METHODS OF MEASURING THE RESILIENCE OF CYBER SECURITY SYSTEMS AT CRITICAL INFRASTRUCTURE FACILITIES

Nazar Zaika [1], Oleg Drobotun [2], Maksym Komarov [1], Oleksii Hlushchenko [2]

1. G.E. Pukhov Institute for Modelling in Energy Engineering
National Academy of Sciences of Ukraine,
Generala Naumov St., building 15, Kyiv, Ukraine, 03164
2. State Research Institute of Cyber Security and Information Protection Technologies,
M. Zaliznyaka Street, building 3, bloc 6, Kyiv, 03142
nazar2611@gmail.com

Abstract: Conducting an audit and analysis of the possible consequences of attacks or destructive disturbances to the state of the cyber security system of critical infrastructure objects. Development of methods for analyzing possible threats and security system reactions to them. Ensuring resilience in security systems of critical infrastructure facilities.

Keywords: attacks, system resilience, system security, cyber security

Cybersecurity of critical infrastructure objects

Today, cybercriminals are finding new ways to profit from enterprises that are the object of extortion and a profitable source of income for organized criminal groups through private information stored and processed by critical infrastructure (CII). Various types of cyber threats are a powerful tool used by cybercriminals to commit malicious acts.

In addition, it is very important to ensure stable functioning under attacks. One of the ways to solve this problem is to build resilient systems that can quickly recover and continue to function in the face of attacks.

The analysis of literary sources allows us to conclude that the majority of studies are devoted to individual principles of the resilience of the security system of OKI, but there are practically no works that consider their simultaneous combination to ensure a synergistic effect. The analysis shows that the known approaches that implement certain properties of resilience do not take into account the principles of rational resilience, which is relevant in conditions of limited resources.

Rational resilience in this context expands the concept of guarantee capability of technical systems, emphasizing the need to create systems that are flexible and adaptive [1]. Cybersecurity specialists formulate resilience as the ability to anticipate, resist, recover and adapt to adverse conditions, external influences, attacks or disruption of the normal functioning of the security system [2].

Other researchers formulate resilience as the ability of a system to maintain functionality and recover from losses caused by extreme events and destructive disturbances.

Planning and preparation

At the stage of planning and preparation for destructive disturbances, a resilient system can perform the following actions:

- risk assessment by performing system analysis and simulation of destructive disturbances;
- implementation of methods of detecting destructive disturbances;
- elimination of known vulnerabilities and implementation of a number of measures to protect the system from destructive disturbances;
- provision of appropriate backup and recovery strategies.

Thus, resilience is a concept of guarantee ability that focuses on studying the impact of changes on system reliability. The concept of resilient systems consists in the implementation of mechanisms of preparation, absorption, recovery and adaptation to ensure stable provision of services in a reliable manner under conditions of internal and external changes and influences.

Warranty is one of the main requirements that applies to computer systems. It can be defined as the system's ability to provide services that can be trusted [3]. Warrantability is an integrated concept that includes such key attributes as:

- availability: the ability of the system to provide a service at any time;
- reliability: the ability of the system to provide a service within a specified period of time;
- functional safety (safety): the ability of the system to provide services under specified conditions without catastrophic consequences for users and the external environment;
- integrity: absence of improper changes to the system;
- maintainability: the ability of the system to be restored to a state in which it can properly provide services;
- confidentiality: absence of unauthorized disclosure of information.

Destructive factors

In general, cyber security systems operate in non-ideal conditions and may be exposed to various destructive factors. Destructive factors can affect both the deployment computing environment and data in the accounting and information storage subsystems [4].

Destructive influences can be malicious, or they can be natural in nature. Destructive influences include the following factors:

- hardware malfunctions;
- noise and competitive attacks;
- concept drift;
- novelty in test data;
- omissions and errors in the data.

Hardware malfunctions (Faults) in the computing system generate errors (Errors). An error is considered to be such a manifestation of a malfunction in the system, which leads to a deviation of the current state of the system element from the expected one [38]. Failures occur as a result of errors, that is, the state of the system's inability to perform its intended functionality or behavior.

Traditionally, threats are classified into the following categories: failures, errors, and defects, and the development of warranty-capable systems is based on four main approaches: fault prevention, fault removal, fault forecasting, and fault tolerance.

