

# Concept of Joint Functioning of Access Control Systems

Mykhailo Strelbitskyi, Valentyn Mazur, Evgenii Prokopenko, Roman Rachok, and Dmytro Mul

*Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine*

<https://doi.org/10.26636/jtit.2023.164322>

**Abstract** — Modern integrated information and telecommunication systems are upgraded on a continuous basis. Such systems contain both new and old components. The approaches to developing individual components of access control systems are different in the majority of cases. As a rule, modernization of outdated but efficient systems that have been operating without any failures for long periods of time is economically unfeasible. Such an approach requires that different subsystems function based on shared data. This necessitates the coordination of various access control systems in order to ensure proper information security levels. This article examines how joint functioning of various versions of access control systems deployed in IT and telecommunication spheres may be achieved at the stage of their modernization. Potential ways in which information flows may bypass the security policies of one of the access control systems concerned are determined. The authors discuss traditional access control models. For role-based and thematic access control models, specific hypotheses are formulated to comply with security policies when different versions of access control systems work together. The structure of the model assuming that different versions of access control systems operate jointly has been developed. Based on the model, the necessary and sufficient conditions are determined under which unauthorized information flows are prevented. The security theorem for the joint functioning of different versions of access control systems is presented and proved. The results of the study showed that the methodological basis for coordinating access control models applicable to information and telecommunication systems undergoing modernization consists in observing, separately, the equality of information flows between shared objects in each of the versions of the access control systems. The approaches developed in this article can be extended to combined access control systems.

**Keywords** — access control model, concept, information and telecommunication system, modernization.

## 1. Introduction

Modern information and telecommunication systems (ITS) have a large number of subsystems (components) that are distributed across various geographical locations. A special feature of such systems is the requirement to operate in real time, and even short-lasting periods of unavailability or shut-downs may lead to serious damage on a nationwide scale. One of the ways in which reliability of such systems may be ensured is to guarantee the security of information flows. Information security can be described using such properties as: confidentiality, integrity, and availability [1], [2]. Compliance with these properties is ensured in ITS solutions,

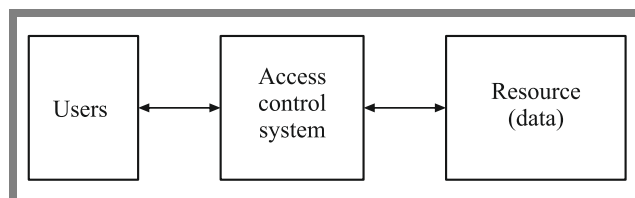
in particular, by the access control system allowing users to access or prohibiting them from accessing a given organization's resources [3]. Many studies focused on analyzing existing access control systems. The traditional access control models are compared in Table 1 [4].

**Tab. 1.** Comparison of traditional access control models.

Criteria	DAC	MAC	RBAC	ABAC
Principle of least privilege	–	–	+	+
Dynamic behavior	–	–	–	+
Safety of models	–	+	+	+
Separation of duties	–	–	+	+
Capability delegation	+	–	–	–
Configuration flexibility	+	–	+	–
Auditing	+	+	+	+

where: DAC – discretionary access control, MAC – mandatory access control, RBAC – role-based access control, and ABAC – attribute-based access control.

Other authors considered theoretical aspects of the process of establishing information security models [4], [5] and examined the formation of combined models based on the traditional components [4]–[7]. However, all authors take into consideration one paradigm of the access control system modeling process, namely whether the system is of the traditional or combined variety (Fig. 1).



**Fig. 1.** Typical application of access control systems.

Some of the ITS that are in use currently were developed a long time ago. The integrated ITS of the State Border Guard Service of Ukraine may serve as a good example here. It consists of numerous subsystems [8] and was created by integrating individual ITS data sets into a higher-level data structure. The adoption of such an approach was conditioned

by completely different requirements that needed to be satisfied (Fig. 2).

