Decentralized Access Demarcation System Construction in Situational Center Network

Viktor Grechaninov[1], Hennadii Hulak[1,2], Evgen Hulak[3], Pavlo Skladannyi[2], and Volodymyr Sokolov[2]

[1] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680, Kyiv, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[3] *DTEK Service Ltd., 57 L. Tolstogo str., 01032, Kyiv, Ukraine*

Abstract

Although there is an understanding in the computer community of the need to improve the cyber protection of the information sector of critical infrastructure and the awareness of the urgent need to implement the best practical and theoretical developments in this area is growing rapidly, the total number of incidents in cyberspace is not significantly decreasing, and the urgency of the search for new technological solutions is only increasing. Without exaggeration, it can be stated that a critically important component of the information protection system is its component—the system of delimiting the access of subjects to the objects of the computer system. In many cases, modern demarcation subsystems are built based on a centralized approach to information security management. This article proposes and justifies a partially decentralized approach to building an information security management system and delimiting access in computer systems so that future security measures can rest on a reliable foundation.

Keywords

Information security policy, cyber defense, access control system, secret distribution, block cipher, perfect cipher.

1. Introduction

First, it seems appropriate to pay attention to the fact that the object of the research is a network of situational centers, which combines several structures—mainly equal partners, the purpose of which cooperation in the information field is the formation of balanced management decisions regarding the adoption of adequate measures in specific crises [1]. At the same time, system users, in contrast to the methods of ensuring integrity or availability, may have their unique requirements for ensuring the confidentiality of the information resources created by them due to the specifics of the methods of obtaining preliminary information and/or methods of their further processing, their own "know-how" and/or copyright for some products, etc. [2–4].

Many scientific studies have been devoted to the problems of building access demarcation systems (ADS). In particular, [5–7] provides a systematic review and analysis of the construction of existing and prospective models. However, their effectiveness in ensuring the confidentiality of information resources is not defined.

In [8], partial indicators of effectiveness are proposed to implement the procedure for evaluating the effectiveness of the system of information protection and cyber security of objects of critical information infrastructure.

In [9], the expansion of access control mechanisms in a specific class of sensitive information systems is investigated.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: vgrechaninov@gmail.com (V. Grechaninov); h.hulak@ukr.net (H. Hulak); geg180579@gmail.com (E. Hulak); p.skladannyi@kubg.edu.ua (P. Skladannyi); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0001-6268-3204 (V. Grechaninov); 0000-0001-9131-9233 (H. Hulak); 0000-0003-4984-686X (E. Hulak); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-9349-7946 (V. Sokolov);

It should be noted that these studies are mainly based on the centralized principle of information security management, when the owner of the system or its manager, by the requirements of regulatory acts and standards [10–12], the procedure for accessing information and the requirements for the architecture of the ADS.

In contrast to the mentioned approach to the construction of a centralized access management system (CAMS), another approach is developing—decentralized [13, 14], which provides the opportunity to delegate part of the powers from the central level of security management to other components of the security system. Namely, in these works, the issue of building a system of access demarcation and a new approach to their architecture will be considered.

This approach consists of placing the element responsible for making decisions about allowing or denying subjects access to objects outside the workstation at which access is restricted. This item resides on another workstation and can be used to restrict access across multiple machines. This approach is called "decentralization of the access delimitation system," considering that the system is divided into several components installed on different workstations.

The proposed article provides a concrete solution to the partial decentralization of the access demarcation system based on an evidence-based approach to information security guarantees [15, 16].

2. Problems of CAMS and the Way of Their Solution

As mentioned above, the cyber protection complexes of modern information systems (IS) are mainly built according to the principle of centralized security management, which provides for the presence of single management in the system, directed by the owner or manager of the information system. In the future, referring to the system's owner, we will understand that the relevant provisions also apply to its administrator. The corresponding security model is shown in Fig. 1.

