Harmonization of Systems of Discretionary Differentiation of Access to Information Systems at the Stage of Modernization

Oleksandr Yudin
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
yudin.ok8@gmail.com

Mykhailo Strelbitskyi
Bohdan Khmelnytsky National Academy of the State Border Guard Service of Ukraine
Khmelnytskyi, Ukraine
mstrelb@gmail.com

Valentyn Mazur
Bohdan Khmelnytsky National Academy of the State Border Guard Service of Ukraine
Khmelnytskyi, Ukraine
mstrelb@gmail.com

Viktoriia Ivannikova
National Aviation University
Kyiv, Ukraine
victoriia.ivannikova@gmail.com

Olha Suprun
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
o.n.suprun@gmail. com

Mykola Prysiazhniuk
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
pnn2016pnn@gmail.com

2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT) | 978-1-6654-3847-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ATIT54053.2021.9678793

***Abstract* — Integrated information and telecommunication systems operate subsystems with their own systems of access differentiation. At the stage of subsystems modernization there is a possibility to change the parameters or structure of their access differentiation systems. This fact is a prerequisite for violation of the information properties, contained in the general field of the integrated information and telecommunications system. Analysis of the existing ways of the unauthorized information flow appearance during usage of discretionary models in the access differentiation systems has shown a possibility of information properties violation. A method for harmonization of access matrices of various options of the discretionary differentiation of access systems has been developed. The security theorem of joint functioning of different options of access differentiation systems, built on the bases of a discretionary model, is formulated and proved.**

Key words — differentiation of access, discretionary model, information and telecommunication system, modernization

I. INTRODUCTION

National integrated information and telecommunication systems have a large number of subsystems that are distributed throughout the country. Such systems are usually operating in real time, and even a minor failure or shutdown can lead to the serious national losses.

Analysis of this type of systems showed a stable tendency to the increasing of risks and threats to the properties of the information, circulating in them.

These findings require constant modernization of the integrated information and telecommunications systems composite parts, which leads to the joint functioning of old, updated and new options of information and telecommunications subsystems at the general data field. At this stage of the system life cycle, there is a problem of transition to a new software and hardware platform without violation of the life cycle.

Construction of information security systems of different information and telecommunication systems, which interact as part of one supersystem, can be carried out both by the same and by the different models of access differentiation. During modernization of one of them, the problem of their harmonization appears. In some cases, the coordination is required for the systems of access differentiation (SAD) to information systems of the old and new options, which are based on the models of discretionary differentiation of access. These models lay in the basis of the information system security policy.

Security policy is a basic category in the field of information systems data protection. It is usually understood as a set of laws, rules, restrictions, recommendations, instructions, etc., which regulate the order of information processing.

Security models play a significant role during development of information systems and determination of their security level [1]. Usage of such models provides a systematic and scientifically grounded approach to the following [2]:

- selection and grounding of main approaches to the structure of information systems, which determines the ways of realizing methods, techniques and means for ensuring the properties of the information resource;
- formal confirmation of the information system security status due to the proving the security theorems of the used security policy models;
- development of a security policy formal description.

So, security models are a main component on the basis of which customers formulate requirements for the information systems security [2]. Selection of the security model, which will be used in a particular information and telecommunications system, depends on the peculiarities of its operation in the supersystem. It will also allow experts to develop methods and specifications for assessment security of the indicated information system, to certify the information system according to the requirements for the composite parts of the information resource properties.

In order to form a methodology for coordinating systems of access differentiation for information and telecommunications systems, it is necessary to develop methods for each of the known models, in particular for the discretionary model of access differentiation.

II. Analysis of the Recent Researches and Publications

There are a lot of researches, devoted to the development and investigation of the models of discretionary differentiation of access. The first papers were published in the 60th years of the last century. The most famous of them are: the ADEPT-50 model, commissioned by the Ministry of Defense of the USA [3, 4], the 5D Hartson space [3], the Harrison-Ruzzo-Ullman model [5] and others. These models operate with a discrete set of triplets "subject-flow (operation) –object".

Structure of the security policies, based on the models of the discretionary differentiation of access, does not foresees operation of joint with other systems objects and subjects, as it is possible during modernization of information systems as the part of departmental automated systems.

III. Ways of Appearance of Unauthorized Information Flows During Joint Functioning of Diferent Options of the Systems of Discretionary differentiation of Access

Security of the information, circulating in the integrated information system, is ensured by the correct formation of the security policy, based on the known, formally proved security models. Principles, laying in the bases of the security models, ground the system's ability to provide information security.

Models of the discretionary differentiation (Harrison – Ruzzo – Ullmann Model, Typed Access Matrices Model, Take – Grant Model, Extended Take – Grant model, etc.) operate with an access matrix $M[s,o]$, the rows of which correspond to subjects, columns correspond to the system's objects, and cells determine the right of subject s access to the object o [6-7].

