Design of Industry Centers of Cyber Security of Facilities of Critical Infrastructure

Anatolii Morozov[1], Alla Hrebennyk[1], Elena Trunova[2], Igor Skiter[3], and Evgen Hulak[4]

[1] *Institute of Mathematical Machines and Systems Problems, 42 Ac. Glushkov ave., 03680, Kyiv, Ukraine*
[2] *Chernihiv National University of Technology, 95 Shevchenko str., 14035, Chernihiv, Ukraine*
[3] *Institute for Safety Problems of Nuclear Power Plants of the National Academy of Sciences of Ukraine, 36a Kirov str., 07270, Chernobyl, Ukraine*
[4] *DTEK Service Ltd., 57 L. Tolstogo str., 01032, Kyiv, Ukraine*

Abstract

The process of designing industry centers of cyber security (ICCS) of critical infrastructure objects, their structure, functional components, elements of hardware and system software are presented. The scheme of interaction of functional components directly involved in security management of the corporate network is considered. The scheme of conducting databases on the basis of operation of search on the Internet is offered. The main functions of industry centers of cyber security are defined and the stages of creation are considered: SOC core and basic sources of information, integration of external platforms and additional sources, auxiliary systems.

Keywords

Industry center of cybersecurity, critical infrastructure, information security.

1. Introduction

At present, the regulations of European countries define the concept of critical infrastructure in different ways and the corresponding lists of industries and facilities that are of strategic importance for national security. There are no generally accepted requirements for building a critical infrastructure protection system and its integral component—information infrastructure. The term “critical information infrastructure” means a set of information systems, information and telecommunications networks, and automated control systems (including process control) that are physically or logically connected to global networks and are essentially part of cyberspace. Disruption of the sustainable functioning of these systems through the implementation of threats to information security and cybersecurity can cause significant damage to the vital interests of the state, society and people.

The processes of global informatization help to improve the quality of human life, but they have resulted in a deep dependence of modern society on the security of the information infrastructure, which is the object of cybersecurity. That is why ensuring the security of critical infrastructure and its important component - critical information infrastructure is one of the priorities in reforming the defense and security sector of Ukraine [1–3].

The basic principle of ensuring the security of critical information infrastructure is a public-private partnership. At the same time, managers or owners of facilities (corporate networks) directly implement security, and the state provides them with all possible assistance [4–6]. It is known that the more complex the IT infrastructure of the organization, the greater the likelihood of vulnerabilities that increase the risks of cyber threats. The recommendations of the Geneva Center for Information Security (DCAF) identify the task of creating a reliable and credible digital infrastructure as a priority measure to combat cyber threats [7].

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: ipmms@immsp.kiev.ua (A. Morozov); grebennik.alla@gmail.com (A. Hrebennyk); e.trunova@gmail.com (E. Trunova); skiteris@ukr.net (I. Skiter); geg180579@gmail.com (E. Hulak)
ORCID: 0000-0002-3923-94945 (A. Morozov); 0000-0002-7464-1412 (A. Hrebennyk); 0000-0003-0689-8846 (E. Trunova); 0000-0003-2334-2276 (I. Skiter); 0000-0003-4984-686X (E. Hulak)

Note that over time, information security issues are becoming more relevant. The availability of information security managers methods and tools for current control of the level (state) of security of the information system allows: increase the efficiency of responding to cyber incidents; choose adequate countermeasures; effectively determine the procedures for restoring the system and reduce its downtime; systematically investigate cyber incidents; purposefully identify measures to eliminate identified vulnerabilities.

In the conditions of high cost and complexity of construction and application of the corresponding tools for control of a condition of information security the application (use) of methods of collective protection of branch corporate information systems is considered as the rational decision. At the same time, they provide for the prompt exchange of information on cyberattacks and recommendations for combating them. In this case, a comprehensive solution to ensure the cyber protection of such systems may be the construction of a sectoral cyber security center (ICCS), which can be created in cooperation and in the interests of regional and municipal authorities, ministries and departments, large companies of industry.

The main task of ICCS is to timely detect and to prevent cyber incidents, eliminate their consequences, monitor the current situation in cyberspace and develop measures to prevent the recurrence of cyber incidents and improve cyber security. From the above it follows that the hardware and software complex ICCS is a complex automated system that requires careful methodological, informational and architectural processing. The purpose of the article is to develop a conceptual framework for the construction of viable industry centers of cyber security that provide increased efficiency of attack detection systems of associated networks.

The process of creating ICCS requires the definition of their tasks and stages of creation, structure, model, functional components, hardware platform, systems and application (special) software.