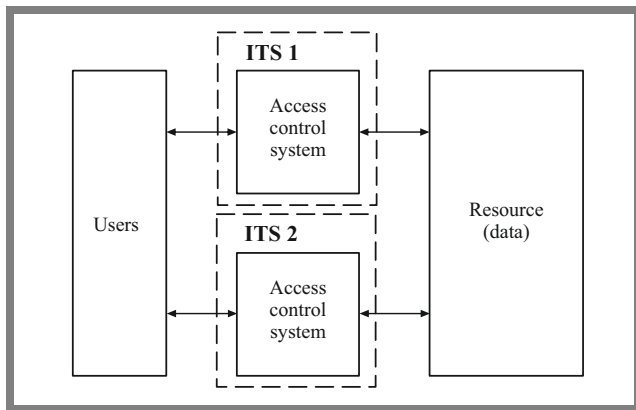


Fig. 2. Typical application of an access control system.

The development of access control systems (ACS) operating within various ITS that interact with one another as part of the same supersystem can be carried out both according to the same and different models of access differentiation. While upgrading the solution, the problem of coordinating various components needs to be taken into consideration, thus requiring that a concept ensuring their joint operation be designed. Unfortunately, information security models do not provide for joint functioning with other similar models in a common data field, and such a scenario may be encountered while performing modernization work. All models cover the functioning of a single system (security monitor, security core, etc.) and ensure compliance with its security policy. Recently, separate methods for coordinating access differentiation have been developed (as described in [9]–[11]), but a general approach has not been formed yet.

## 2. Aim of the Article

This paper analyzes the joint functioning of existing information security and focuses on the stage of modernization of specific information and telecommunication systems in order to:

- determine potential information flows bypassing one of the security models,
- determine hypothetical conditions under which their joint functioning is possible,
- define a concept for their safe joint functioning.

## 3. Joint Operation of Access Control Models

### 3.1. General Theoretical Provisions

It is not possible to define an ITS security policy which ensures the reliability of the information flow without relying on information security models serving as a formalized description of the basic principles of the solution to be adopted. Only with the help of formal models, the system’s security

may be proven based on mathematical conditions. Security models define the basic principles of security policies, are used in their design and in the creation of technological solutions offering suitable levels of information security. In the context of ITS upgrades, if information security functionalities are implemented, in advance, in both the old and new versions of the software in order to eliminate conflicts caused by differences in models, it is necessary to perform their verification. So far, a number of strategies for modeling the behavior of security systems have been proposed in the literature [12]–[16]. Furthermore, each known model operates based on three elements: subject, object, and operations the former may perform on the latter (reading, writing, deletion, etc.). To represent an ACS, three sets of elements need to be defined:

- objects  $\{O\}$  – terminals, network nodes, communication channels, external devices, applications, volumes, directories, files, records, recording fields,
- subjects  $\{S\}$  – users or processes running on their behalf, i.e. administrators, applications, processes, terminals,
- operations  $\{\Omega\}$  – sequences of the subject’s actions concerning the object (information flow).

Based on such an assumption, an ACS is an object of set-theoretic calculus, i.e. a Cartesian product of the form:  $S \times O \times \Omega$ . This means that access control rules will be described by an information security model, the results of which will cause operation  $\omega_i$  performed by outside  $s_i$  and related to  $o_i$  being permitted or prohibited.

If the old version of the ACS is represented as:  $S_1 \times O_1 \times \Omega_1$ , and the new version as:  $S_2 \times O_2 \times \Omega_2$ , then for the case where such an expression is true:

$$(S_1 \cap S_2 = \emptyset \wedge (O_1 \cap O_2 = \emptyset) \wedge (\Omega_1 \cap \Omega_2 = \emptyset) \vee (S_1 \setminus S_2 = \emptyset) \wedge (O_1 \setminus O_2 = \emptyset) \wedge (\Omega_1 \setminus \Omega_2 = \emptyset)). \quad (1)$$

Equation (1) assumes that there are no conflicts between the new and old versions of the ACS in ITS. Other cases are not included in the scope of the research.