Malfunctions, in turn, can be classified by their time characteristics of changes. Change is a broad term that can be viewed differently in different fields. Changes can be systematized according to their nature, perspective and time [5]:

- nature: functional, infrastructural or technological;
- perspective: foreseeable and unforeseen changes;
- time: instantaneous (less than a second), short-term (e.g. seconds to hours), medium-term (e.g. hours to months) and long-term changes (e.g. months to years).

There are several physical methods of injecting malicious faults. In practice, fault injection is implemented due to the failure of the system counter, i.e., the synchronization of circuits, power failure to a certain level, electromagnetic influence on semiconductors, the influence of a laser beam on memory, as well as software attacks on memory bits.

The target of attacks

The target of attacks can be OKI security subsystems, data storage environment. According to the purpose of the attack, it can be divided into three main types:

– an attack on availability, which leads to the unusability of using the services by the end user;

– an integrity attack that leads to the incorrect classification of an incoming observation (a targeted integrity attack forces a specific incorrect decision to be made - to provide another service or to block the provision of services);

– a privacy attack, where the attacker's goal is to intercept communication between two parties and obtain private information.

According to the attack strategy, it can be classified into: evasion attacks and poisoning attacks [6]. Evasion attacks are attacks on the system in its decision-making mode, that is, it is a search attack aimed at confusing the cybersecurity subsystem. This attack involves an optimization process of finding a small perturbation that will cause an incorrect decision. According to the frequency of updating and optimization of competitive samples, they are divided into one-shot attacks and iterative attacks. Poisoning attacks are the corruption of data in a security subsystem to impair the effectiveness of cyber security.

Regarding the data analysis model, the attack can be classified into:

– white-box attacks, for the formation of which the attacker has full knowledge of the data, model and attack algorithm. This method can most likely be used by the system developer himself to check data protection and evaluate the effectiveness of the security system;

– gray-box attacks, for the formation of which the attacker has partial information, but sufficient to attack the system;

– black-box attacks, for the formation of which the attacker has an understanding of the data at the input and output of the cybersecurity subsystem [7].

As a result of the influence of threats, the information and technical state of the computer system changes, when either the integrity of the information is violated, or the external environment (another system) gains unauthorized access to it.

The principles of the resilience of the OKI

The concept of the resilience of the OKI in the conditions of cyber attacks is based on the principles [8]:

- proactiveness (proactivity);
- adaptability (adaptability);
- resistance to interventions (resistance);
- diversity (diversity);
- elasticity (plasticity);
- controlled degradation (controlled degradation);
- defense in depth (defense in depth);
- ability to evolve (evaluability).

A significant part of information security is based on proactivity, adaptability and resistance to system interventions during attacks. If the system is properly protected, the level of risk is reduced and thus the probability of a loss event is also reduced. If an unknown attack occurs, a properly hardened system will be more resistant to the actions of an attacker (attacker) who infiltrated or compromised the system.

Similarly, it is possible to resist the attacker's actions by making the task of attacking the system more difficult. The diversity of system components and their construction (for example, operating system, programming language, access channel) requires the attacker to formulate several attack strategies. Modularity in the system allows configuration and replacement of components without requiring changes in the interface between them, thereby providing greater diversity. Diversity typically creates a level of overhead for administrators and may not be appropriate for all situations, but is feasible and justified in today's complex systems.

Elasticity and controlled degradation allow the system to reduce performance without total destruction. Concepts such as redundant components, excess processing or communication capacity, and avoiding single points of failure are common ways to allow a system to absorb unexpected events while still providing at least a minimally acceptable level of service. Controlled degradation is the concept that a system can be pre-configured with a set of progressively less functional states that represent acceptable trade-offs between continued functionality and ensuring safety parameters.

Defense in depth (defense in depth) is an approach to ensuring the resilience of the OKI cyber security system in the face of attacks, in which a number of defense mechanisms are combined to protect valuable data and information. If one mechanism fails to provide protection, another is engaged to prevent the attack. This approach increases the security of the system as a whole and addresses many different attack vectors. Mitigating the effects of the attack relies on excessive channel redundancy, the use of filtering services to detect and block unwanted responses from cyber security subsystems, and the use of additional routing to redirect all incoming traffic through the external network, to check incoming traffic, all unwanted responses from subsystems are detected and blocked.