2. Collective Protection of Corporate Networks against Computer Attacks

As mentioned earlier, it is advisable to rationally apply the methods of collective protection to ensure the cybersecurity of corporate networks of the class of industry information systems.

In this case, managing the settings of the attack detection system (ADS) analyzers, which protect the components of the network association, can be assigned to the Industry Center for Cyber Security (ICCS), while the ADS and *i* elements of the S*i* network association will take over operational management functions.

Intensive exchange of information about the settings, about the danger of the environment, about the attacks on the network is being carried out between ICCS and IDS. It should also be borne in mind that S_i can be created at different times and on different computing platforms. Therefore, one of the best ways to combine the networks of the industry association $S = \{S_1,\ S_2, \ldots, S_k\}$ can be an architectural solution in the form of an integration information bus [8–17] (Fig. 1). Integration information bus (IIB) is based on the ideas of using Web-services, HTTP, XML and its extensions SOAP, WHD [18–21].

Collective defense requires an intensive exchange of information about attacks, the speed of their spread, recommendations for combating them.

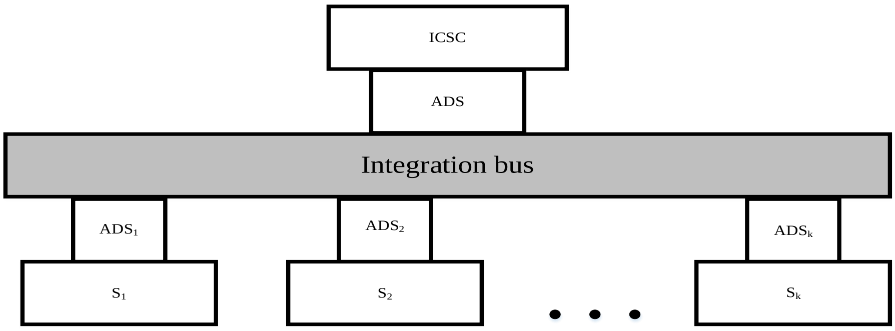

Figure 1: Integration bus of network association

To do this, ICCS must provide:

- Communication with international and national computer security centers.
- Monitoring of the Internet and social networks by sources and types of attacks.
- Maintaining databases on security issues.
- Distribution by elements of the association of information on the parameters of setting ADS$_i$ elements of S_i, obtained on the basis of forecasting the state of threats.
- Dissemination among the elements of the association of information about unusual behavior, attacks of unknown type and recommendations to combat them.
- Structuring of unknown types of attacks.
- Organization of collective protection of the network association for the corporation.

It follows from the above that the information and software complex of ICCS is a complex software and hardware design that requires careful methodological, informational and architectural elaboration.

The tasks of word processing and assessment of cyber threat indicators for corporate networks are inherent in the global network layer of the network architecture. Therefore, given the time requirements required for the ADS, it can be assumed that the inclusion of such tasks will lead to a slowdown in the performance of basic functions and an unjustified increase in resource consumption. We offer delegation of functions of a global network level of protection of a corporate network to functions of a separate computer complex. When it manages this level of protection for several corporate networks and determines the threat indicators for each of them, it will be, in our opinion, a promising solution. Let's call this part of the complex a threat monitoring system (TMS).

Peculiarities of information circulation on the Internet are: severe shortage of time to search, collect, extract and process information, its accumulation, systematization according to certain classification criteria, further analysis, synthesis, generalization and delivery to interested users, as well as transformation into synthesized conclusions and recommendations. This necessitates, firstly, the automation of all measures associated with these processes in integrated threat monitoring systems and, secondly, the configuration of ADS subordinate TMS corporate networks in accordance with their characteristic risk vectors.

In addition to the parallelism in the performance of certain functions of TMS and ADS, this solution allows for collective protection of subordinate corporate computer networks from computer attacks. The essence of this protection is to conduct self-diagnostics of corporate computer networks by ADS, exchange information with partners about attacks and unusual behavior, about interference in work. Here you can solve the problem of determining the rate of spread of external interventions, coordination of ADS parameters, including coordination of efforts to analyze unknown intrusions.

The structure of such a complex is presented in Fig. 2 [5].

