Risk Assessment in Critical Infrastructure Computer Networks

Igor Zhukov[1], Tetiana Okhrimenko[1], Sergii Balakin[1], Olena Chaikovska[2], and Krzysztof Sulkowski[3]

[1]National Aviation University, 1 Lyubomyra Huzara ave., Kyiv, 03058, Ukraine
[2]Kyiv National University of Culture and Arts, 36 Yevgeny Konovaltsya str., Kyiv, 01601, Ukraine
[3]University of Applied Sciences in Nowy Sącz, 1 Staszica str., Nowy Sącz, 33–300, Poland

Abstract

Risk assessment is an important domain of computer network security in critical and other infrastructures. There are many approaches to risk analysis and assessment that can be implemented in critical infrastructure. 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 identification; risk assessment; critical important object; indicator; information system; crisis management; attacks

1. Introduction

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 conducting cyber conflict methods (disabling critical objects) [1, 2]. 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 [3, 4].

Critical information infrastructure protection 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 information confidentiality [5]. Also, an appropriate level of critical infrastructure protection allows for identifying the weakest nodes for malicious interference in an information system or telecommunications network for additional monitoring and research. Cross Technologies, depending on their application, make it possible to organize multifactor systems and data protection using mutual observation and search for anomalies in the actions of the network or user [6].

Key elements for critical information infrastructure protection 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

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: zhukov.ihor@sfk.nau.edu.ua (I. Zhukov); taniazhm@gmail.com (T. Okhrimenko); balakin@gmail.com (S. Balakin); chaikovska_o@i.ua (O. Chaikovska); k.sulkowski@ckz-ns.edu.pl (K. Sulkowski)
ORCID: 0000-0002-9785-0233 (I. Zhukov); 0000-0001-9036-6556 (T. Okhrimenko); 0000-0002-5102-1675 (S. Balakin); 0000-0001-7769-1004 (O. Chaikovska); 0009-0002-5523-5010 (K. Sulkowski)

systems. Determination of attack directions on important information system objects.

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 information systems.
7. Testing methods development.

1.1. Partnerships with Private Companies

The most advanced security structures are mostly run by commercial rather than government-owned companies. In this case, 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.

1.2. Information Exchange Schemes

In some countries, protocols for the exchange of information and data have been introduced to distribute the work of maintaining security among the relevant structures. This distribution allows us to timely inform the necessary departments about the arrival of important updates or the presence of the threat. 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 [7]. 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 sharing only non-critical data on the operation of government networks). Information exchange takes place through UP KRITIS and Alliance for Cyber Security [8]. 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 [9–14].

*The paper aim*s to review and comparison of critical object protection methods to identify vulnerable nodes in the used systems.

2. Papers Review

2.1. Risk Assessment

Risk assessment helps to identify possible intrusions, their consequences, and their probability [15]. 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 take 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.

2.2. Crisis Management

Dealing with information security crises is about assigning responsibilities to each node in the network. Coordination and decision-making algorithms allow generalizing the experience gained by one node to the entire hierarchy. Crisis

management must be coordinated with all elements of the crisis management network [16].

The Netherlands, where the National Manual on Decision-making in Crisis Situations is applied, is an example of 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.

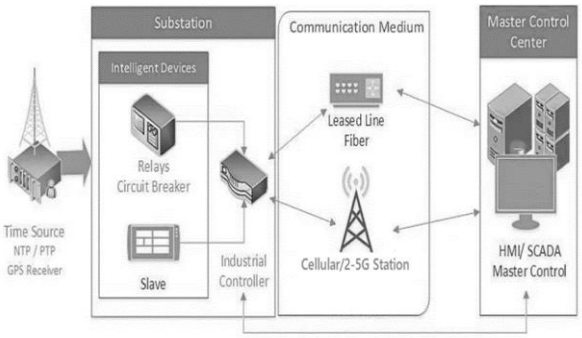

Figure 1: Functional architecture for an attack scenario

Fig. 1 shows the functional architecture on which most of the attacks are based. Also, potential risks depend on the type of systems and their implementation. The dependence of the electric power industry on telecommunications differs depending on the technologies used, the subjects involved, and the settings of the devices included in the system [17].

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 is threshold meters for normal and abnormal user activity and system performance [11, 12, 18].

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.
- The imperfection of legal regulation of information warfare, 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 locally 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.

2.3. 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, financial system, communications) and unrelated ones (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 chemicals 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.
- Trunk structures (in the United States there are about 7 million km of roads, of which more than 80,000 trunks, and more than 600,000 bridges. The length of the railways is about 550,000 km.
- Large airports (more than 500 large airports and more than 14,000 small airports and sites.
- Large communication centers'.
- Main pipelines.

2.4. Risk Identification

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 Synflood 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:

$$L_{tot} = (L_{hum} + L_{res}) \times P_a \times P_t \times P_s \quad (1)$$

where: L_{tot} is a total loss; L_{hum} is human losses; L_{res} is loss of resources; P_a is the probability of attack; P_t is the probability of a certain type of attack; P_s is the 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 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 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 finding effective solutions for the containment of air traffic [19].

Also, it is important not to allow exceeding the threshold values of the crisis range for a critical facility.

Being able to calculate risk, it becomes possible to assess the effectiveness of protection, which can be made based on 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 several limitations, mainly related to the need to match the result to a certain range of predefined data, which is not always possible to implement. The main difficulties can arise when calculating the possible results and the adequacy of the likely responses to them (machine learning is not applicable here, since the threat of an inadequate response to a threat or its omission will remain, which is not acceptable for critical systems). Therefore, the most appropriate for assessing the effectiveness of protection will be the estimate for instantaneous 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 [20, 21].