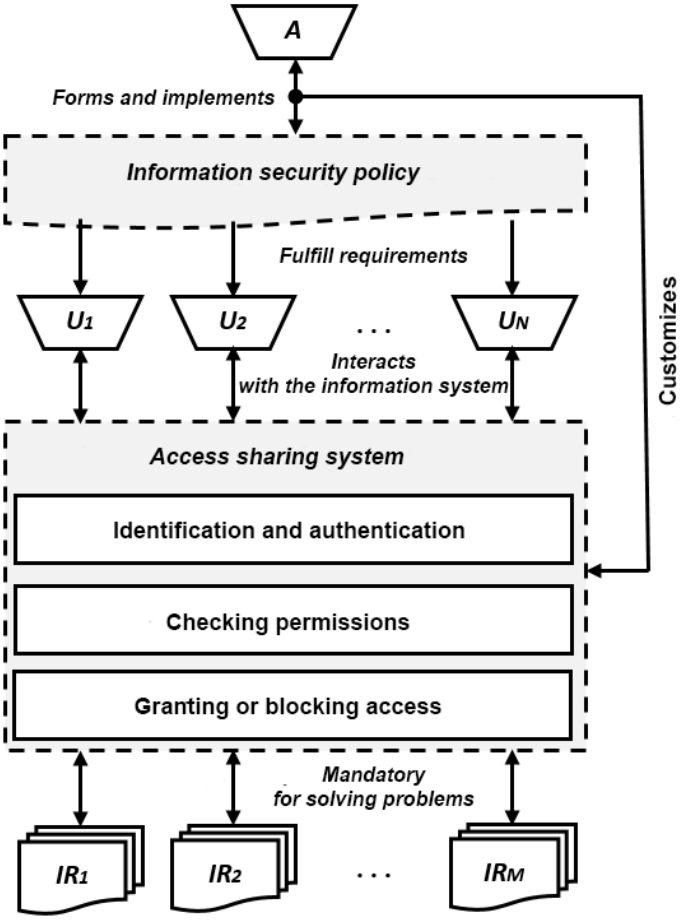

Figure 1: Ontological model of the centralized security system in protected IS

This model includes a conditionally single administrator A, who forms and implements the information security policy (ISP), which is approved by the management of the organization - the owner of the system, and also configures the components of the cyber protection system and monitors the implementation of measures that are provided by the ISP and regulatory documents [10] . Information system users $U_1, U_2, \dots, U_N$ following the rules defined by the ISP, interact with IS to gain access to information resources $IR_1, IR_2, \dots, IR_M$ that are necessary for solving certain problems. As a rule, users do not participate in forming ISP and configuring security measures, including the access control system.

The advantages of this approach to building an information security management system are:

- Unification of protection requirements for all system components.
- Reducing the risk of formation of relatively weak links or vulnerabilities.
- A single vertical of management and control of delimitation of access to information system resources.

At the same time, this approach is not free from some disadvantages, namely:

- Potentially, a security system administrator, thanks to too much authority, can personally gain access to the contents of confidential information resources or, without sufficient grounds, grant access to a particular user of the system.
- In the case of overcoming protective barriers, for example, in case of abnormal functioning of the protection system, the attacking party may attempt unauthorized access to an insufficiently protected resource.
- There is a potential danger of copying and unauthorized distribution by insiders of open resources that were created at the expense of the owner and users of the system or are subject to copyright.

It should also be noted that in information systems that combine several different corporate subsystems, in general, a user can act in one or two guises: as the owner of an information resource and as a consumer of the resource (client/utilizer).

At the same time, taking into account the potentially sensitive nature of the method or method of obtaining or collecting (receiving) the original information that forms the information resource, its owner may have legal grounds for approval or restriction of access to consumers (clients) to it, and can also provide suggestions regarding ISP to the system as a whole and perform security administration of its segment and control its status.

A similar situation, in particular, can be observed in the network of situational centers of state bodies.

The model of a partially decentralized security system in a protected IS, which considers the corresponding shortcomings of a centralized system, is shown in Fig. 2.