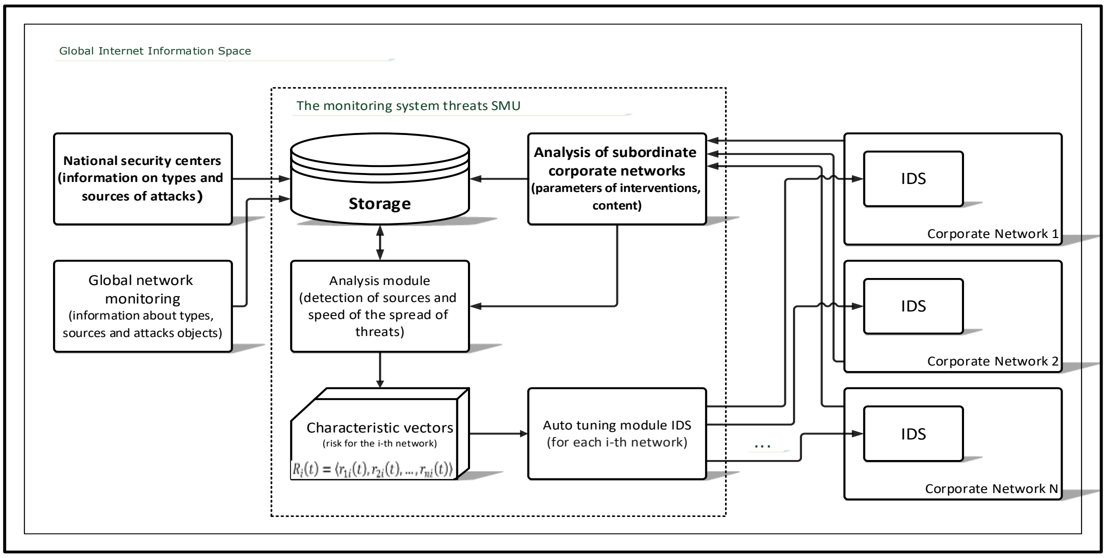
Global Internet Information Space
The monitoring system threats SMU
National security centers (information on types and sources of attacks)
Storage
Analysis of subordinate corporate networks (parameters of interventions, content)
Global network monitoring (information about types, sources and attacks objects)
Analysis module (detection of sources and speed of the spread of threats)
Characteristic vectors (risk for the i-th network)
$R_i(t) = (r_{1i}(t), r_{2i}(t), \dots, r_{ni}(t))$
Auto tuning module IDS (for each i-th network)
...
IDS
Corporate Network 1
IDS
Corporate Network 2
IDS
Corporate Network N

Figure 2: TMS architecture

Organizational and technical model of the branch center of cybersecurity management consists of two zones CyberCenter and CyberNet and the corresponding interaction between them and is presented in publications [22–24].

Development of a corporate network protection model with adaptive and collective protection properties, methods of detecting and identifying computer attacks by means of Internet content analysis and the corresponding ADS architecture will create a basis for the synthesis of reliable and high-performance adaptive cyber threat detection systems and decreasing the next generation computer attack cycle [25–27].

The use of adaptive network security management methods justifies the need to create industry security centers that improve the efficiency of the ADS networks subordinate to them [28,29].

3. Functional Components of ICCS as Elements of its Special Software

In our opinion, the functional components of ICCS for corporate network security management should include:

- Threat forecasting unit for the period [t, t + Δt], the input information of which will be a database of the history of threats, which accumulates information from ADS analyzers of corporate networks, with settings for the period [t-Δt, t].
- Determination of analyzer settings for the period [t, t + Δt].
- Determining the style of the source of attacks.
- Search for sources of attacks by similarity of style.
- Ranking of potential sources of attacks.
- Making decisions about the sources of attacks in conditions of uncertainty.

The scheme of interaction of ICCS functional components that are directly involved in the management of computer network (CN) security is shown in Fig. 3.

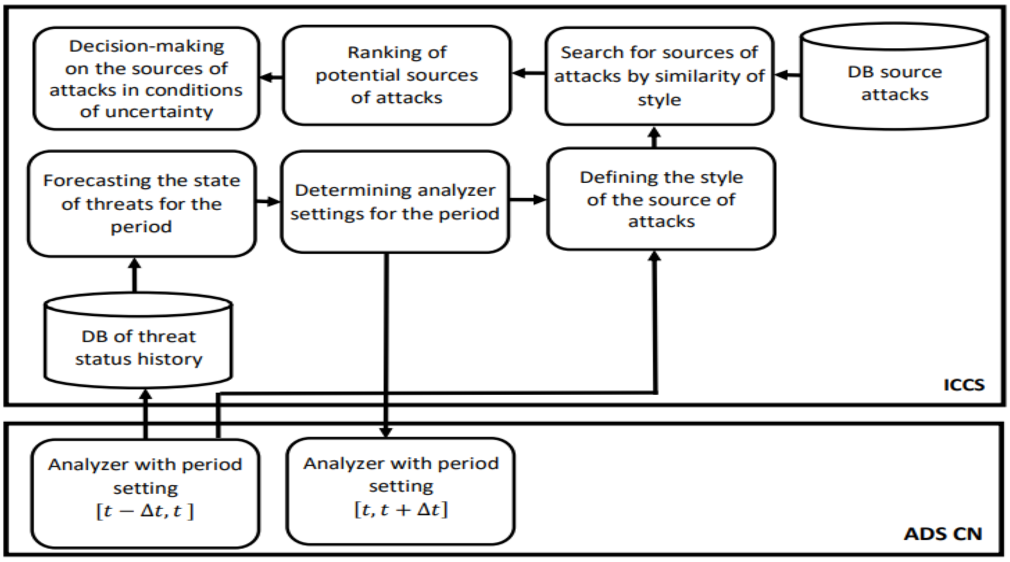
Decision-making on the sources of attacks in conditions of uncertainty
Ranking of potential sources of attacks
Search for sources of attacks by similarity of style
DB source attacks
Forecasting the state of threats for the period
Determining analyzer settings for the period
Defining the style of the source of attacks
DB of threat status history
ICCS
Analyzer with period setting [$t - \Delta t, t$]
Analyzer with period setting [$t, t + \Delta t$]
ADS CN

