UDC 004.725.7

DOI: 10.18372/2073-4751.70.16840

Balakin S.V.,
orcid.org/0000-0002-5102-1675,
Dolintse B.I.,
orcid.org/0000-0002-7529-4117

RISK ASSESSMENT IN COMPUTER NETWORKS INHERENT IN CRITICAL INFRASTRUCTURES

National Aviation University

bpys@i.ua

The development of global information systems creates a wide range of opportunities both for the development of various branches of human activity, and for the complication and improvement of methods of conducting cyber conflicts (disabling critical objects). In such an information space, the number of malicious programs and attacks on computer networks is rapidly growing. Antiviruses and firewalls handle the vast majority of them, but some attacks can bypass such protection, causing harm to the user or company. Most often, the existing protection is triggered with a delay, when the system has already been attacked and there has been a loss of data or control over certain network components.

Protecting critical information infrastructure is a key part of information security defense. The main goal of protecting critical infrastructure facilities is to reduce the risk of losing critical data and increase the confidentiality of information [1]. Also, an appropriate level of security of critical infrastructures allows you to identify the weakest nodes for malicious interference in an information system or telecommunications network for the purpose of additional monitoring and research. Cross Technologies, depending on their application, make it possible to organize multifactor system and data protection by means of mutual observation and search for anomalies in the actions of the network or user [2].

Key elements for securing critical information infrastructure include:

1. Collecting information about the customer's business processes.

2. Categorization of service objects of information systems, highlighting important processes.

3. Modeling of situations that threaten information systems, networks and control systems. Determination of directions of attack on important objects of information systems.

4. Elaboration and coordination of general requirements for the level of information protection.

5. Development of a technical design and a set of working documentation.

6. Updating the existing protection or performing debugging work when setting up a new line of defense for informatio systems.

7. Development of testing methods.

The most advanced security structures are mostly run by commercial rather than government-owned companies. In this case, in order to improve security, even government agencies need to interact as much as possible (transfer the protection of critical facilities) or adopt the best practices of private firms. Private companies have a comparatively better performance over the state ones, since free competition forces them to monitor the quality of their products all the time.

In some countries, protocols for the exchange of information and data have been introduced in order to distribute the work of maintaining security among the relevant structures. This distribution allows you to timely inform the necessary departments about the arrival of important updates or the presence of threats. Coordination of actions is also improved, which contributes to the efficient use of resources.

This model is implemented in Germany, where mechanisms for the distribution

of important data function at the state level, which are the basis for building systems for protecting important infrastructure facilities. Based on this technology, the interaction between the police and special services has been built through the appropriate information centers, which allow unifying and transmitting the necessary information to the necessary agencies [3]. This exchange is built only between government departments, but interaction with private companies has also been set up to establish an exchange of experience in combating intrusions (allowing share only non-critical data on the operation of government networks). Information exchange takes place through UP KRITIS and Alliance for Cyber Security [4]. The first company is responsible for security in the area of Critical Information Infrastructure Protection between private and public structures, focusing on the work of critical sectors. Alliance for Cyber Security is responsible for the area of computer security. For the interconnection of companies, meetings are held on current intrusions into computer networks [5].

Risk assessment helps to identify possible intrusions, their consequences and probability [6]. Risk analysis is an important part of crisis management. Depending on the scope of the company's activities, risk assessment can be carried out both on its own and with the involvement of private companies that specialize in working with critical infrastructures.

A typical example of a government risk assessment is Sweden, where an algorithm is used that identified 27 serious intrusions and developed 11 scenarios to counter the emerging risks.

Denmark does not adhere to a national risk assessment plan, allowing its departments to independently manage security, and a Cyber Threat Assessment Unit has been created for the interconnection of departments, through which communication and discussion of anti-intrusion plans and risk assessment for different industries takes place.

Switzerland is an example of decentralized risk management. Switzerland takes an approach that places great emphasis on individual responsibility. Sub-sectors independently manage intrusion and attack detection. Sub-industries are believed to have the best knowledge of how their systems work.