The studied contradictions occur if the result of taking the Cartesian difference between  $S_1 \times O_1 \times \Omega_1$  and  $S_2 \times O_2 \times \Omega_2$  is different from  $\emptyset$  subset  $S_R \times O_R \times \Omega_R$  which, generally, will consist of components of both generations of the ACS of a heterogeneous system. The elements of this set form a common field through which the interaction of different components of the ITS is carried out. Let us analyze what properties the ACS structure should have and what requirements it should meet  $S_R \times O_R \times \Omega_R$  to eliminate inconsistencies that lead to the possibility of a violation of the security policy or the occurrence of a hidden information flow.

By hidden information flow, we mean a mechanism by which information may transferred between various entities within the ITS, bypassing the access control rules (policies).

In this article, the following models are selected in order to study the joint functioning of different computer system security models: discretionary, role-based, mandated, and thematic access control. Information flow security-based and

subject-oriented models used in isolated software environments are taken into consideration as well.

### 3.2. Discretionary Access Control Models

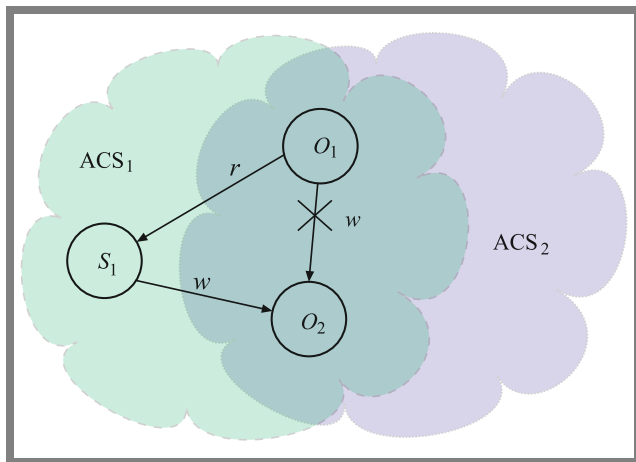
The known discretionary access control models, i.e. Harrison-Ruzzo-Ullman, typed access matrices, Take-Grant, and extended Take-Grant varieties, operate with an access matrix  $M[s, o]$ , where rows correspond to subjects, and columns relate to system objects. The cells define the rights that subject  $s$  has to access object  $o$  [5].

In a scenario in which different versions of these models work together, two situations may take place in which a security policy violation may occur. First, the values of access rights of different versions of ACS for familiar entities and objects are different:

$$\exists s_i, \exists o_j \text{ when } M_1[s_i, o_j] \neq M_2[s_i, o_j],$$

where  $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$ .

In this case, it is a clear violation of the security policy applying to the subject and concerning a given object. A given operation is allowed in one version of the ACS and is prohibited in the other. In the second case, the values of access rights of different ACS versions for familiar entities and objects are the same, i.e.  $M_1[s_i, o_j] = M_2[s_i, o_j]$ , for  $\forall s_i \in S_1, \forall s_i \in S_2, \forall o_j \in O_1, \forall o_j \in O_2$ . At a given moment, the presence of entities and objects not included another ACS version means that information flows may bypass the security policy of one of the versions (Fig. 3).



**Fig. 3.** A variant in which information flow bypasses the security policy of one of the versions of the access control system.

Figure 3 shows one element (subject  $S_1$ ) present in the first ACS and absent another  $ACS_2$ , through which the information flow is carried out, bypassing the access matrix  $M_2[s, o]$ .

So, when determining the “bypass” data stream, it is necessary to consider all objects and subjects of the system.

### 3.3. Role-based Access Control Models

Role-based access control models are a further development of discretionary access control policies. The difference is that access rights assigned to specific system entities are

combined to form groups with the same rights. The said groups are determined taking into account the specifics of their functional tasks within the system [5]. Thus, when two ACS solutions relying on the principle of role-based access control work together, an information flow may bypass one of the ACS versions in the same way as it was the case with discretionary access control.