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

$$E_f(x_i) = \frac{Chance(x_i)}{Risk(x_i)} = \frac{v(x_i)[1-F(x_i)]}{u(x_i)(\Delta x)f(x_i)}, \qquad (2)$$

where, x_i is the value of the boundary threshold state on the interval (X_l, X_m);

$v(x_i) = X_l\left(\frac{x_i}{X_l} - 1\right) - \lambda\left(\frac{x_i}{X_l} - 1\right)^2$ is damaged when exceeding the boundary values of the point x_i, of crisis interval (X_l, X_m);

$u(x_i) = \lambda\left(\frac{x_i}{X_l} - 1\right)$ is expected benefit from reaching extreme point values x_i, of crisis interval (X_l, X_m); X_l, X_m are safety thresholds within which the odds and risks are assessed; μ and β are parameters of the position and shape of the distribution curve.

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

$$E_f(x_i) = \frac{\underline{v}(x_i)(1-F(x_i))}{\underline{u}(x_i)(f(x_i)\Delta x)} = \frac{\beta(1-e^{-e^{\frac{\mu-x_i}{\beta}}})\underline{v}(x_i)}{(e^{\frac{\mu-x_i}{\beta}-e^{\frac{\mu-x_i}{\beta}}})\underline{u}(x_i)\Delta x}, \qquad (3)$$

where Δx is critical state change step.

By calculating efficiency in this way, can be 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 Fig. 2.

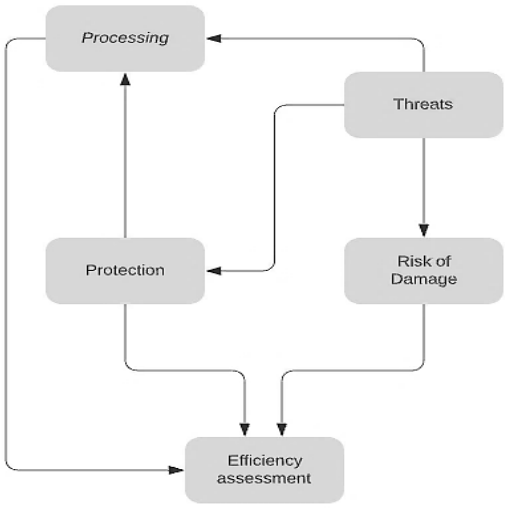

Figure 2: The structure of the process of ensuring the safety of a critical facility

3. Conclusions

The stability of the social and economic development of the country and its security is 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 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 based on the analysis of the corresponding risks and chances, are proposed.

4. References

[1] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[2] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in

Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.
[3] TajDini, M., Sokolov V., Buriachok V. (2019). Men-in-the-middle attack simulation on low energy wireless devices using software define radio. Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 287–296.
[4] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.
[5] E. Sakrutina, Some Functions of the "Safety management system" in the Transportation Area Safety Assurance, 2017 International Siberian Conference on Control and Communications (SIBCON), Astana, Kazakhstan, 2017, 1–5. doi:10.1109/SIBCON.2017.7998576
[6] I. Zhukov, S. Balakin, Detection of Computer Attacks Using Outliner Method, Sci. J. Young Sci. 9(36) (2016) 91–93.
[7] Building and Community, Federal Ministry of the Interrior, 2020.
[8] Kritis, URL: http://www.kritis.bund.de/SubSites/Kritis/EN/Home/ home_node.html
[9] Federal Office for Information Security, 2020. URL: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html
[10] ENISA, 2020. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report
[11] ENISA, 2020. URL: https://www.enisa.europa.eu/publications/ccc-study
[12] ENISA, 2020. URL:https://www.enisa.europa.eu/publications/power-sector-dependency
[13] K. Scarfone, P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP, 2007, 800–94. doi:10.6028/NIST.SP.800-94
[14] M.A. Hadidi, et. al., Methods of Risk Assessment for Information Security Management, Int. Rev. Computs. Softw. 11(2) (2016) 81–91. doi:10.15866/IRECOS.V11I2.8233
[15] I. Zhukov, Implementation of Integral Telecommunication Environment for Harmonized Air Traffic Control with Scalable Flight Display System's, Aviat. 14(4) (2010) 117–122. doi:10.3846/AVIATION.2010.18
[16] I. Zhukov, et. al., 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), 2588 (2019) 137–142.
[17] L. Sakovych, et. al., Study on Complex Assessment of the Information and Communication Systems Efficiency, CEUR Workshop Proceedings, (2020) 680–691.
[18] Z. Avkurova, S. Gnatyuk, B. Abduraimova, Structural and Analytical Models for Early APT-Attacks Detection in Critical Infrastructure, ICTERI 2021 Workshops, Commun. Comput. Inf. Sc. 1635 (2022). doi:10.1007/978-3-031-14841-5_30
[19] S. Gnatyuk, et. al., Method for Calculating the Criticality Level of Sectoral Information and Telecommunication Systems, CEUR Workshop Proceedings, 3347 (2022) 234–245.
[20] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meet. Secur. Challs. Thr. Data Anal. Deci. Support, IOS Press Ebooks, 47(3) (2016) 308–316.
[21] R. Berdibayev, et al. Studies on cloud-based cyber incidents detection and identification in critical infrastructure, CEUR Workshop Proceedings 2923 (2021) 68–80.