The Netherlands, where the National Manual on Decision-making in Crisis Situation is applied, is an example of a well-structured management of this type. With this approach, in the event of an intrusion, the control of the situation is transferred to the National Coordinator for Security and Counterterrorism, so qualified professionals are involved in solving the problem, who can quickly suppress unwanted activity. This structure allows accumulating the maximum possible information about intrusions in one department, which makes it possible to correctly respond to any incidents that arise.

For successful counteraction to crises, it is recommended to work together with outsourcing companies, then during an invasion, a specially created department (Bureau of Rapid Response) is engaged in its solution. This Bureau is formed as a public-private partnership that advises on intrusion handling. Thus, security is organized taking into account all the features of the operation of this system.

Communication between the power station and the control center can be one-way or two-way. One-way communication usually involves receiving data from the SCADA system, while two-way communication additionally involves sending commands back. Industrial controllers are often used as middleware to unify device protocols and relayed commands. This means that potential attackers must also compromise software and controller systems before any substations can be controlled.

Substation applications include visualization and simulation of distributed power systems, modal power balancing and production analysis, post-event analysis that can trigger a trip-close relay function, timing checks for substations, and flow analysis. One of the most widespread and frequently used tools are threshold meters for normal and abnormal user activity and system performance.

Features of intrusions of critical facilities:

- difficulties in ensuring the protection of interconnected critical infrastructure facilities;
- difficulties in ensuring the protection of network nodes that are not accountable to one command center;
- according to some characteristics, private information security companies can outperform and respond faster to threats than government ones;
- due to the rapid development of security systems, the number and complexity of new types of attacks is growing;
- the complexity of assessing the possible harm to the entire system, when the network nodes are out of order;
- imperfection of legal regulation of information warfare, which may not always qualify an attack on critical objects as an attacker.

At this stage, the user has little protection provided by the majority of antivirus companies, since it is often not timely (first, the virus spreads and only then the antiviruses are engaged in eliminating it), which is enough for an attacker to access the necessary information or damage the existing one. It is the timely notification of the system and the user that would help increase the efficiency of intrusion detection both on the local and on the Internet. When planning protection, it is important to calculate the degree of protection of each network node, which will make it possible to identify possible ways of attacking an intruder and build effective protection.

Criteria for the selection of critical objects

In the United States, the security of critical facilities that make up critical infrastructure is well-developed and includes:

- agricultural and food supply systems;
- financial and banking system;
- transport system;
- water supply system;
- rescue and ambulance services;
- power supply system;
- public administration system.

In the United States, it is customary to subdivide critical facilities into infrastructure facilities associated with international organizations (energy facilities, transport, banking and financial system, telecommunications) and unrelated (water supply, rescue services, government).

Based on the analysis of the views of the US leadership, three categories of critical facilities are identified:

Vital:

- Nuclear Plant;
- HPP (over 2 Gw);
- hydraulic structures;
- storage facilities for strategic oil and gas reserves;
- harmful chemical and petrochemical;
- warehouses for storing nuclear materials and ammunition.

Extremely important:

- power supply systems (more than 2 GW);
- subway;
- water supply lines;
- underground sewerage systems;
- main pipelines

Important:

- seaports;
- treatment facilities;
- large airports (more than 500 large airports and more than 14,000 small airports and sites;
- large communication centers;
- main pipelines.

There are 6 main categories of impact:

- destruction or damage;
- economic;
- damage to the environment;
- damage to national defense;
- symbolic;
- secondary problems of national security.

Each invasion scenario is rated on a five-point threat scale. With this approach, it becomes possible to miscalculate the risks associated with each type of threat, which will make it possible to effectively allocate

computing resources when planning the protection of network nodes. For example, if an invasion is possible with a probability of 0.5 (50/50), it can be determined that the chance of using a specific attack (for example, a Syn-flood attack on a computer network) is 75/25 – a probability of 0.75, the success of such an attack is assessed as successful 70/30, i.e. the probability is 0.3. The criterion for a successful attack can be the failure of 25 network nodes, and financial losses of up to 15 million euros. This risk is assessed by the formula:

$L_{tot} = (L_{hum} + L_{res}) \times P_a \times P_t \times P_s$,

where: L_{tot} – total loss; L_{hum} – human losses; L_{res} – loss of resources; P_a – probability of attack; P_t – probability of a certain type of attack; P_s – probability of a successful attack.

From the above data, it can be concluded that the potential damage will amount to the failure of 2.8 network nodes, and economic damage in the amount of 1.68 million euros.

With many intrusions into critical systems, a simplified hazard rating system can be used, for example, maximum threat level, medium or minimum. In these categories, threats will be easier to classify and handle.

The above risk assessment is well suited for multi-vector analysis of possible scenarios of attacks on key nodes of critical systems in order to identify the weakest or less reliable network elements. Also, this method is good for building a hierarchy of network elements, the failure of which can entail the greatest financial losses (which is especially important for banking structures, interruptions of which entail not only the loss of money, but also customers). This approach is also applicable to find effective solutions for the containment of air traffic [8].

Being able to calculate risk, it becomes possible to assess the effectiveness of protection, which can be made on the basis of an analysis of the corresponding risks and chances. Based on this approach, two types of estimates are possible. The first is an estimate for instantaneous values at which the state variable takes on a certain value.

The second is an integral estimate when the state variable belongs to a certain range of values.

The integral assessment of the state has a number of limitations, mainly related to the need to match the result to a certain range of predefined data, which is not al-ways possible to implement. The main diffi-culties can arise when calculating the possi-ble results and the adequacy of the likely responses to them (machine learning is not applicable here, since the threat of an inade-quate response to a threat or its omission will still remain, which is not acceptable for critical systems). Therefore, the most ap-propriate for assessing the effectiveness of protection will be the estimate for instanta-neous values, at which the state variable takes on a certain value. These estimates, to a certain extent, will have a predictive nature. This approach is often used in the statistical calculation of possible risks in the operation of closed automated systems [9].

In this case, it is necessary to assess the expected effectiveness based on the ratio of chance and risk:

$E_f(x_i) = \frac{\text{Chance}(x_i)}{\text{Risk}(x_i)} = \frac{v(x_i)[1-F(x_i)]}{u(x_i)(\Delta x)f(x_i)}$,

where, x_i – the value of the boundary threshold state on the interval (X_l, X_m); $v(x_i) = X_l\left(\frac{x_i}{X_l} - 1\right) - \lambda\left(\frac{x_i}{X_l} - 1\right)^2$ – damage when exceeding the boundary values of the point x_i, of crisis interval (X_l, X_m); $u(x_i) = \lambda\left(\frac{x_i}{X_l} - 1\right)$ – expected benefit from reaching extreme point values x_i, of crisis interval (X_l, X_m); X_l, X_m – safety thresholds within which the odds and risks are assessed; μ и β – parameters of the position and shape of the distribution curve.

Thus, the efficiency at the moment of reaching the critical valuex_i, will be:

$$E_f(x_i) = \frac{\overline{v}(x_i)(1-F(x_i))}{\overline{u}(x_i)(f(x_i)\Delta x)} = \frac{\beta(1-e^{-e^{\frac{\mu-x_i}{\beta}}})\overline{v}(x_i)}{(e^{\frac{\mu-x_i}{\beta}-e^{\frac{\overline{\mu}-\overline{x_i}}{\beta}}})\,\overline{u}(x_i)\Delta x)},$$

where Δx – critical state change step.

By calculating efficiency in this way, you can more efficiently allocate computing resources when building protection for

critical objects. The process of predicting the effectiveness of protection of an important object, in the context of ensuring protection of state variables, is shown in Figure 1.

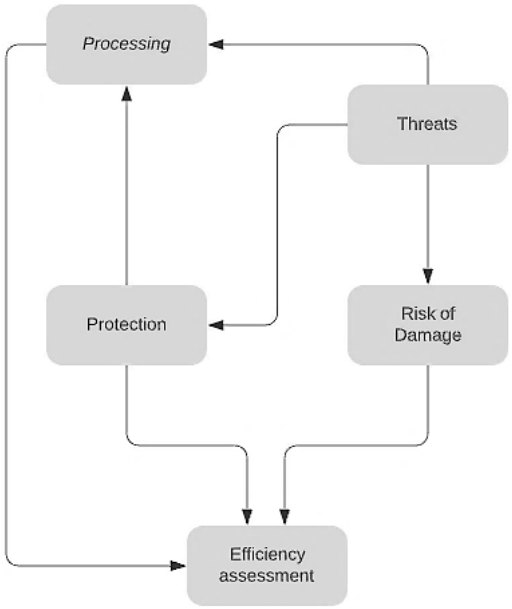

Fig. 1. The structure of the process of ensuring the safety of a critical facility