To ensure the resilient functioning of the cyber security system in conditions of attacks, the system should [9]:

- be prepared for possible attacks (be prepared);
- be protected (be protected);
- have the ability to detect attacks (able to detect attacks);
- have the ability to resist attacks (able to respond / adsorb attacks);
- be adaptable (be adaptable);
- be recoverable.

Analytical methods

The ingenuity of the system lies in the ability to diagnose problems, set priorities and initiate solutions to problems by identifying and mobilizing material, monetary, informational, technological and human resources. In theory, if infinite resources were available, the recovery time would approach zero. In practice, even with huge financial and labor opportunities, there is some minimum recovery time. However, recovery times can be quite high even with large resources due to inadequate planning, organizational failures, or ineffective policies.

Analytical, simulation and test methods can be used to evaluate and certify system resilience indicators. Analytical methods require decomposition of the system and aspects of its functioning, in-depth analysis of its structure and elements to obtain an analytical expression of resilience. Many complex systems are very difficult or impossible to describe analytically, or existing analytical models do not allow obtaining a stable solution, so they require an accessible prototype of the system, and can be carried out according to the principles of transparent or black box. In many cases, testing a real type of system is either dangerous or very expensive. Therefore, the effectiveness of all resilience assessment methods depends on the application area, on the specifics of the system itself. An audit is conducted to study the system.

The principle of taking into account changes is a continuation of the principle of development (historicity, or openness) of systems during system analysis procedures. In addition to the need to take into account system changes during development, evolution, adaptation, replacement of components or expansion of the system, attention needs to be paid to changing the parameters of the external environment [10].

The Cyber Security Evaluation Tool

During the life cycle of a cyber security system, changes are possible to subsystems or its components, as well as to the environments in which the system is designed, developed, tested, and operated [11].

The following software tool is offered for conducting a cyber security audit of OKI in Ukraine:

The Cyber Security Evaluation Tool (CSET®) is a software tool for conducting cyber security evaluations of enterprise and industrial management cyber systems. The Cybersecurity Assessment Tool is a product of the Cybersecurity & Infrastructure Security Agency (CISA) that helps organizations protect their key national cyber assets [12].

CSET was designed to help asset owners identify vulnerabilities and improve an organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements and best practices. The requirements questionnaires presented are based on selected industry standards, general requirements, and network design (or network topology and architecture). CSET includes both general and detailed questions related to all industrial control systems and IT systems.

Recommendations

Recommendations for increasing system resilience in the face of cyber threats:

- Planning / preparation (goal #1: anticipate the attack). Implementation of protection and monitoring methods for timely detection of a possible attack, provision of alternative data processing and communication capabilities. For the purpose of early detection of the attacker's actions in preparation for the attack and study of the object of the attack.
- Defense (goal #2: prevent attack). Application of system security methods in order to limit the consequences of attacks, to minimize the probability that an attack can be successful. Assessment of system security, taking into account the implementation of an attack, or attempts to identify vulnerabilities to penetrate the security system.
- Detection (goal #3: identify the attack). Development and implementation of measures to quickly detect an attack and ensure a timely response. Continue monitoring the system for other signs related to this attack, checking the security system, in order to evaluate the effectiveness of protection methods.
- Absorption / response (goal #4: counter attack). Application of notification/coordination methods and mechanisms to resist attacks (configuration, update, reallocation of resources, isolation, failover), as well as ensuring separation of critical data from non-critical data. Support of the minimum necessary productivity for the provision of services and services by the system. Determination of actions to maintain control over the system and isolation of its important resources in case of confirmation of penetration into the system, or presence in the attacked system with full or partial control over the system.
- Recovery (goal #5: restore the system). Applying actions to restore the system after an attack by returning the system to its initial state. Definition of communications and data processing methods for monitoring the state of the security system. Determination of criteria and compromises for redistribution of resources and system functionality. Analysis of costs and recovery.
- Adaptation (goal #6: develop the system). Changing the system structure, developing and applying new security scenarios, re-designing system components, developing system modularity. Preparing the system for new attacks.

Conclusions. The concept of resilience is based on fairly general ideas and principles and can be developed for complex systems of various types, taking into account the specifics of threats and protection opportunities inherent in them.

