System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure

Igor Skiter[1], Hennadii Hulak[2], Viktor Grechaninov[2], Vitalii Klymenko[2], and Nikolay Ievlev[2]

[1] *Institute for Safety Problems of Nuclear Power Plants of the National Academy of Sciences of Ukraine, 36a Kirov str., 07270, Chernobyl, Ukraine*
[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680, Kyiv, Ukraine*

Abstract

The tasks of creating secure reliable cybersecurity centers to protect critical infrastructure objects, taking into account their industry specifics, are formulated. The proposed systematic approach to the creation of industry centers of cybersecurity (ICCSs), aimed at defining the main tasks and functions of the center. The basic principles of ICCSs CIO implementation are formed. The CIF Information Infrastructure at several hierarchical levels with different degrees of information aggregation is presented. A three-level hierarchical model of information system security policy is described. A systematic approach to the creation of ICCS will prevent interference in CIO information systems.

Keywords

Industry center of cyber security, systems approach, critical infrastructure object, information security

1. Introduction

From the point of view of systems analysis, critical infrastructure facilities (CIFs) are complex systems of structural type [1]. They circulate a large number of disparate information flows. Accidental or malicious influence on information flows is a potential source of danger for CIFs. Minimization of such actions can be provided by creation of automated control systems of technical means of such objects Therefore, the priority tasks of scientific research in the field of cybersecurity of CIF are, firstly, the creation of a model of cybersecurity centers and, secondly, ensuring the warranty of automated CIF systems as a technological basis for their operation.

The creation of industrial cybersecurity centers for objects of critical infrastructure is due to the following problems:

- uncertainty of ways to implement cyberattacks;
- algorithmic complexity of realization of some cybersecurity functions;
- the need for coordinated operation of disparate subsystems and elements of ICCS;
- limited time for processing a significant amount of information about cyber incidents and deciding on the tactics of cyber security, etc.

In these circumstances, a clear definition of the exhaustive list of tasks and functions of ICCS and the provision of their information resources is crucial for the guaranteed cyber protection of CIFs and their normal functioning. It should be noted that the reliable implementation of certain tasks of ICCSs must take place in difficult conditions. Namely - in the event of accidental failures and failures of hardware and software platforms, intentional or natural influences on the hardware of information

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: skiteris@ukr.net (I. Skiter); h.hulak@ukr.net (H. Hulak); vgrechaninov@gmail.com (V. Grechaninov); vklimenko@immsp.kiev.ua (V. Klymenko); ievlev@immsp.kiev.ua (N. Ievlev)
ORCID: 0000-0003-2334-2276 (I. Skiter); 0000-0001-9131-9233 (H. Hulak); 0000-0001-6268-3204 (V. Grechaninov); 0000-0001-6951-4091 (V. Klymenko); 0000-0002-9364-9495 (N. Ievlev)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3187/short3.pdf

processing, etc. That is, due to external and internal influences, which can significantly reduce management efficiency and even blocked decision-making processes at the CIF.

Thus, the task is to build a guarantly-protected ICCS to protect the CIF, taking into account their industry specifics. It is the creation of automated systems for managing information flows, ensuring their integrity and counteracting internal and external influences that should ensure the cybersecurity of the CIF of a certain branch of social production, law enforcement agencies, the national security and defense sector, etc. In the future, the subjects of ensuring the sustainability, reliability and efficiency of information and technical and technological systems of the CIF industry centers of cyber security CIF should be connected by a secure telecommunications network, including the main and backup government centers of cyber security CIF.

2. System Approach to Cybersecurity Management of the Critical Infrastructure Facilities

Structurally, CIFs include a large number of elements and subsystems with their own local tasks, which ensure the implementation of the main technological tasks of the object. The existence of links between elements and subsystems, their mutual influence leads to the need to assess and monitor their condition. From the point of view of information security such tasks will allow to solve the uniform automated systems of management of information security. A systematic approach to the creation of sectoral cybersecurity centers (ICCSs) should be aimed at defining the main tasks and functions of the center namely:

- creation and implementation of information security model;
- formation of requirements and parameters of CIF information systems taking into account the specifics of industries;
- formation of information security culture at CIF;
- technical measures aimed at assessing the level of vulnerabilities and their minimization in CIF information systems.