Figure 3: ICCS functional components involved in corporate network security management

The functionality of ICCS components is provided by searching the Internet for information necessary for the maintenance of ICCS databases and the proper functioning of the system as a whole.

Strategies that ensure the filling of DB ICCS can be the use of indicators and methods such as:

- Place of registration of IP-addresses and domains that participate in the attack or provide the infrastructure for the attack.
- Tracing the attack to its source or at least the location of the area in which the source is located.
- Time parameters.

- Analysis of program code, in which you can find comments, links to sites, domains, IP-addresses involved in the attack.
- Handwriting of programmers and programming school.
- Stylmetry, which allows you to determine the style of language in the comments or related texts.
- Fraudulent systems or honepot / honeynet.
- Operational development.
- Analysis of activity on forums and social networks.
- Identification ex post facto by actions.
- Methods of competitive intelligence, etc.

Internet search, as well as the use of databases of national security centers, allows you to keep up to date such important databases as: DB of competitors, DB of attack initiators, DB of attack sources. As well as DB of ntermediate information, based on which you can build an information portrait of the source, his preferences for functioning, style of attacks of different types, etc. (Fig. 4). This greatly facilitates the process of finding sources of attacks in the conditions of “sweeping the tracks” and adjusting the network information in the packets.

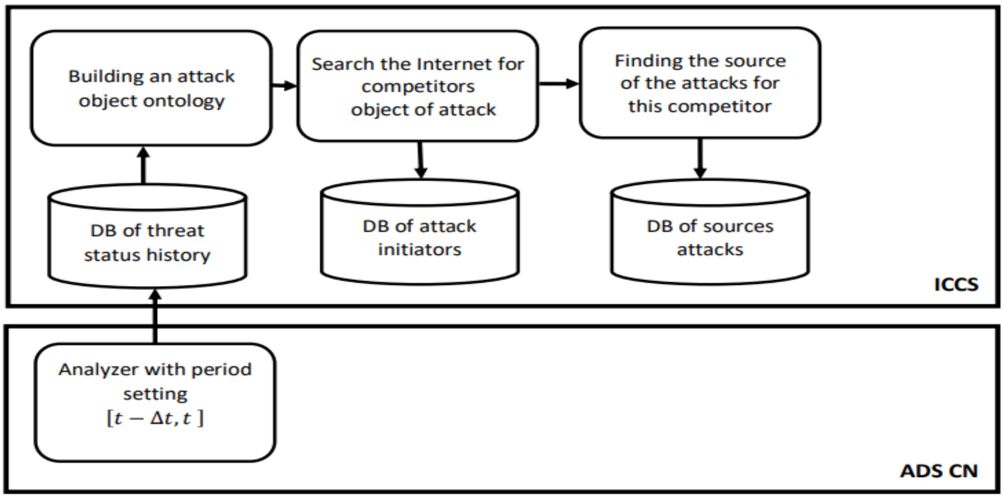
Building an attack object ontology
Search the Internet for competitors object of attack
Finding the source of the attacks for this competitor
DB of threat status history
DB of attack initiators
DB of sources attacks
ICCS
Analyzer with period setting
$[t - \Delta t, t]$
ADS CN

Figure 4: Scheme of DB ICCS based on the Internet search operation

ICCS hardware and system software must ensure close integration of its elements and subsystems, contain open and / or specialized interfaces for interaction and data exchange.

The technological core of the Center should be provided with server equipment, additional software and hardware components, in particular they should include:

- Systems of storage, archiving and backup of data of sufficient capacity for storage of telemetry data and analytics of the Centers for at least three years in the mode of “hot” and “cold” archives.
- Firewalls for segmentation of security centers of the Centers.
- Technical devices for routing and switching.
- Workstations for the Center’s employees.
- Software and hardware (server) software for managing firewalls, virtualized computing environment, etc.

4. Elements of Technical and System Software of the Center

The components of the sensors of the system for monitoring, detection and response to incidents are designed for direct deployment at information security facilities, monitoring and control of the level of cybersecurity at these facilities. Installed sensors must provide such services [12, 25]:

- Collection and correlation of security events, which also includes the collection of network telemetry with detailed information about network flows and sessions.
- Monitoring and detection of known threats and attacks, detection of network intelligence and network sounding.
- Detection and analysis of malicious software transmitted by the network, tracking its spread at the network level.
- Monitoring and detection of new types of attacks through the analysis of network behavior and anomalies, which includes the detection of indicators of compromise and traces of targeted attacks.
- Collection, preliminary analysis and indexing of other information, including work logs (syslog), SNMP from network devices and workstations.
- Traffic collection in Full Packet Capture mode (optional) to enable further analysis by DPI systems and study the details of possible cyberattacks.

Sending information to ICCS and managing the system should be done using a router with a separate communication channel, it is recommended to use a dedicated physical channel, or LTE/3G, independent of the infrastructure of the protected object. The data transmitted in the channel must be cryptographically protected using IPSec VPN technologies, using authentication using certificates issued by the CA of the central monitoring system. If it is not possible to use a dedicated channel, the possibility of organizing a VPN channel through a standard Internet channel used to connect the monitored object to the Internet should be considered.

The sensor must consist of the following components:

- Router for communication with ICCS.
- A switch for combining components, receiving information from the monitored network and supporting telemetry collection.
- Network branch for removing a copy of traffic from the network.
- Device for analyzing network traffic to detect events and incidents.
- Network traffic telemetry collection and correlation system.
- System for collecting, analyzing and indexing log information as well as information collected by other components of the sensor for further transmission of this information to ICCS.
- Platform for deploying a virtual environment for additional information security management, monitoring and analysis programs.
- Uninterruptible power supply to ensure power supply and uninterrupted power supply of the software and hardware complex.
- Protective cabinet with the possibility of signaling unauthorized access.

5. Functions of a Typical ICCS

The functions of a typical ICCS are shown in Fig. 5.

1. Department of monitoring, detection and response

1.1. Management of monitoring and detection of network attacks:

1.1.1. Monitoring:

- Provision of telemetry from devices located in state-owned enterprises and critical infrastructure facilities.
- Selection of data with suspicious characteristics.
- Interaction with the response function.
- Provision of the Call Center function for connections with CyberNet entities.
- Protection of web access and web traffic.

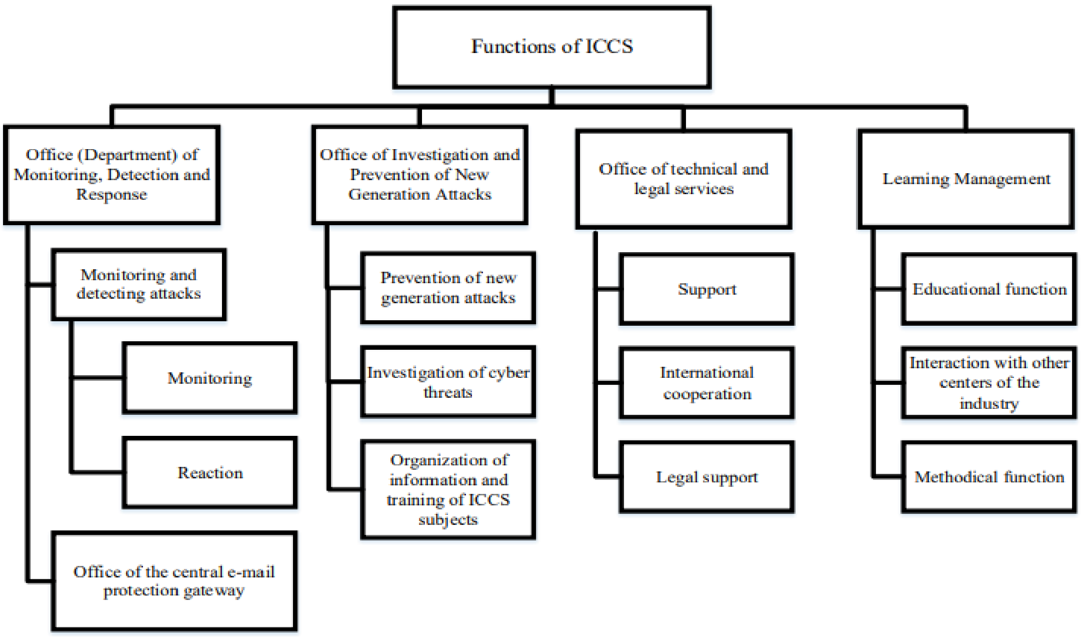
Functions of ICCS
Office (Department) of Monitoring, Detection and Response
Monitoring and detecting attacks
Monitoring
Reaction
Office of the central e-mail protection gateway
Office of Investigation and Prevention of New Generation Attacks
Prevention of new generation attacks
Investigation of cyber threats
Organization of information and training of ICCS subjects
Office of technical and legal services
Support
International cooperation
Legal support
Learning Management
Educational function
Interaction with other centers of the industry
Methodical function