In the case of joint operation of different options of these models, two situations can be realized, at which a violation of security policy is possible. In the first case, the access rights of various options of the system of access differentiation for common subjects and objects are different, i.e. $\exists s_i, \exists o_j$ for which $M_1[s_i,o_j] \neq M_2[s_i,o_j]$, where $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$. In this case, there is a violation of the security policy, because during realizing the operation of the subject with respect to the object, allowed by the one option of the SAD, there is a prohibition in another option or vice versa. In the second case, the access rights of different options of the SAD for common subjects 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 the same time, the existence of subjects and objects, that are not included into the SAD of another option, allows the information flow to pass over the security policy of one of the option (Figure 1).

Figure 1 shows one element (subject S_1), which is presented in the first SAD and is absent in the second one and through which the information flow is passing over the access matrix $M_2[s,o]$. It should be noted that one of the properties of information flows is their transitivity, that's why during determination of the "bypass" information flow it is necessary to take into account all objects and subjects of the system.

Therefore, ensuring of the information security in the conditions of joint functioning of different options of the SAD requires development of the method for their harmonization.

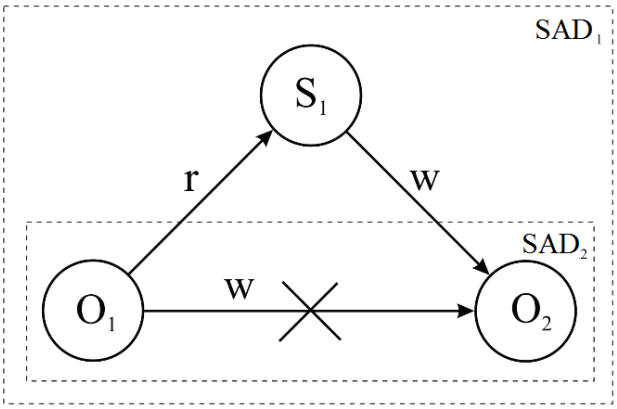

Fig. 1. Option of information flow realization passing over the security policy of one of the options of the access differentiation system

IV. Method of Harmonizing Access Matrixes of Different Options of the Systems of Discretion differentiation of Access

The method is intended for formation of the common access matrix for both options of the SAD at the stage of information systems modernization.

The essence of the method of coordinating access matrices of different options of access differentiation systems lays in the formation of the common single access matrix for both options, in which it is impossible to realize unauthorized information flow in each option of the SAD, separately (Figure 1).

Let's describe the initial data for the analytical description.

$M^{old}_{|S_{old}|\times|O_{old}|} = M^{old}[s_{old}, o_{old}]$ – access matrix of the old SAD;

$M^{new}_{|S_{new}|\times|O_{new}|} = M^{new}[s_{new}, o_{new}]$ – access matrix of the new SAD;

$M^{join}_{|S_{join}|\times|O_{join}|} = M^{join}[s_{join}, o_{join}]$ – access matrix of the common option of the SAD.

Moreover, $S_{join} = S_{old} \cup S_{new}$ and $O_{join} = O_{old} \cup O_{new}$.

Let's determine the sets of subjects and objects that are common for both options of the SAD, namely

$S_{sub} = S_{old} \cap S_{new}$ and $O_{sub} = O_{old} \cap O_{new}$.

If the elements of the access matrices of both old and new options of the SAD do not correspond to each other, it is impossible to harmonize the matrices, so the joint operation of both options of the access differentiation system will lead to the violation of the information properties. Therefore, a necessary, but not sufficient condition for the coordination of different options of the access differentiation systems, namely, their access matrices, is

$$M^{old}[s,o] = M^{new}[s,o], \forall s \in S_{sub}, \forall o \in O_{sub}. \quad (1)$$

The next step of the method is determination of the possibility to create an information flow, which is authorized in one option of the SAD and unauthorized in another one.

The initial conditions for coordination of different options of the SAD are that the security policy in each of them is formed separately correctly and does not allow violation of the information properties. Therefore, it is necessary to consider only the common part of the access matrices of different options of the SAD, namely, $M^{sub}_{|S_{sub}|\times|O_{sub}|} = M^{sub}[s_{sub}, o_{sub}]$ in case of compliance with the condition (1). Harmonization of different options of the SAD, namely, the common access matrix $M^{join}[s_{join}, o_{join}]$ is possible only if the information flows about objects $M^{sub}_{|S_{sub}|\times|O_{sub}|}$ are equal in the different access matrices.

Let's $F^{old}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{old}_{|S_{old}|\times|O_{old}|}, O_{sub}\right)$,

$F^{new}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{new}_{|S_{new}|\times|O_{new}|}, O_{sub}\right)$ are the binary matrices of information flows of the old and new options of the SAD between common objects, respectively, and $\Re$ is the formation operator of the binary matrix of information flows between the common objects of both options of the SAD and a certain access matrix.

The initial data for the operator of the binary matrix of information flows formation is the access matrix $M_{|S|\times|O|} = M[s, o]$ and a subset of objects O', where $O' \in O$.

The next step of the method is formation of the adjacency matrix. In order to do this, let's divide the set of access rights R into the subsets: $\vec{R} \in R$ is a subset of access rights, which forms the information flow from the subject to the object (for example, the right to write); $\overleftarrow{R} \in R$ is a subset of access rights, which forms the information flow from the object to subject (for example, the right to read); $\tilde{R} \in R$ is a subset of access rights, which does not form an information flow (for example, the right to delete). The elements of the adjacency matrix $E_{|O|\times|O|} = \{e_{ij}\}$ are formed by the following way:

$$e_{ij} = \begin{cases} 1, \exists k\, M[s_k, o_i] \in \overleftarrow{R}, M[s_k, o_j] \in \vec{R} \\ 0, else \end{cases}. \quad (2)$$

In the future, taking into account properties of the graph, the reachability matrix is defined as the sum of disjunctions of the adjacency matrices, namely

$$E^* = \bigcup_{n=1}^{|O|} E^n. \quad (3)$$

In order to reduce the number of calculations, it is proposed to use the algorithm, presented in Figure 2.

The essence of the algorithm lays in stopping of the calculations if a new path does not appear in the next iteration.

The final stage of the operator of a binary matrix of information flows formation between common objects of both options of the SAD is creation of a subset of information flows between the specified subset of objects

$$F = \{e^*_{ij}\}, \forall o_i, o_j \in O'. \quad (4)$$

Thus, the result of the described above calculation methodology is determination of the binary matrix of information flows between the common objects of both options of the SAD.

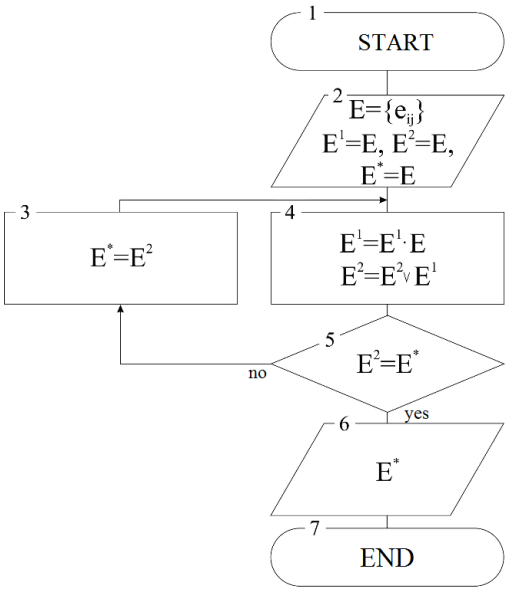

Fig. 2. Block diagram of the algorithm for determination of the reachability matrix

Usage of the operator, described above, will give possibility to form a set of information flows, taking into account the access matrices for each option of the SAD. The equality of the binary matrices of information flows between common objects in each option points to the harmonization of both options of the SAD.

Block diagram of the method for harmonizing the access matrices of different options of the access differentiation systems is presented in Figure 3.

The method, presented above, requires formulation and proving of the fact that in case of equality of information flows of common objects of both SAD options it is impossible to realize the forbidden information flow in one option of the SAD and permitted in another one (Figure 1).

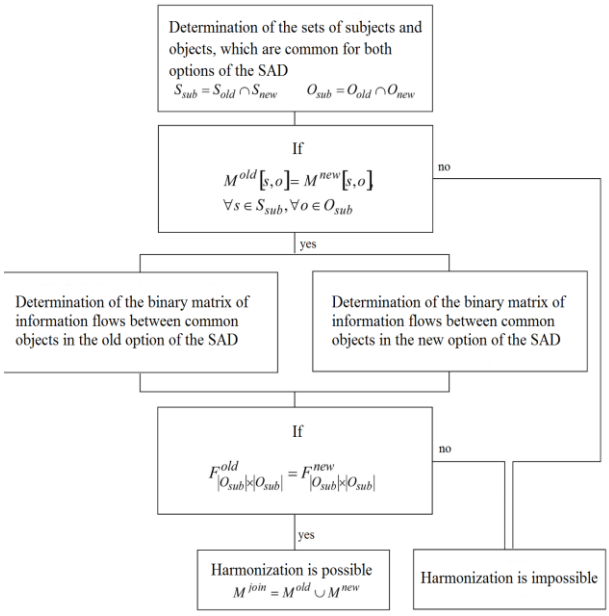

Fig. 3. Block diagram of the method for harmonizing the access matrices of different options of the access differentiation systems

Theorem. In order to harmonize the access matrices of different options of the systems of discretionary access differentiation, it is necessary and sufficient to ensure equality of information flows between the common objects of both options.

Proof of the need. In the models of discretionary access differentiation, an unauthorized information flow is a flow that is not provided by the access matrix. Note that in each separate option of the SAD access matrix is formed correctly and does not violate the information confidentiality, i.e. appearance of an unauthorized information flow. Consequently, in the case of equality of information flows of both options, the violation of information security is impossible. Let's assume that in one option there is a possibility of appearance of the information flow, which is unauthorized one in another option. This means that in one option of the SAD such flow is possible, and in the second option it is impossible, in other words, there are different information flows between subjects and objects of the SAD, which contradicts the theorem condition.

Proof of sufficiency. Any violation of the information confidentiality foresees existence of the information flow only to the subject of the system contrary to the access matrix. The information flow between objects does not violate confidentiality. At the same time, the information transfer between subjects is possible only through the physical carrier of information (file, database, etc.), i.e. the object of the system. Therefore, it is sufficient to consider only the common objects of the system, because the correctness of the information flows of non-common objects are provided by separate options of the SAD.

Usage of the method for harmonizing the access matrices of different options of the discretionary access differentiation systems is done in the following way. Checking of the possibility of access matrices coordination is carried out before joint operation of the existing and upgraded SAD (fulfillment of the condition 1). If its harmonization is impossible, it is necessary to change access parameters in the one of the SAD option in order to be prepared for the next stage of the method. Then, the consistency of information flows of the different SAD options is checked. If an inconsistency is detected, there is a possibility to correct one of the options of the access matrices and re-check it. In the case of equality of information flows for common objects, different options of the SAD can operate in tandem at a common data field. If dynamic change of access matrices parameters is needed, it is possible to implement the harmonization mechanism, which will check changes for the existence of unauthorized information flows. Therefore, in case of joint operation of existing and upgraded information and telecommunication system, there is a possibility of an unauthorized information flows appearance, and as a result violation of information security.

V. CONCLUSION

During development of the integrated information and telecommunication system composite parts, a certain security policy is formalized and realized, which is based on the known models of information security. Their usage in the separate information and telecommunication subsystems ensure performance of functions, connected with provision of an information resource properties observance. At the same time, during modernization of the existing composite parts of the supersystem or integration of new ones, a situation of joint functioning of access differentiation systems in the common data field appears.

A method for harmonizing access matrices of systems of discretionary differentiation of access to information systems at the stage of modernization is developed. It is intended for the formation of access matrices common for both options of the SAD at the stage of information systems modernization.

The essence of the method for harmonizing access matrices of different options of access differentiation systems lays in the formation of common and unique access matrix for both options, in which it is impossible to realize an unauthorized information flow in each option of the SAD separately.

The scientific basis of the method is formulation and proof of the security theorem of joint functioning of different options of the systems of discretionary differentiation of access. The developed method of harmonizing access matrices of different options of the discretionary access differentiation systems will allow to formally describe the procedure of joint functioning of both information systems complying with information properties and determining the conditions under which unauthorized information flows cannot occur.

REFERENCES

[1] Yudin O., Ziubina R., Buchyk S., Matviichuk-Yudina O., Suprun O., Ivannikova V. Development of Metods for Identification of Informationcontrolling Signals of Unmanned Aircraft Complex Operator: Easten-European Journal of Enterprise Technologies, Vol 2, No 9(104) (2020), pp. 56-64, https://doi.org/10.15587/1729-4061.2020.195510.

[2] Suprun, O., Nechyporuk, O., Kashkevich, I.-F., Nechyporuk, V., Poburko, O., Apenko, N. Identification of Combinations of Faults in Multilevel Information Systems: Proceeding of the International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, April 22-26, 2020, IEEE Part Number: CFP2064A-PRT, ISBN (IEEE): 978-1-7281-7179-1, pp.76-81.

[3] Weissman, Clark. "Security controls in the ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

[4] Linde, Richard R., Clark Weissman, and Clay E. Fox. "The ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

[5] Hartson, H. Rex, and David K. Hsiao. "A semantic model for data base protection languages." Proceedings of the second international conference on Systems for Large Data Bases. VLDB Endowment, 1976.

[6] Harrison, M.H., Ruzzo, W.L. and Ullman, J.D. "Protection in Operating Systems." Communications of ACM 19(8), 1976, pages 461-471.

[7] Sorokun, A., Suprun, O., Matviichuk, V., Voskoboinikov, S., Babenko, Y. Research of Features and Possibilities of Modern Real Time Video Services : Proceeding of the International Conference on Advanced Trends in Information Theory (ATIT 2020), Kyiv, Ukraine, 25.11.21-27.11.20, 2020. IEEE Catalog Number: ISBN 978-1-7281-9799-9/20/$31.00©2020 IEEE, pp.92-96.