The functioning of the center in addition to coordinating and controlling functions should provide interaction with the information and technological subsystems of the industry.

The main functions of the center should be:

- identification of threats and vulnerabilities in CIF information systems;
- identification of cyberattacks and counteraction to them;
- conducting training of personnel on information security;
- reduction of information risks;
- carrying out security measures.

Ensuring the functioning of complex systems of structural type - critical infrastructure objects - in terms of information security is defined in international [2], [3], [4], [5] and domestic regulations and standards [6] - [8].

The tasks of monitoring information flows, their analysis and synthesis of management decisions taking into account external and internal factors can be solved on the basis of an automated information security management system of CIF. The issue of distribution and ranking of cybersecurity assessment tasks for different levels of protection of distributed information systems is presented in [9]. The complex model of interaction of elements of CIF on an example of objects of nuclear power [1] - branch of CIF - describes interaction of system of protection of the information with external and internal factors (threats) (Fig. 1).

In [9], two groups of subjects of cyber threats for CIF information systems are identified - external and internal. The main threat to information systems is external factors. Accordingly, CIF cybersecurity systems should have basic functions: network protection of systems and subsystems; security monitoring, audit and management, data protection and storage; protection and software updates.

Therefore, in terms of system analysis, the information security management system (cybersecurity) CIF is a comprehensive organizational and technical system. The functions of the system are: analysis of the state, control, monitoring, security of individual functional elements and processes, and the system as a whole.

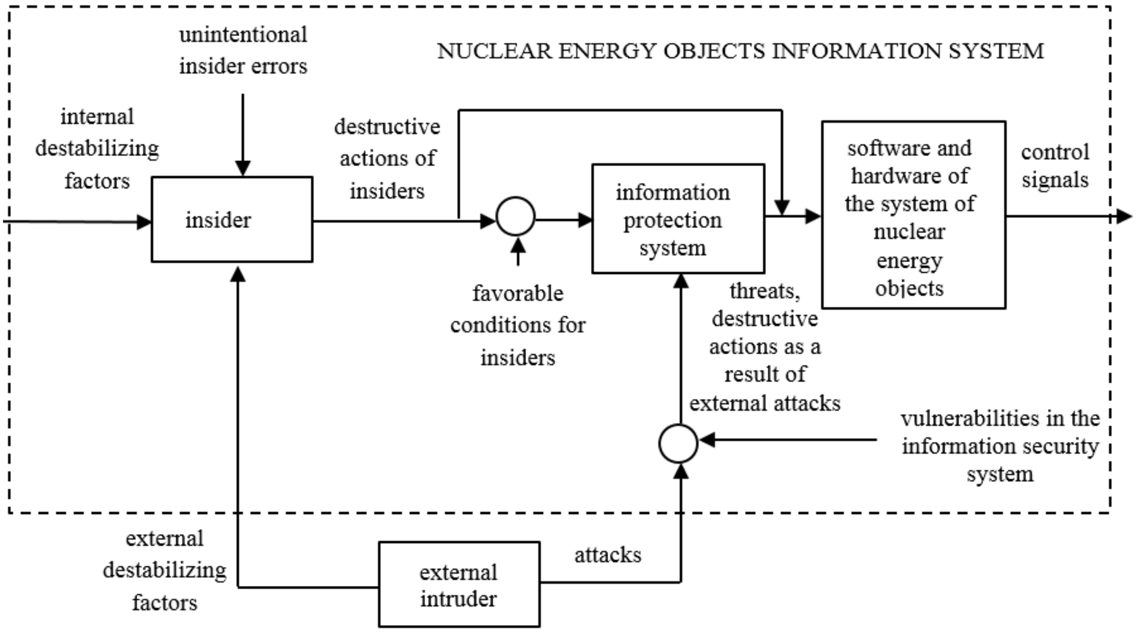
NUCLEAR ENERGY OBJECTS INFORMATION SYSTEM
unintentional insider errors
internal destabilizing factors
insider
destructive actions of insiders
favorable conditions for insiders
information protection system
threats, destructive actions as a result of external attacks
software and hardware of the system of nuclear energy objects
control signals
vulnerabilities in the information security system
external destabilizing factors
external intruder
attacks

Figure 1: The Model of interaction of elements of the CIF information system on the example of a nuclear energy facility [1]

The CIF cybersecurity management system should provide:

- stable, durable and safe operation of facilities;
- environmental safety;
- protection of the interests of the individual, society and the state, as well as consumers of services.