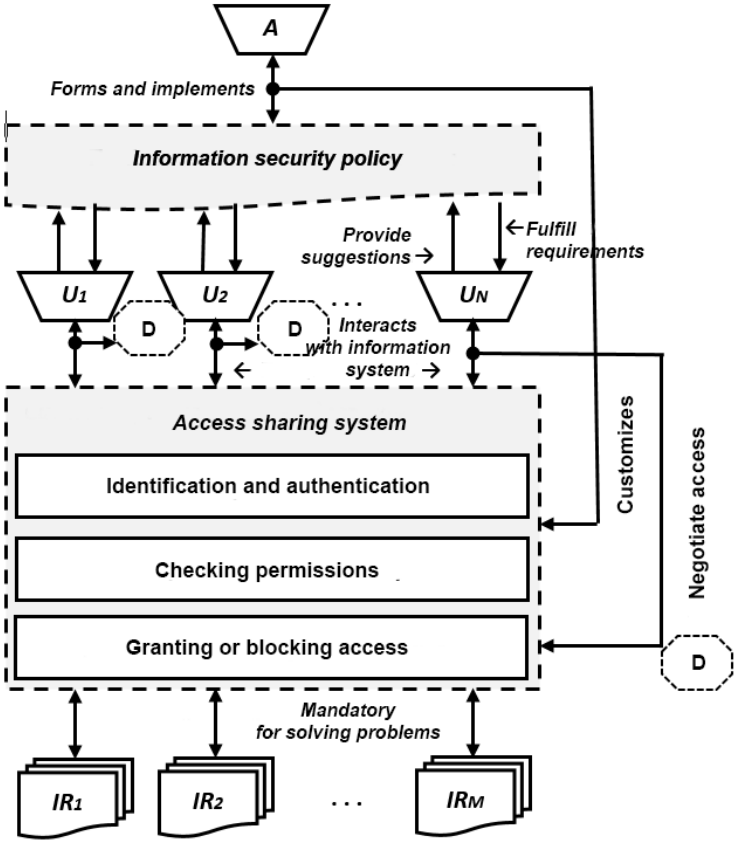

Figure 2: Ontological model of partially decentralized security systems in protected IS

In this model, the management of the central segment of the network still plays a crucial role in organizing and ensuring security. However, unlike in the previous case, the owner U_i set of information resources $\Omega_i = \{IR_{i1}, IR_{i2}, \dots, IR_{ip}\}$ acquire the authority to coordinate access to them by other users of the information system and to provide proposals for the formation of ISP.

Obviously, we have

$$\bigcup \Omega_i = \{IR_1, IR_2, \dots, IR_M\}, where\ \Omega_i \cap \Omega_j = \emptyset \text{ для } i \neq j. \quad (1)$$

Let us call a two-row table the descriptor of data belonging to their owners, the upper row of which is the user number of the IS, and the lower row is the set of information resources corresponding to it

$$D_s = \begin{pmatrix} 1 & 2 & \dots & N \\ \Omega_1 & \Omega_2 & \dots & \Omega_N \end{pmatrix}. \quad (2)$$

Based on the ownership descriptor, security management should form access matrices and markers of the owners of folders and data files for the combined matrix—mandate access demarcation system—MADS. MADS must contain the Resource's Owner Unique Number (RWUN) and the resource's confidentiality code—*CC*. For example, $CC = 0$ may indicate that the resource can be available to any identified and authenticated user of the system, $CC = 1$ may indicate certain restrictions on the use of the resource, etc.

Building a mechanism for delimiting access is based on applying cryptographic transformations of information. For this purpose, each file transferred to the single database of the information system is encrypted using an approved block cryptographic algorithm $E_k(M)$ in ECB (Electronic Codebook) mode [17] using a key file generated by the owner k.

The secret distribution procedure [17, 18] between interested parties of the information system is used to decrypt files. The file owner securely stores the key and never circulates it publicly on the network. Next, we will consider the mathematical foundations of the proposed secret distribution mechanism.

3. Mathematical Principles of Secret Distribution Procedure

Let us formulate some necessary mathematical propositions to substantiate the proposed remote distribution procedure.