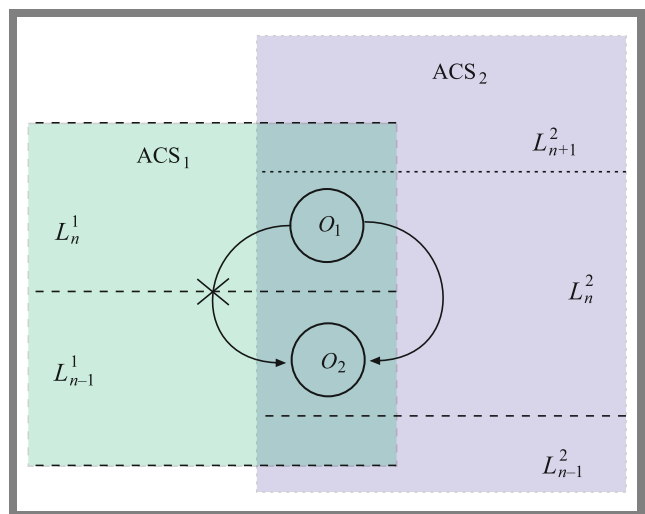
However, equality of rights for each role is not mandatory in the context of the joint functioning of different ACS versions. In this case, if there is an old role  $r_i^1$  and a new ACS  $r_2^j$  under which the rights to object  $o_k$  are set (if those rights are different, then a clear violation of the security policy of one of the ACS versions is noticed. This is due to the fact that a user performs an operation with role  $r_i^1$  concerning an object that one ACS version considers forbidden in role  $r_2^j$  of a different version or vice-versa.

Such a hypothesis has been advanced after researching information flows in scenarios involving joint functioning of different versions of role-based access control systems. To comply with the security policy and ensure coordinated operation of both versions of role-based access control systems, equal sets of access rights for roles of different versions of ACS for combined objects are necessary and sufficient.

### 3.4. Mandated Access Control Models

The classical Bell-LaPadula model, the secure transition model, the military message system model, the low-watermark policy, the Bib integrity model, and others allow to analyze the conditions under which information flows from objects with a higher level of privacy to the ones with a lower level of privacy are impossible [5]. The occurrence of an unauthorized information flow in one of the cooperating versions of ACS solutions is possible if:

- there are inconsistencies in the lattices of the privacy levels of ACS objects which may lead to an information flow prohibited in one of the versions (Fig. 4),



**Fig. 4.** Information flow bypassing the security policy of one of the ACS versions in a scenario in which the lattices do not match the privacy levels.

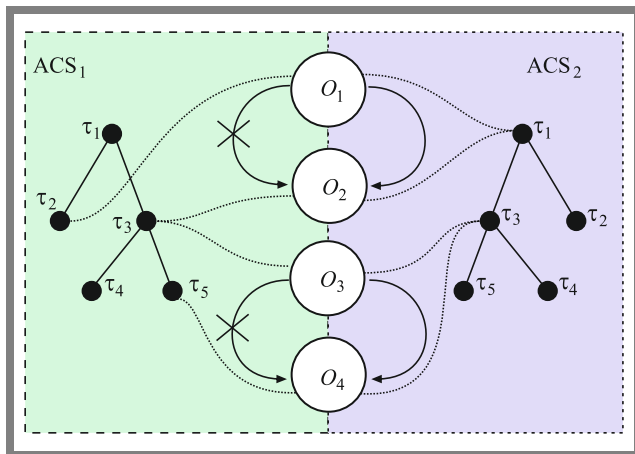
- there is a mismatch between access matrices  $M[s, o]$ .

It is worth noting that the existing regulatory framework clearly defines the grid of privacy levels of specific objects. Hence, the occurrence of an unauthorized information flow in the first method is rare. At the same time, the second method may be implemented in a manner similar to the discretionary access control model.

### 3.5. Thematic Access Control Models

Thematic access control models operate with a thematic hierarchical classifier (rubricator) which includes a finite set of thematic headings on which a partial order is established and determined by the root tree. Many entities in thematic access control models  $X = S \cup O$  are classified based on their mapping to a set of multi-rubrics defined in the root tree of a hierarchical rubricator.

