajodia, "Managing attack graph complexity through visual hierarchical aggregation", In Proceedings of the ACM CCS Workshop on Visualization and Data Mining for Computer Security, October 2004, pp. 109-118. Access mode: https://doi.org/10.1145/1029208.1029225

[23] Jajodia, S., and Noel, S. “Topologica lvulnerability analysis,” In Cyber Situation al Awareness: Issuesand Research, Sushil Jajodia, Peng Liu, Vipin Swarup, Cliff Wang, eds., Springer, 2009, P. 139-154.

[24] S.Noel, S.Jajodia, B.O’Berry, M.l Jacobs. "Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs", Proceedings of the 27th Annual Computer Security Applications Conference, December 2011, P. 31–40. Access mode: https://doi.org/10.1145/2076732.2076738

[25] Novikov A., Rodionov A. The synthesis of information protection systems with optimal properties //Complexity and Security. NATO Science for Peace and Security Series – E. – 2008. – Volume 37. – pp. 307-316. Access mode: https://ebooks.iospress.nl/volume/complexity-and-security

[26] Novikov O.M, Rodionov A.M. Lohiko-ymovirnisna model zakhyshchenosti komponentiv informatsiino-komunikatsiinykh system. Informatsiini tekhnolohii ta kompiuterna inzheneriia, №1, 2008, pp. 170-175. Access mode: https://elibrary.ru/item.asp?id=22017530

[27] Martynenko L.P., Novikov O.M., Rodionov A.M. Syntez optymalnoi struktury systemy zakhystu informatsii z vykorystanniam lohiko-imovirnisnoho pidkhodu - Visnyk Vinnytskoho politekhnichnoho instytutu, 2009, pp. 51-57. Access mode: https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/697

[28] Hraivoronskyi M.V. Bezpeka informatsiino-komunikatsiinykh system / Hraivoronskyi M. V., Novikov O. M. - K.: BHV. – 2009. –p. 608. Access mode: https://ela.kpi.ua/handle/123456789/44867