The development of resilient systems must necessarily include the ability to evolve them in such a way as to take into account the experience of previous attacks and to be

able to make the necessary structural, architectural or other changes to the system that will reduce vulnerability and increase resistance to potential future attacks.

In recent years, issues of comprehensive provision of indicators for guaranteeing the normal functioning of cyber security systems, which were previously separated into different disciplines, have become topical. Cyber-incidents in the field of energy supply of Ukraine, the analysis of which is given in the projects of the American NIST standards, infrastructure breaches, etc.

1. Development of the construction of reliable security systems from unreliable (from the point of view of functional and cyber security) components.

2. The use of security subsystems as intended in the conditions of changing requirements, changing environmental parameters, occurrence of failures due to physical and design defects and vulnerabilities, requires updating and restoring the system, and giving it resilience properties.

3. Use of multi-purpose service using strategies combined for different properties supported by service (reliability, functional security, cyber security).

Resilience expands the concept of resiliency, emphasizing the need to create systems that are flexible and adaptive. It requires the implementation of advanced mechanisms and flexible strategies to cope with attacks and destructive disturbances.

Reference list

1. Yu. L. Ponochovnyy Methodology of guaranteeing information management systems using multi-purpose service strategies / Yu. L. Ponochovnyi, V. S. Kharchenko // Radioelectronic and Computer Systems. 2020. No. 3. P. 43–58. DOI: https://doi.org/10.32620/reks.2020.3.05.

2. Resilience of computer systems in the face of cyber threats: taxonomy and ontology / S. M. Lysenko [et al.] // Radioelectronic and Computer Systems. 2020. – No. 1. – P. 17–28. - DOI: https://doi.org/10.32620/reks.2020.1.02.

3. Haimes Y. Y. On the Definition of Resilience in Systems / Yacov Y. Haimes // Risk Analysis. - 2009. - Vol. 29, no. 4. – P. 498–501. DOI: https://doi.org/10.1111/j.1539-6924.2009.01216.x.

4. Cimellaro G. P. Framework for analytical quantification of disaster resilience / G. Paolo Cimellaro, A. M. Reinhorn, M. Bruneau // Engineering Structures. 2010. Vol. 32, no. 11. P. 3639–3649. DOI: https://doi.org/10.1016/j.engstruct.2010.08.008

5. Yodo N. Engineering Resilience Quantification and System Design Implications: A Literature Survey / Nita Yodo, Pingfeng Wang // Journal of Mechanical Design. 2016. Vol. 138, no. 11. DOI: https://doi.org/10.1115/1.4034223.

6. Review of Artificial Intelligence Adversarial Attack and Defense Technologies / Shilin Qiu [et al.] // Applied Sciences. 2019. Vol. 9, no. 5. P. 909. DOI: https://doi.org/10.3390/app9050909.

7. Efficient Decision-Based Black-Box Adversarial Attacks on Face Recognition / Yinpeng Dong [et al.] // 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA. 2019. DOI: https://doi.org/10.1109/cvpr.2019.00790.

8. Procedural Noise Adversarial Examples for Black-Box Attacks on Deep Convolutional Networks / Kenneth T. Co [et al.] // CCS '19: 2019 ACM SIGSAC

Conference on Computer and Communications Security, London United Kingdom. New York, NY, USA, 2019. DOI: https://doi.org/10.1145/3319535.3345660.

9. Moskalenko V.V. Development of models and methods for measuring and certifying the resilience of artificial intelligence systems for the protection of cyber-physical systems. UDC 002.6, 002.001; 002:001.8. 2022. Amounts. 117 p.

10. Geida, A. and Lysenko, I. Operational Properties of Agile Systems And Their Functioning Investigation Problems: Conceptual Aspects. Applied Informatics, vol. 5 (71), 2017, pp. 93-106.

11. Ponochevny Yu. L., Kharchenko V. S. Methodology for ensuring the guarantee capacity of information management systems using multi-purpose maintenance strategies. Modeling and development of warranty systems. 2020. DOI: 10.32620/reks.2020.3.05

12. The Cyber Security Evaluation Tool (CSET®). https://csirt.csi.cip.gov.ua/uk/pages/cset