The occurrence of an unauthorized information flow in one of the versions of thematic access control systems during their joint operation is possible if the topics of the system entities do not match (Fig. 5).



**Fig. 5.** Information flow in a scenario in which thematic hierarchical classifiers do not match in different versions of access control systems.

As an example, two cases of contradictions in information flows in different versions of thematic access control systems with four shared objects are:

- in the first ACS<sub>1</sub> objects  $o_1$  and  $o_2$  are located in entities that are not comparable in terms of their subject matter. Consequently, such flows are prohibited. At the same time, in ACS<sub>2</sub>, these items are related to the same topic, so information flow between them is allowed;
- in the second ACS<sub>1</sub> object  $o_3$  is located in an entity with a broader theme and  $o_4$  with a narrower one, so this flow is prohibited. While in ACS<sub>2</sub> these items are on the same topic, the information flow between them is allowed.

To comply with the security policy when coordinating both thematic access control arrangements, the hierarchical equality of thematic classifiers for objects shared in different ACS versions is necessary.

### 3.6. Security-based Information Flow Models

Non-withdrawal and non-interference models are based on the distribution of all potential flows between objects within the system into two non-intersecting sets, i.e. authorized and unauthorized flows [5]. Thus, the main task of the security system relying on the security-based information flow model is to prevent the occurrence of unauthorized information flows. This information flow segregation model is mainly based on other security policies, such as discretionary or mandated access control. Thus, when different versions of access control systems relying on the security-based information flow model work together, a violation of security policies is possible. For example, such a breach may occur if the privacy levels do not match or if the access matrices in other types of security policies are not consistent.

### 3.7. Subject-oriented Model of an Isolated Software Environment

The subject-oriented model of an isolated software environment is similar to the information flow security model and operates with two non-overlapping sets: streams that represent unauthorized access and streams that represent legal (authorized) access. It is worth noting that this model does not specify any known security policies. The security policy describes only the criterion for dividing all information flows into the two subsets. Thus, the subject-oriented model of an isolated software environment is invariant to the security policy adopted in the system and has its disadvantages when different versions of the access control system work together.

## 4. Methodology for Coordinating Access Control Models

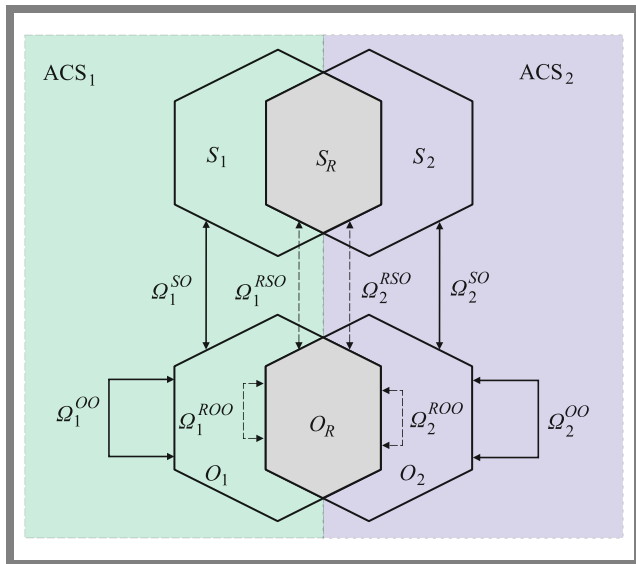
According to [17], threats related to unauthorized access to information constitute a privacy violation. That is why research focusing on access control systems aims to ensure the confidentiality of information. The “information threat” concept requires, in essence, that a subject-object model of a computer system be used, as the need exists for the subject to be an element of the system that becomes acquainted with the information and an object – a material data medium. In the absence of at least one of those two components, we can no longer talk about violating confidentiality. Moreover, it is necessary to introduce a third concept – the flow of information from the object to the subject, since the absence of such flow offers no threat to confidentiality. There are different approaches to defining subjects, objects, and information flows. This work is based the following definitions:

- A subject is a representation of a physical user of a computer system that is created during the user’s entry into the system and is fully characterized by its context (alias, identification code, permissions, etc.);
- An object is a computer system resource that is managed by a set of security tools and is characterized by specific attributes and behaviors;

– Information flow is a transfer of information from one object of a computer system to another.