The CIF cyber security management system is a comprehensive organizational and technical system that performs the functions of condition analysis, control, monitoring and security of functional elements, subsystems and processes.

Thus, at the system level, the task is to minimize the risks and threats to information security of the CIF. It can be implemented through optimal management and targeted impact on the characteristics of the object. Optimal management is achieved by monitoring, analyzing and controlling the parameters that characterize the managed object.

3. The System Principles for Defining Tasks and Functions of ICCSs CIF

The following principles must be implemented when creating ICCSs CIFs [1]:

- integration,
- centralization,
- unification,
- scalability,
- modularity,
- survivability.

The principles of integration and consolidation should be implemented in relation to disparate data sets about CIF. Technically implemented through a consolidated repository of data sets about the object.

The principle of centralization is implemented by using for all subsystems of the automated control system a single metadata and regulatory information.

The principle of unification is implemented in the part of a single information and communication system for all structures of the information system and data formats.

The principle of scalability is realized through the possibility of gradual development and implementation of ICCSs CIF, the possibility of expanding the functional complement of the center without a fundamental replacement of the system and technical platform.

The principle of modularity is realized through the construction of ICCS as a set of modules for the implementation of individual functions and tasks. This will provide flexibility in the formation of the functionality of individual automated workstations, subsystems and the system as a whole under the necessary structure and mechanisms of security management.

The principle of survivability is realized through ensuring uninterrupted work, obtaining reliable results, protection against unauthorized actions.

The implementation of the described principles of ICCSs CIF was practically tested during the creation of the information security center at the National University "Chernihiv Polytechnic" within the NATO project "Cyber Rapid Analysis for Defense Awareness of Real-time Situation CyRADARS" [10]

Thus, the implementation of the proposed principles of ICCSs will increase the level of information and security of the CIF. The operation of ICCSs will ensure coordination and control of measures to deploy the information security system of critical infrastructure.

4. The Critical Infrastructure Facilities Information Systems Data Management Model

Methodological and methodical bases of information security are quite general recommendations based on the international experience and the theory of systems. The development and implementation of automatized control systems show that none of the security information tools is completely reliable.

The research and analysis of foreign and local experience demonstrate the necessity for building an integrated system of CIF information security, that includes operational, operational-technical and organizational measures for information protection. This system should provide flexibility and adaptation to rapidly changing factors of internal and external environment. It is impossible to provide this level of information security without making an analysis of existing threats and potential possibilities for information leakage.

The CIF information infrastructure can be presented in several hierarchical levels, each of which is characterized by the degree of information aggregation and its role in the management process. “Analytical stack” [11] developed by Gartner can be an example of systematic representation of the CIF information infrastructure. There are several levels in this hierarchy (Fig. 2):

-the level of transactional systems;

-the level of business intelligence, including data warehouses, data marts and OLAP-systems;

-the level of analytical applications.

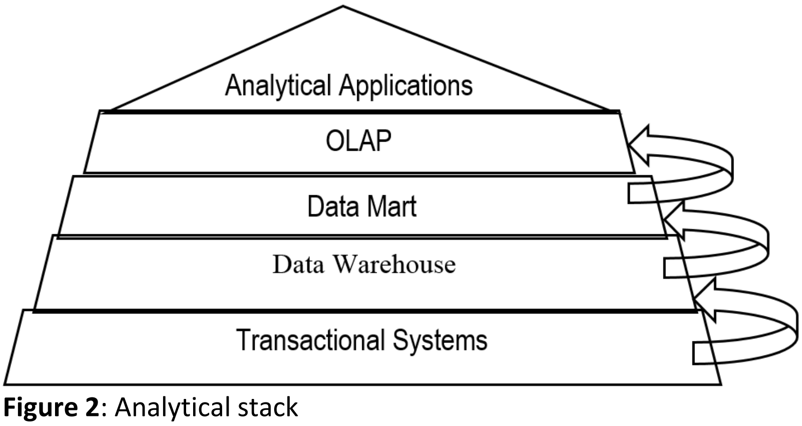

Figure 2: Analytical stack

Transactional systems include enterprise resource management systems and provide the information needs of management at the operational level. Despite the objective differences, all these systems have a common feature: they are designed to handle certain operations (On-Line Transaction Processing (OLTP) - processing transactions in real time). The goals, objectives and sources of information at the operational level are initially defined and have a high degree of structure and formalization.

Transactional systems are the sources of primary information, which after the appropriate processing are used for further analytical processing and presentation for making management decisions. From transactional systems, data can be passed to analytical applications either sequentially through all the levels of analytical stack or by passing one or more levels ("bypass" - "direct transfer").

Data warehouse (DW) is defined by Bill Inmon [12] as "subject-oriented, integrated, stable, supporting the chronology of data sets, organized for the purpose of management support, designed to act as "one and the only one source of truth" that provides managers and analysts with reliable information necessary for rapid analysis and making decisions".

However, the large amount of data contained in warehouses, usually make them unavailable for processing in real time. This problem is solved on the following hierarchy levels – data marts and OLAP- systems.

Data marts are structured information files, but their difference is that they are subject-oriented, the information is stored in data marts in the most favorable form for solving specific analytical problems.

The next level of the analytical stack is occupied by On-Line Analytical Processing (OLAP-system). This is the system of analytical data processing in real time that can provide the solutions of many analytical problems and work with relevant data despite of the company's activities characteristics.

OLAP-systems are characterized by large dimensions of stored data (as opposed to relational tables), preliminary calculation and aggregation of values, which makes it possible to build quick independent requests to operational database using a number of different analytical measures.

At the highest level of the analytical stack there are analytic applications, aimed at the analysis and decision support at the strategic level. The information system on the strategic level (Executive Support Systems, ESS) provides the support of making decisions concerning the implementation of promising strategic aims of enterprise development on the basis of solving unstructured problems, special problems that require professional judgments, estimates and intuition.

5. System Approach to the Formation of CIF Information Systems Security Policy

The development of information system security policy should include three levels: basic, segment and marginal. The security policy of base and segment levels must ensure the protection of information flow within the information system, the marginal level of security provides the protection of information exchange with the environment (Fig. 3).

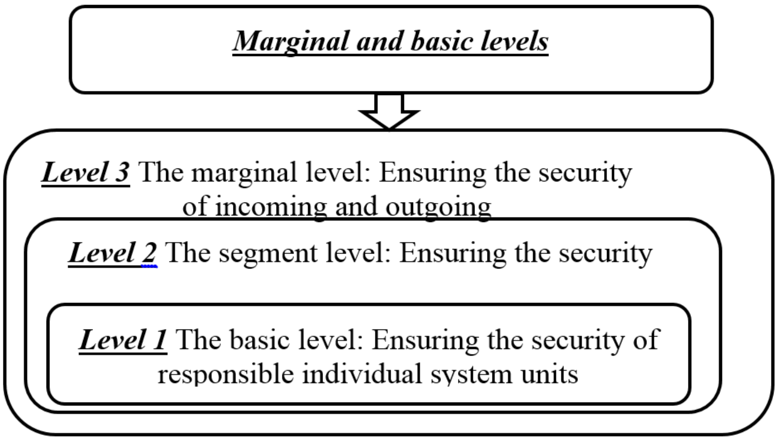
Marginal and basic levels
Level 3 The marginal level: Ensuring the security of incoming and outgoing
Level 2 The segment level: Ensuring the security
Level 1 The basic level: Ensuring the security of responsible individual system units

Figure 3: The hierarchical model of information security policy

There are the following types of information computer systems security policy [13]: discretionary security policy, mandate (authority) security policy, information system security policy and role differentiation of access.

Discretionary security policy is the security policy, based on the Discretionary Access Control, which is defined by two properties:

- all subjects and objects are identified;

- the rights of access to system objects and subjects are based on some external rules in relation to the system.

The main element $|S|\cdot|O|$, the lines of which correspond to subjects and the columns correspond to objects. In such a case every element of the access matrix *M[S,O]* with *R* determines the access rights of the subject *S* to the object *O*, where *R* is the set of permissions.

The advantages of discretionary security policy include the relatively simple implementation of access control systems; the disadvantages include the static of defined rules of access therein.

Mandate (authority) security policy is a security policy based on Mandatory Access Control, which is defined by four conditions:

- unambiguous identification of all subjects and objects of the system;
- given hierarchical levels of information confidentiality;
- every system object has the level of confidentiality that determines the value of information;
- every system subject has the access level.