Statement 1. Let the system of linear equations be given

$$\begin{cases} \bar{\beta}_1 = \bar{k} \oplus \bar{\alpha}_1 \\ \dots\dots\dots \\ \bar{\beta}_s = \bar{k} \oplus \bar{\alpha}_s \end{cases}, \tag{3}$$

where are binary vectorsαi, $\bar{\alpha}_i, \bar{\beta}_i, \bar{k} \in V_2^n,\ i = \overline{1,s},\ V_2^n$ is vector space of dimension n over a field of two elements. Here and further, the operation $\oplus$ means coordinate-by-coordinate addition of vectors modulo 2 (exclusive OR). If there is equality

$$\bar{\alpha}_1 \oplus \dots \oplus \bar{\alpha}_s = \bar{0}, \tag{4}$$

where $\bar{0}$ is a vector, all coordinates of which are equal to zero, and the condition is fulfilled

$$\bar{\alpha}_{i_1} \oplus \dots \oplus \bar{\alpha}_{i_m} \neq \bar{0}, \tag{5}$$

where $m < s$ and the elements of the index set $\{i_1, \dots, i_m\}$ pairwise do not coincide, then in the case of an odd s vector $\bar{k}$ is uniquely calculated by expression

$$\bar{k} = \bar{\beta}_1 \oplus \dots \oplus \bar{\beta}_s. \tag{6}$$

In the case of a doubles, the result of the addition in (4) is equal to 0.

The conclusion of the statement is easy to prove by adding equations in the system (3).

Vectors from the set $\{\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_s\}$ will be called masks of the secret parameter (key) $\bar{k}$.

Statement 2. If in the system of equations (3), the components of vectors $\bar{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{in}), i = \overline{1,s}$ have a random uniform distribution, i.e.

$$P(\alpha_{ij} = 1) = P(\alpha_{ij} = 0) = 0.5, for\ \forall\ i,j \tag{7}$$

and do not depend on $\bar{k}$, then the components of the vectors $\bar{\beta}_i = (\beta_{i1}, \dots, \beta_{in}), i = \overline{1,s}$ also have a random uniform distribution

$$P(\beta_{ij} = 1) = P(\beta_{ij} = 0) = 0.5, for\ \forall\ i,j. \tag{8}$$

Indeed, the probability that some component $\beta_{ij} = 1$ is equal to

$$\begin{gathered} P(\beta_{ij} = 1) = 1 - P(\beta_{ij} = 0) = P(k_j \oplus \alpha_{ij}) = 1 = \\ P(\alpha_{ij} = 0) \cdot P(k_j = 1) + P(\alpha_{ij} = 1) \cdot P(k_j = 0) = \\ 0.5 \cdot P(k_j = 1) + 0.5 \cdot P(k_j = 0) = 0.5 \cdot \left(P(k_j = 1) + P(k_j = 0)\right) = 0. \end{gathered} \tag{9}$$

Statement 3. If, under the conditions of statements 1 and 2, binary vectors $\{\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_s\}$ are chosen with equal probability at random from the vector space V_2^n, i.e.

$$P(\bar{\alpha}_i = \bar{\gamma}) = 2^{-n}\ for\ \forall\ \bar{\gamma} \in V_2^n,\ i = \overline{1,s}, \tag{10}$$

then each equation

$$\bar{\beta}_i = \bar{k} \oplus \bar{\alpha}_i, for\ \ \forall i = \overline{1,s} \tag{11}$$

specifies a perfect cipher, and (3) determines the distribution of the secret key $\bar{k} \leftrightarrow \{\bar{\beta}_1, \bar{\beta}_2, \dots \bar{\beta}_s\}$ among the community of s users, and (6) establishes the secret key recovery rule.

Recall that according to [16] , when random variables A, K, B take the value from V_2^n, and the reflection $E(K,A) = B: V_2^n \times V_2^n \to V_2^n$ is bijective for any fixed value A, then it $E(K,A)$ is called a perfect cipher if the equality holds:

$$P(K) = P(K/B) \text{ для } \forall\ K. \tag{12}$$

This means that guessing the value of the secret K does not depend on whether we know the corresponding value of B or not.

Note that according to the definition of conditional probability [19] holds

$$P(K,B) = P(K) \cdot P\left(B/K\right) = P(B) \cdot P\left(K/B\right). \quad (13)$$

Proceeding from (11) and (13) based on the approach [20], we have

$$P(K,B) = P(K) \cdot P\left(B/K\right) = P(K) \cdot P(B \oplus K) = P(K) \cdot P(A) = P(K) \cdot 2^{-n}. \quad (14)$$

From the last expression and based on (13)

$$P\left(B/K\right) = P(K,B)/P(K) = 2^{-n}. \quad (15)$$

Bayes' theorem [19] we have

$$P\left(K/B\right) = \frac{P(K) \cdot P\left(B/K\right)}{P(B)} = \frac{P(K) \cdot P\left(B/K\right)}{\sum P\left(\bar{k}\right) \cdot P\left(B/\bar{k}\right)} = \frac{P(K) \cdot 2^{-n}}{2^{-n} \cdot \sum P\left(\bar{k}\right)} = P(K). \quad (16)$$

In the last expression, the sum is calculated over all possible values of the secret parameter $\bar{k}$.

Thus, regardless of the probability distribution of the random variable *K*, Shannon's condition [16] for a perfect cipher holds.

At the same time, it should be noted that condition (4) contradicts the requirement of independent selection of mask values from the general population, since

$$\bar{\alpha}_1 \oplus \ldots \oplus \bar{\alpha}_{s-1} = \bar{\alpha}_s. \quad (17)$$

But this situation should be compensated by reliable and safe storage of a full set of masks $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_s\}$.

In addition, condition (5) slightly narrows the set of different admissible sets of masks $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_s\}$, which is of minor importance from the point of view of security in the case of sufficiently large n. It is easy to see that the number of checks N_p condition (5) is evaluated as

$$N_p = \sum_{m=2}^{s-1} C_s^m = \sum_{m=0}^{s} C_s^m - C_s^0 - C_s^1 - C_s^s = 2^s - s - 2. \quad (18)$$

In particular, Table 1 shows the calculated values N_p for really applicable values.

Table 1

Number of checks N_p conditions (5)

Method	$s = 3$	$s = 5$	$s = 7$	$s = 9$	$s = 11$
N_p	3	25	119	501	2035
Identification sessions	3	10	21	36	55

In particular, in the case of length $n = 128$ binary key $\bar{k}$ their total number is $2^{128} \approx 10^{37}$, at the same time $s = 11$ is the number $N_p = 2035 < 10^4$.

Also, condition (5) can be somewhat simplified by applying the condition $\bar{\alpha}_i \neq \bar{0}$, for $\forall i = \overline{1,s}$.

Note that in the event of an increase in the number of parties to the distribution of the secret s the number of party identification sessions is rapidly increasing, which increases the total time of the consumer's access to the necessary information resource, and this can significantly affect the responsiveness of the information system as a whole to emergencies.

4. Construction Mechanism of Access Distribution based on Secret Distribution

Taking into account the fact that the number of secret sharing participants s must be an odd number, considering the complexity of communications in overloaded systems, and based on the roles of participants in information exchange, it is suggested to choose the value of $s = 3$.

Namely, it is advisable to define the following roles: the security administrator of the central network segment *A*, the owner of the information resource *B*, and the consumer of resource *C* (Fig. 3).

If necessary, for some systems, the number of different roles can be increased to $s = 5$, in the case of connecting additional categories of control in state systems.

A separate file encryption key and a corresponding set of key masks $\{\bar{\alpha}_{Aj}, \bar{\alpha}_{Bj}, \bar{\alpha}_{Cj}\}$ that meet conditions (4), (5), (7), and (10) are generated randomly [21] for each confidentiality code CC_j.

Formed parts of the secret $\bar{k}_j \to \{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\}$ using standard cryptographic protocols are sent by the owner to the administrator and the consumer. In Fig. 3, this transmission is shown by dashed lines. Solid lines show requests - responses sent by the participants of the information exchange to each other, in particular, within the framework of identification and authentication protocols.

After the distribution of parts of the secret, the need for their complete set $\{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\}$ is lost. In order to ensure the security of the proposed scheme, this set must be destroyed. In case of accidental loss of a single part or suspicion of its compromise, a new set of parts must be generated and distributed.

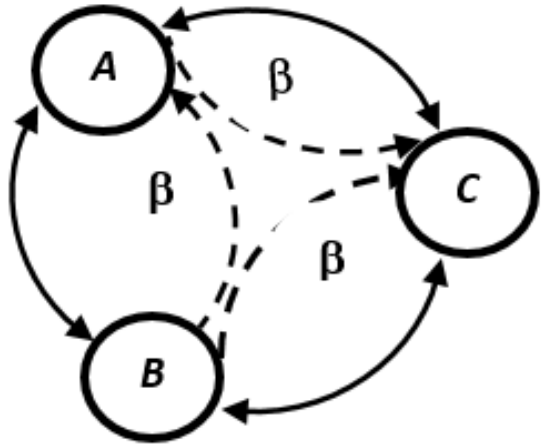

Figure 3: Interaction graph "administrator—owner—consumer"

Table 2 shows the main steps of the access delimitation procedure based on secret distribution. As a result of the procedure, the consumer gets an opportunity to recover the key $\{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\} \to \bar{k}_j$ and decrypt the desired resource corresponding to the privacy code $CC = j$.

As a result of the relevant procedures, each user forms his access matrix $\|\bar{\beta}_{ij}\|$, the size of which is determined by the number of users in the information system and the number of different privacy codes.

Table 2
Step-by-step procedure for delimiting access

	Role		
	Administrator	Owner	Consumer
1	• Participates in identification and authentication procedures • Defines the unique number of each data owner • Forms a Ds descriptor based on file registers • Forms an access matrix	• Participates in identification and authentication procedures • Creates a file registry and provides it to the administrator • Defines the privacy code for the files being created • Creates a token of the owner of folders and data files • Matches requests and handle • Generates keys in some different *CC* codes	• Participates in identification and authentication procedures • Forms a request for access to a specific category of files of the owner
2	• Receives parts of the secret using a secure protocol • Makes adjustments to the access matrix	• Encrypts and transfers files to IS • Forms masks and secret parts • Sends parts of the secret to other roles	• Receives parts of the secret using a secure protocol • Gets access to the content of the encrypted resource thanks to the provided parts of the secret
3	• Receives reports on the destruction of part of the secret	• Receives reports on the destruction of part of the secret • Safely stores keys and secret parts	• Destroys the decrypted file, key, and parts of the secret received from the administrator and owner of the resource • Informs about the execution of destruction

A prerequisite for the security of the proposed decryption procedure is the destruction of the corresponding decryption key $\bar{k}_j$ and decrypted files from the consumer immediately after the end of the processing session. In this sense, the security of the procedure is facilitated by the use of hardware and software cryptographic modules, which exclude the possibility of unauthorized access to the downloaded parts of the secret and keys [22].

Note that, according to the procedure, the security administrator never receives part of the user's $\bar{\beta}_{Cj}$ secret, which according to (5), excludes his ability to decrypt the corresponding files and gain access to their contents. Since only the content part of the files is subjected to this encryption, and its attributes are not changed, it does not affect their overwriting or archiving procedures.

The specified feature of the proposed mechanism of access delimitation also solves the problem of information systems inspection for state control over the state of information protection since the persons who carry out the inspection (audit) of the system do not get access to the content of information resources.

5. Conclusions and Prospects for Further Research

As part of the study of the project of building a network of situational centers as a block algorithm for data encryption in the access demarcation system, the use of reliable cryptographic algorithms defined by the national standard D STU 7624:2014 [23] and the international standard AES [24] in the software implementation of cryptographic modules was tested key lengths of 256 bits. Both implementations had sufficient speed. Further research is planned to be directed to develop methods for reducing data processing delay time associated with the implementation of key and key mask generation procedures, as well as data encryption.

6. Acknowledgment

The authors thank Anatoliy Morozov, Academician of the National Academy of Sciences of Ukraine, for helpful advice and research support.

5. References

[1] H. M. Hulak, I. S. Skeeter, E. G. Hulak, Methodological principles of creation and functioning of the cyber security center of the information infrastructure of nuclear energy facilities. Electronic professional scientific publication “Cybersecurity : education, science, technology,” vol. 4, no. 12, 172–186, 2021.

[2] I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring subsystem for wireless systems based on miniature spectrum analyzers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, 2018. https://doi.org/10.1109/infocommst.2018.8632151.

[3] V. Buriachok, V. Sokolov, P. Skladannyi, Security rating metrics for distributed wireless systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 222–233, 2019.

[4] Kipchuk, F., et al. Investigation of Availability of Wireless Access Points based on Embedded Systems. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019. https://doi.org/10.1109/picst47496.2019.9061551

[5] W. Xiong, R. Lagerstrom, Threat modeling—a systematic literature review, Computers & Security, vol. 84, 53–69, 2019.

[6] W. Xiong, et al., Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix, Software and Systems Modeling, 2021.

[7] R. Abdunabi, An access control framework for mobile applications, Dissertation, Colorado State University, https://mountainscholar.org/handle/10217/78814, 2013.

[8] Y. Khlaponin, et al., Functions systems protection information and cyber security critical informative infrastructure, Electronic professional scientific edition Cyber security: education, science, technology, 3(15), 124–134, 2022. https://doi.org/10.28925/2663-4023.2022.15.1241341

[9] D. A. Kakhun, Steps towards adaptive situation and context-aware access: A contribution to the extension of access control mechanisms within Pervasive Information Systems, Doctoral thesis, Institut de Recherche en Informatique de Toulouse—UMR 5505 CNRS, http://www.theses.fr/2012TOU30072, 2012.

[10] ISO/IEC 27000, “Information technology - security techniques – information security management systems - overview and vocabulary” https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en, 2018.

[11] NIST, Framework for improving critical infrastructure cybersecurity, ver. 1.1, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] American National Standards Institute, “American National Standard for Information Technology—Role Based Access Control”, ANSI INCITS 359, 2004.

[13] A. Y. Chadov, Development of requirements for a decentralized access control system. Issues of information protection, no. 3, 13–16, 2018.
[14] A. Y. Chadov, Description of the formal model of the decentralized access control system, Complex information protection: materials of the XXV scientific and practical conference, Sept. 15–17, 115–121, 2020. https://www.okbsapr.ru/library/publications/opisanie-formalnoy-modeli-detsentralizovannoy-sistemy-razgranicheniya-dostupa1/
[15] A. A. Hrusho, E. E. Tymonina, Theoretical bases of information protection, Yachtsman, 1996.
[16] K. Shannon, The theory of communication in secret systems, Works on the theory of information and cybernetics, ed. by R.L. Dobrushyna and O.B. Lupanova, 1963.
[17] B. Schneier . Applied cryptography: protocols, algorithms and source code in C, 2nd edition . Dialectic-Williams, 2017. ISBN: 978-5-9908462-4-1
[18] L. Harna, et al., Realizing secret sharing with general access structure, Information Sciences, vol. 367–368, 209–220, 2016.
[19] H. Cramér. Mathematical Methods of Statistics, Princeton University Press, 1999. ISBN 978-0691005478
[20] V. M.. Fomichev Methods of discrete mathematics in cryptology, Dialog-MYFI, 2010.
[21] H. Hulak, L. Kovalchuk, Different approaches to determining random sequences, Scientific and technical collection “Legal, regulatory and metrological support of the information protection system in Ukraine,” vol. 3, 2001, 127–133.
[22] I. D. Horbenko, Y. I. Horbenko, Applied cryptology: Theory. Practice. Application. Monograph. FORT, 2012.
[23] R. Oliynykov, et al., A New Encryption Standard of Ukraine: The Kalyna Block Cipher. IACR Cryptol, 2015.
[24] A. Biryukov, D. Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256. Advances in Cryptology, ASIACRYPT, vol. 5912, 2009. https://doi.org/10.1007/978-3-642-10366-7_1.