In order for a confidentiality threat to be present, the concept of “familiarization” of the subject with the information contained in the object needs to be taken into consideration as well. Familiarization consists in the user becoming acquainted with the process and with the information contained in the object. It is worth noting that according to the definitions adopted, a confidentiality violation occurs when the user has read the information and the respective process has received it.

When developing or upgrading an ITS, the developer implements the ACS based on proven security policies and ensures information protection based on the criteria established by the customer. At the same time, the upgraded components are implemented in the system in stages and over a certain period of time during which the old version of the ISS functions simultaneously with the upgraded ACS. Such an approach leads to uncontrolled actions concerning individual objects being undertaken by one of the versions of the ACS. This means that information flows may emerge that comply with the security policy framework and ones that fail to do so.



**Fig. 6.** Model of a scenario in which different versions of access control systems operate jointly.

In general, the modernization period is characterized by the occurrence of information flows that are not allowed in one of the versions, thus leading to a violation of the confidentiality of information. The confidentiality requirement will be met when equal information flows are ensured for common subjects and objects of the system in both versions. To prove the safety theorem for matching different versions of ACS, we describe a structural model of their joint functioning (Fig. 6):

- $S_R = S_1 \cap S_2$  are common subjects for both versions,
- $O_R = O_1 \cap O_2$  are shared objects for both versions,
- $\Omega_1^{SO}, \Omega_2^{SO}$  are information flows between ACS subjects and objects,
- $\Omega_1^{RSO}, \Omega_2^{RSO}$  are information flows between familiar entities and ACS objects,

$\Omega_1^{OO}, \Omega_2^{OO}$  are information flows between ACS objects,  
 $\Omega_1^{SOO}, \Omega_2^{SOO}$  are information flows between shared ACS objects.

In addition:

$$\Omega_1^{RSO} \subseteq \Omega_1^{SO} \subseteq \Omega_1, \Omega_2^{RSO} \subseteq \Omega_2^{SO} \subseteq \Omega_2,$$

$$\Omega_1^{ROO} \subseteq \Omega_1^{OO} \subseteq \Omega_1, \Omega_2^{ROO} \subseteq \Omega_2^{OO} \subseteq \Omega_2.$$

Note that a violation of confidentiality or the rules of the ACS security policy is only possible if there is an unauthorized information flow between the object containing the information and the subject. Therefore, information flows between subjects are not considered in this model. Obviously, if all information flows are equal, no violation of confidentiality takes place.

Let us define a necessary and sufficient condition under which an unauthorized information flow is impossible. To this end, we will consider four degenerate variants of joint functioning of both versions of the ACS, provided that each system fully ensures the confidentiality of information following the basic models of the ACS:

- Option 1.** In the case when  $S_R = \emptyset, O_R = \emptyset$  the ACS involved do not have any common elements and function independently of each other. There are no unauthorized information flows.
- Option 2.** In the case when  $S_R \neq \emptyset, O_R = \emptyset$  the ACS only have familiar users. The presence of an object containing information prohibited from being made available to the user is a necessary condition for violating the privacy requirement. Concurrently, the ACS security policy will not allow such information to be present in an object that belongs to the user (the has access to such an object). Thus, in this case, there is no violation of confidentiality.
- Option 3.** In the case when  $S_R = \emptyset, O_R \neq \emptyset$  the ACS have only common objects. This option allows for an information flow between objects not provided for in one of the versions of the ACS, which in turn will lead to an unauthorized information flow to a particular subject. Thus, this option may violate confidentiality.
- Option 4.** In the case when  $S_R \neq \emptyset, O_R \neq \emptyset$  the ACS have common subjects and objects. This option combines the second and third cases and allows for an information flow between objects not provided for in one of the versions of the ACS. Thus, this option may violate confidentiality.