Mandate security policy application helps to prevent the overflow of information from the objects with higher hierarchy level to the objects with low access level; on the other hand, the introduction of systems based on the security policy of this type is complicated and requires significant hardware and software resources of information system.

The approach of information flow security policy should be mentioned. It is based on the sharing of all possible information flows between the objects of the system into two disjoint sets: the set of enabling information flows and the set of adverse information flows, the purpose of implementation of which is to ensure the unavailability of emergences in the computer system information flows.

Role differentiation of access is the development of discretionary differentiation access policy, and the rights of access to system objects are based on their application-specific basis, defining their roles thereby. Role differentiation of access allows realizing flexible access control rules that take into account the dynamics of the computer system operation process.

In addition to the abovementioned policy we can name the policy of isolated software environment implemented by determining the order of safe interaction of system subjects that ensures the impossibility of influence on information and security systems and their settings modification or configuration.

The basis for constructing a system of information systems protection is the development of the security policy that is based on: organizational and management structure of the company; informational management needs of the enterprise; used organizational, technical and software; processing technology.

The security policy development should be based on a strict hierarchy; this means that the protection degree of different system units cannot be the same. Thus, the data that is being processed in these sites will be under the thread of unauthorized exposure risks. Having divided the information in several categories according to its importance (critical and non-critical), the model of any company's protection can be optimized.

6. Conclusions

The implementation of a systems approach in the creation of ICCSs will prevent interference in CIO information systems through the exchange of information and the functioning of centralized and decentralized technological systems. The consequence of creating ICCSs will be to reduce vulnerabilities, increase the efficiency of identifying new threats. ICCSs will enable: protection against existing threats by cooperating with specialized services in the virtual environment, raising the level of cybersecurity culture, monitoring and implementing CIO information security standards, developing new cybersecurity measures.

7. Acknowledgments

The work was carried out and funded under the NATO project CyRADARS (Cyber Rapid Analysis for Defense Awareness of Real-time Situation) – grant agreement number: G5286.

8. References

[1] H. Hulak, I. Skiter, E. Hulak, Methodological principles of establishment and functioning of the cyber security center of information infrastructure of nuclear energy facilities: education, science, technique 4(12) (2021) 172–186. doi:10.28925/2663-4023.2021.12.184186.

[2] International Electrotechnical Commission, IEC 61226, Nuclear power plants—Instrumentation and control important to safety—Classification of instrumentation and control functions, 2009.

[3] International Electrotechnical Commission, IEC 62645, Nuclear power plants—Instrumentation and control systems—Requirements for security programmes for computerbased system, 2014.

[4] Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, E03341, Energy Expert Cyber Security Platform, EECSP, 2017.

[5] DCAF Horizon 2015 Working Paper, No 1. URL: https://css.ethz.ch/en/services/digital-library/series.html/118118.

[6] Technical Committee for Standardization “Information Technology” (TC 20) with the participation of the Technical Committee for Standardization "Banking and Financial Systems. Information Technology. Methods of protection. Information security management systems. Requirements, ISO/IEC 27001:2015, 2016. DP UkrNDNC.

[7] Technical Committee for Standardization “Information Technology” (TC 20). Information Technology. Security methods. Information security management systems. Requirements, ISO/IEC 27001:2013, 2014, DP UkrNDNC.

[8] P. L. Turner, S. S. Adams, S. M. Hendrickson, Enhancing power plant safety through simulated cyber events. submitted to the American Nuclear Society’s, in: 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies, 2017, pp. 301–313. American Nuclear Society, ANS.

[9] Understanding SOA Security Design and Implementation. An IBM Redbooks publication. URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf.

[10] NATO SPS Project CyRADARS, Cyber Rapid Analysis for Defense Awareness of Realtime Situation. URL: https://www.cyradars.net, last accessed 2021/03/25.

[11] V. Lytvynov, et al., Computer Nets Attacks Defense Tools based on Extended Information about Environment, Monograph, Chernihiv: Chernihiv Politechnic National University, 2021.

[12] W. H. Inmon, F. Puppini, The Unified Star Schema: An Agile and Resilient Approach to Data Warehouse and Analytics Design, Technics Publications, 2020. isbn:978-1634628877.

[13] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction, No. 4009, 2010.