Figure 5: Functions of a typical ICCS

1.1.2. Responding to network attacks:

- Detection of network intelligence and sounding.
- Detection and blocking of known threats and attacks in accordance with the rules and signatures.
- Detection and blocking of botnet control centers (C&C).
- Tracking and preventing attempts to spread malware (malware).
- Protection against DoS/DDoS attacks.

1.2. Central e-mail gateway management:

- Protection of e-mail of CyberNet entities with the help of centralized e-mail support services and Internet communications.
- Filtering malicious code.
- Detection of spam and phishing attacks in e-mails.
- Interaction with technical support.

2. Office of Investigation and Prevention of New Generation Attacks:

2.1. Prevention of new generation attacks:

- Collection and correlation of security events, data on network telemetry.
- Early detection of indicators of compromise and traces of targeted attacks.
- Advanced analysis of new types of malware.
- Monitoring of threat response at facilities by conducting appropriate tests, research and development at critical infrastructure facilities.
- Tracking new trends in methods and means of protection.
- Development of new methods and approaches to information security protection of CyberNet entities.
- Assessment and forecasting of existing and possible threats in the industry.
- Detection and prevention of new types of attacks by analyzing network behavior and anomalies.
- Threat assessment.

- Development of measures aimed at preventing, responding to and eliminating the consequences of incidents.

2.2. Cyber threat investigations:

- Recording of detected incidents.
- Collection, accumulation and storage of incident data.
- Interaction with competent and regulatory bodies in the field of information security protection and international organizations in the framework of incident investigations.
- Conducting investigations of incidents in accordance with the legal framework of Ukraine.

2.3. Organization of information and training of SOC subjects:

- Providing comprehensive information on the regulatory and legal framework for cybersecurity.
- Development of cybersecurity policies.
- Establishment of mandatory information security requirements for critical information infrastructure facilities, including during their creation, commissioning, operation and modernization, taking into account international standards and the specifics of the industry to which the relevant critical information infrastructure facilities belong. Monitoring their implementation.
- Development of measures to strengthen the general situational awareness of incidents and vulnerabilities among industry institutions and their critical infrastructure.
- Development of information exchange measures and coordination of actions to reduce current vulnerabilities, prevent new ones and, in case of threats, effectively localize them.
- Critical infrastructure, information security and cybersecurity.
- Planning, organizing and conducting cyber training.

3. Technical and legal service management

3.1. Technical Support

- Operation and maintenance of SOC infrastructure.
- Installation, adjustment and maintenance of sensors.
- Organization and support of restoration of efficiency of systems of objects of critical infrastructure.
- Automation and software support of methods of monitoring, detection, response and recovery of critical infrastructure systems.
- Conducting research, designing, developing and deploying new tools to ensure the effective operation of CyberCenter.
- Writing new signatures of detected malicious codes.
- Collection and storage of materials and results of audits.

3.2. International interaction:

- Establishing communications with the victorious centers.
- Exchange of relevant information.
- Interaction during joint counteraction to threats, detection of international incidents, cyber-terrorist campaigns, etc.

3.3. Legal support:

- Ensuring the correct application of regulations and other documents in ICCS.
- Develops and participates in the development of draft acts and other documents on ICCS activities, monitors the compliance of documentation with legislation.
- Participates in the preparation and conclusion of economic and other agreements with enterprises, institutions, organizations.
- Tracking the current state of the regulatory framework of Ukraine in the field of information security.

- Registration of results of investigations of cyber incidents according to regulatory requirements.

4. Learning management

- Development of own training programs aimed at getting acquainted with the main goals and objectives of ICCS.
- Interaction with other Centers of the branch, software and hardware, policies of the information security management system and other normative and regulatory documents.
- Planning, organizing and conducting cyber training.

6. Stages of creating a typical ICCS

The main stages of creating a typical ICCS are presented schematically below in Fig. 6.

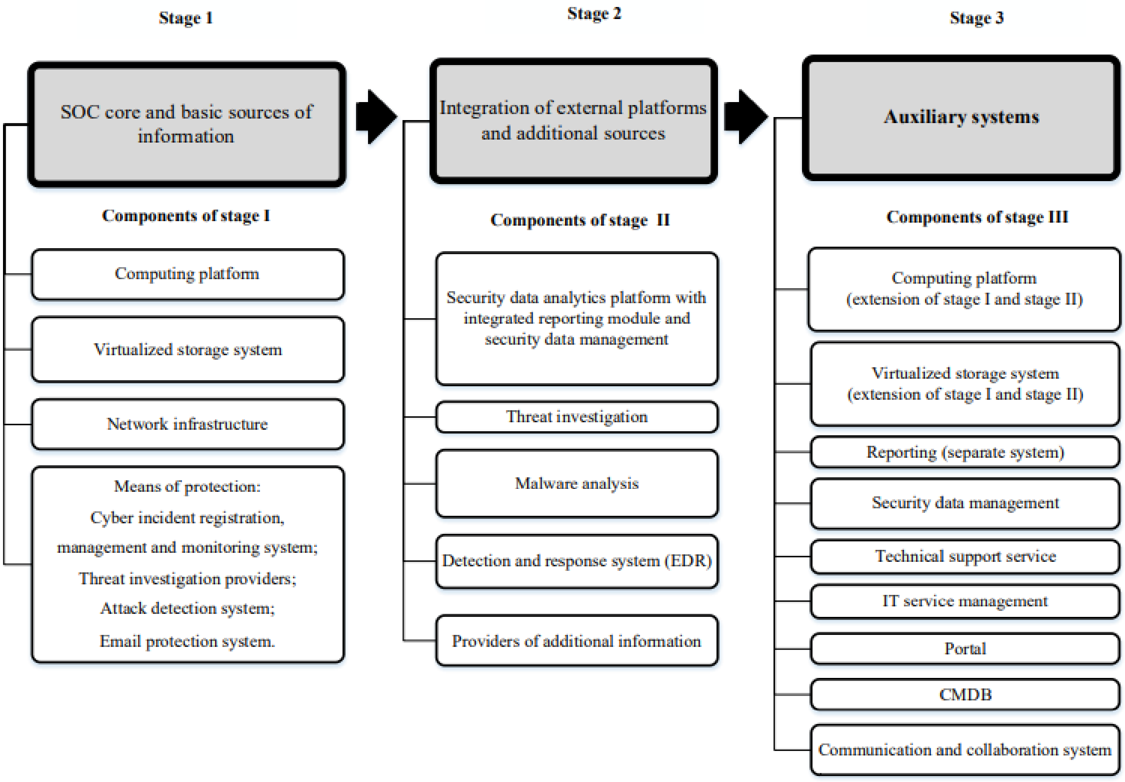
Stage 1
Stage 2
Stage 3
SOC core and basic sources of information
Integration of external platforms and additional sources
Auxiliary systems
Components of stage I
Computing platform
Virtualized storage system
Network infrastructure
Means of protection:
Cyber incident registration,
management and monitoring system;
Threat investigation providers;
Attack detection system;
Email protection system.
Components of stage II
Security data analytics platform with integrated reporting module and security data management
Threat investigation
Malware analysis
Detection and response system (EDR)
Providers of additional information
Components of stage III
Computing platform (extension of stage I and stage II)
Virtualized storage system (extension of stage I and stage II)
Reporting (separate system)
Security data management
Technical support service
IT service management
Portal
CMDB
Communication and collaboration system

Figure 6: The main stages of creating a typical ICCS

Stage I Core SOC and basic sources of information.

1.1. Computing platform.
1.2. Virtualized data storage system.
1.3. Network infrastructure.
1.4. Means of protection: system of registration, conducting and monitoring of cyber incidents; threat investigation providers; analysis of network anomalies; attack detection system; email protection system.

Stage II Integration of external platforms and additional sources.

2.1. Security data analytics platform with integrated reporting module and security data management.
2.2 Threat investigation.
2.2. Malware analysis.
2.3. Security incident management.
2.4. Detection and response system (EDR).
2.5. Providers of additional information.

Stage III Auxiliary systems.

3.1. Computing platform (expansion based on the results of Stage I and II).
3.2. Virtualized data storage system (expansion based on the results of Stage I and II).
3.3. Reporting (separate system).
3.4. Security data management (separate system).
3.5. Technical support service.
3.6. IT service management.
3.7. Portal.
3.8. CMDB.
3.9. Communication and collaboration systems.

7. Conclusions

Designing industry-leading cybersecurity centers for critical infrastructure in accordance with the proposed structure, functional components, hardware and system software elements and certain functions and stages of creation allow to increase the efficiency of ADS networks under their jurisdiction. This justifies the need to create them. The presented results were used in the process of implementation of the international scientific project “Cyber Rapid Analysis for Defense Awareness of Real-time Situation—CyRADARS” under the grant of NATO SPS.

8. 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 [24].

9. References

[1] Resolution of the Cabinet of Ministers of Ukraine of October 9, 2020 No. 943 “Some questions of objects of critical information infrastructure” (Extraction). URL: https://cis-legislation.com/document.fwx?rgn=128253.

[2] Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated 09.10.2020 “Certain issues on critical infrastructure objects.” URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

[3] Resolution of the Cabinet of Ministers of Ukraine of November 11, 2020 No. 1176 “About approval of the Procedure for carrying out survey of condition of cybernetic protection of critical information infrastructure, the state information resources and information which requirement concerning protection is established by the law.” URL: https://cis-legislation.com/document.fwx?rgn=128947.

[4] Corporate network. URL: https://www.insee.fr/en/metadonnees/definition/c1927.

[5] V. Lytvynov, Corporate networks protection against attacks using content-analysis of global information space, Technical sciences and technology (2018). doi:10.25140/2411-5363-2018-1(1)-115-130.

[6] V. Lytvynov, et al., Principles of adaptive corporate network security management, Advances in Intelligent Systems and Computingthis link is disabled (AISC) 1265 (2021) 255–265. doi:10.1007/978-3-030-58124-4_25.

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

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

[9] Service Oriented Architecture Security Risks and their Mitigation. Sarath Indrakanti. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a576267.pdf.

[10] The importance of a standard securit y archit ecture for SOA-based iot middleware. URL: https://ieeexplore.ieee.org/document/7355580.

[11] Secure your SOA. Enterprise-grade SOAs require a plan for addressing diverse security needs. URL: https://www.javaworld.com/article/2071751/secure-your-soa.html.

[12] The ISO 27001:2013, Statement of Applicability (SoA): The Complete Guide. URL: https://www.isms.online/iso-27001/iso27001-statement-applicability-simplified/.

[13] The importance of the Statement of Applicability in ISO 27001—with template. URL: https://www.itgovernance.co.uk/blog/the-importance-of-the-statement-of-applicability-in-iso-27001.

[14] The ISO/IEC WD 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity. URL: https://www.iso.org/standard/44375.html.

[15] Part III. Enterprise SOA security. URL: https://livebook.manning.com/book/soa-security/part-iii-enterprise-soa-security/5.

[16] A standardized SOA based solution to guarantee the secure access to EHR. URL: https://core.ac.uk/download/pdf/82597744.pdf.

[17] SOA Security. URL: https://www.manning.com/books/soa-security.

[18] HTML. URL: https://ru.wikipedia.org/wiki/HTML.

[19] H. Hulak,et al. Formation of requirements for the electronic record-book in guaranteed information systems of distance learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923, Kyiv, 2021, pp. 137–142.

[20] WHDL. URL: https://www.whdl.org.

[21] J. C. Kim, Comparing web APIs with service-oriented architecture and enterprise application integration. Integration architecture. Published on March 18 (2015). URL: https://developer.ibm.com/technologies/web-development/articles/comparing-web-apis-with-service-oriented-architecture-and-enterprise-application-integration.

[22] V. Lytvynov, et al., Using decision support in finding sources of attacks on computer networks under uncertainty. Mathematical Mashines and Systems (2019). doi:10.34121/1028-9763-2019-4-38-51.

[23] V. Lytvynov, et al., Attacks defense of computer nets by tools using extended information about environment: monograph, Chernihiv Politechnic National University, 2021.

[24] S. Shkarlet, et al., The Model of Information Security Culture Level Estimation of Organization, Advances in Intelligent Systems and Computing, AISC, Springer, Cham (2020). doi:10.1007/978-3-030-25741-5_25.

[25] M. Vladymyrenko, et al. (2019). Analysis of Implementation Results of the Distributed Access Control System. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), doi: https://doi.org/10.1109/picst47496.2019.9061376

[26] A. Carlsson, et al. Sustainability Research of the Secure Wireless Communication System with Channel Reservation. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020. https://doi.org/10.1109/tcset49122.2020.235583

[27] V. Buriachok, et al., “Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies,” Cybersecurity Providing in Information and Telecommunication Systems (CPITS), pp. 23–32, Jul. 2020.

[28] G. Radchenko, Distributed Computer Systems, Chelyabinsk: Photo artist, 2012. URL: https://glebradchenko.susu.ru/doc/Radchenko_Distributed_Computer_Systems.pdf.

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