The analysis of various options concerned with the sharing of ACS elements has shown that an unauthorized information flow can only occur if there are common objects in different versions of ACS. Thus, to prevent unauthorized information flows during the joint functioning of both versions of the ACS, equality of data flows between objects shared in each of the ACS is necessary. Such an approach serves as a formulation of the security theorem for the joint functioning of different versions of ACS. The proof of the theorem is clear from the above.

It is worth noting that the developed approach is invariant to the access differentiation models themselves, which makes it possible to coordinate not only systems of the same type, but also systems built based on different access control models.

## 5. Conclusions

The study was concerned with the joint operation of various versions of access control systems that are based on security models applicable to computer systems. This article has identified potential ways of ensuring that information flows bypass the security policies of one of the versions of the access control systems involved.

Discretionary access control models rely on an access matrix and use a privacy level grid. This means that some degree of coordination is required when different versions of ACS operate together. For role-based and thematic access control models, specific hypotheses are formulated allowing to achieve compliance with the security policies applicable to the joint operation of different versions of ACS.

The results of the study showed that the methodological basis for coordinating access control models applicable to information and telecommunication systems undergoing modernization consists in observing, separately, the equality of information flows between shared objects in each of the versions of the access control systems concerned. By relying on the methodological basis developed, we will be able to continue with the development of other methods for coordinating various access control models.

## References

- [1] H. Huang, F. Shang, J. Liu, and H. Du, "Handling least privilege problem and role mining in RBAC", *Journal of Combinatorial Optimization*, vol. 30, no. 1, pp. 63–86, 2015 (<https://doi.org/10.1007/s10878-013-9633-9>).
- [2] J. Hassan *et al.*, "A lightweight proxy re-encryption approach with certificate-based and incremental cryptography for fog-enabled e-healthcare", *Security and Communication Networks*, vol. 2021, Article ID 936824, 2021 (<https://downloads.hindawi.com/journals/scn/2021/9363824.pdf>).
- [3] H. Zhang, J. Wang, and J. Chang, "An access control model for multilevel security in multi-domain networking environments", *Proceedings of the 9th International Conf. on Modelling, Identification and Control (ICMIC)*, pp. 809–814, Kunming, China, 2017 (<https://doi.org/10.1109/ICMIC.2017.8321566>).
- [4] M.U. Aftab, A. Hamza, A. Oluwasanmi, X. Nie, M.S. Sarfraz, D. Shehzad, Z. Qin, and A. Rafiq, "Traditional and hybrid access control models: A detailed survey", *Security and Communication Networks*, vol. 2022, Article ID 1560885, 2022 (<https://doi.org/10.1155/2022/1560885>).
- [5] S. Pierangela and S. de Capitani di Vimercati, "Access control: Policies, models, and mechanisms", in *International School on Foundations of Security Analysis and Design*, R. Focardi and R. Gorrieri, Eds. LNCS, vol. 2171, pp. 137–196. Berlin, Heidelberg: Springer, 2000 ([https://doi.org/10.1007/3-540-45608-2\\_3](https://doi.org/10.1007/3-540-45608-2_3)).
- [6] D.J. Bokefode, A.S. Ubale, S.S. Apte and G.D. Modani, "Analysis of DAC MAC RBAC access control based models for security", *International Journal of Computer Applications*, vol. 104, no. 5, pp. 6–13, 2014 (<https://doi.org/10.5120/18196-9115>).
- [7] A.K. Malik, N. Emmanuel, S. Zafar, H.A. Khattak, B. Raza, S. Khan, A.H. Al-Bayatti, M. O. Allassafi, A. S. Alfakheeh, and M. A. Alqarni,

"From conventional to state-of-the-art IoT access control models", *Electronics*, vol. 9, no. 10, 1693 (<https://doi.org/10.3390/electronics9101693>).