Conclusion

The stability of the social and economic development of the country and its security are directly dependent on the reliability and safety of the operation of critical facilities, therefore it is extremely important to investigate the possible risks arising from unforeseen situations or attacks by intruders. This paper provides an overview and comparison of methods for protecting critical objects in order to identify vulnerable nodes in the systems used. The basic tools for protecting critical objects and ensuring their performance during emergencies are considered. Identified main security threats in automated control systems and proposed methods for calculating their stability. The ways of assessing the effectiveness of protection, which can be made on the basis of the analysis of the corresponding risks and chances, are proposed.

References

1. *Sakrutina E.* Some Functions of the "Safety management system" in the Transportation Area Safety Assurance. Proceedings of 2017 International Siberian Conference on Control and Communications (SIBCON). – Astana, 2017. – P. 1-5.

2. *Zhukov I., Balakin S.* Detection of computer attacks using outliner method. Naukoviy zhurnal «Molodiy vcheniy». – Vol. 9(36). – 2016. – P. 91-93.

3. Federal Ministry of the Interrior, Building and Community, 2020. [Electronic resource]. – Access point: https://www.bmi.bund.de/EN/topics/security/security-node.html.

4. Kritis, 2020. [Electronic resource]. – Access point: http://www.kritis.bund.de/SubSites/Kritis/EN/Home/ home_node.html.

5. Federal office for information secirity, 2020. [Electronic resource]. – Access point: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

6. ENISA, 2020. [Electronic resource]. – Access point: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report.

7. *Zhukov I.* Implementation of integral telecommunication environment for harmonized air traffic control with scalable flight display systems. Aviation. – Vol. 14(4). – 2010. – P. 117-122.

8. *Zhukov I., Pechurin N., Kondratova L., Iavich M., Yerzhanov K.* Increasing the Accuracy of the Information Load Annual Growth Evaluation on the Internet of Things. The 1st International Conference on Cyber Hygiene & Conflict Management in Global Information Networks 2019 (CMiGIN-2019). – Vol. 2588. – P. 137-142.

Balakin S.V., Dolintse B.I.

RISK ASSESSMENT IN COMPUTER NETWORKS INHERENT IN CRITICAL INFRASTRUCTURES

This work is devoted to the problem of risk assessment in computer networks that are inherent in critical infrastructures. The work shows the place of the risk assessment process in

the global risk management process, as well as its goals, content and objectives. The most important infrastructure nodes and their interrelations are considered. The system of security indicators proposed for risk assessment in computer networks of critical infrastructures. Aspects of risk management of exceeding critical state variables of the threshold values of the crisis range for the object's information technology infrastructure are considered. The main research methods included structural and system analysis. The authors identified the main security threats in automated control systems, and also proposed methods for calculating their stability.

Keywords: *critical infrastructures, information security, risk assessment, critical important object.*

Балакін С.В., Долінце Б.І.

ОЦІНКА РИЗИКІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ, ЯКІ ПРИТАМАННІ КРИТИЧНИМ ІНФРАСТРУКТУРАМ

Дана робота присвячена проблемі оцінки ризиків у комп'ютерних мережах, які притаманні критичним інфраструктурам. У роботі показано місце оцінки ризиків у глобальному процесі управління ризиками, а також його цілі, зміст і завдання. Розглянуто найважливіші вузли інфраструктури та їх взаємозв'язки. Запропонована система індикаторів безпеки для оцінки ризиків у комп'ютерних мережах критичної інфраструктури. Розглянуто аспекти управління ризиками перевищення критичними змінними стану порогових значень кризового діапазону для інформаційно-технологічної інфраструктури об'єкта. Основними методами дослідження були структурний та системний аналіз. Авторами визначено основні загрози безпеці автоматизованих систем управління, а також запропоновано методи розрахунку їх стійкості.

Ключові слова*: критичні інфраструктури, інформаційна безпека, оцінка ризику, критично важливий об'єкт.*