- [8] O.K. Yudin and M. A. Strelbitskiy, "Content and hierarchy of the register of information resources of the state border guard service of Ukraine", *Problems of Informatization and Management*, vol. 4, no. 56, pp. 85–91, 2016 (<https://doi.org/10.18372/2073-4751.4.13148>) [in Ukrainian].
- [9] M.A. Strelbitskiy, "Analysis of joint functioning of access differentiation models at the stage of modernization of information and telecommunication systems", *Collection of Scientific Works of Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine*, vol. 4, no. 70, pp. 276–287, 2016 [in Ukrainian].
- [10] V.V. Kuzavkov, M.A. Strelbitskiy, and V.O. Danko, "Method for harmonizing the privacy level grids of mandatory access control systems for information and telecommunication systems at the modernization stage", *Collection of Scientific Works of the Military Institute of Telecommunication and Informatization*, no. 1, pp. 56–60, 2017 ([http://nbuv.gov.ua/j-pdf/Znpviti\\_2017\\_1\\_9.pdf](http://nbuv.gov.ua/j-pdf/Znpviti_2017_1_9.pdf)) [in Ukrainian].
- [11] M.A. Strelbitskiy, "Method of coordination of access matrices of discretionary access control systems of information and telecommunication systems at the stage of modernization", *Modern Information Technologies in the Field of Security and Defense*, vol. 1, pp. 58–62, 2017 [in Ukrainian].
- [12] Y. Deng, J. Wang, J.J.P. Tsai, and K. Beznosov, "An approach for modeling and analysis of security system architectures", *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 5, pp. 1099–1119, 2003 (<https://doi.org/10.1109/TKDE.2003.1232267>).
- [13] J.E. Kobza and S.H. Jacobson, "Probability models for access security system architectures", *J. of the Operational Research Society*, vol. 48, no. 3, pp. 255–263, 1997 (<https://doi.org/10.2307/3010424>).
- [14] Ş. Bahtiyar and M.U. Çağlayan, "Extracting trust information from security system of a service", *Journal of Network and Computer Applications*, vol. 35, no. 1, pp. 480–490 (<https://doi.org/10.1016/j.jnca.2011.10.002>).
- [15] M. Fugini and G. Martella, "Acten: A conceptual model for security systems design", *Computers and Security*, vol. 3, no. 3, pp. 196–214, 1984 ([https://doi.org/10.1016/0167-4048\(84\)90041-5](https://doi.org/10.1016/0167-4048(84)90041-5)).
- [16] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments", *Computer Communications*, vol. 31, no. 18, pp. 4343–4351, 2008 (<https://doi.org/10.1016/j.comcom.2008.05.007>).
- [17] T. Carlson, "Information Security Management: Understanding ISO 17799", International Network Services Inc. (INS), Whitepaper, 2001 ([http://www.secureict.co.za/wp-content/uploads/2018/06/03\\_ins\\_info\\_security\\_iso\\_17799\\_1101-1.pdf](http://www.secureict.co.za/wp-content/uploads/2018/06/03_ins_info_security_iso_17799_1101-1.pdf)).

### Mykhailo Strelbitskiy, D.Sc.

Professor at the Department of Communications, Automation, and Cyber-security


 <https://orcid.org/0000-0001-8030-3228>

E-mail: m.strelb@ukr.net

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine

### Valentyn Mazur, D.Sc.

Professor at the Department of Border Security


 <https://orcid.org/0000-0002-3405-6200>

E-mail: vumazur154@gmail.com

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine

**Evgenii Prokopenko**

Candidate of Technical Sciences, Associate Professor at the Department of Communications and Information Systems

 <https://orcid.org/0000-0002-6825-2357>

E-mail: mydocent@gmail.com

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine

**Roman Rachok, D.Sc.**

Professor at the Department of Telecommunication and Information Systems


 <https://orcid.org/0000-0002-3283-9690>

E-mail: rrvnadpsu@i.ua

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine

**Dmytro Mul**

Candidate of Technical Sciences, Associate Professor at the Department of Communications and Informatization

 <https://orcid.org/0000-0003-2662-4770>

E-mail: dmitry.mul@gmail.com

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine