Estimation of Security of Objects of Informatization on the Basis of Mathematical Simulation as an Alternative to Certification Testing

Artem M. Sychov, Nadezhda A. Sukhorukova, Denis A. Kholod
Information Protection Department (IU10)
Bauman Moscow State Technical University
Moscow, Russian Federation
zi@bmstu.ru; nadya.suh.24@yandex.ru; runc@inbox.ru

Constant perfection of methods of unauthorized access to information, as well as significant damage to this kind of action resulted in a focused and systematic improvement of technologies of information security and mechanisms for responding to security threat information. One of the main areas of improvement is to ensure the compliance of the characteristics of these mechanisms demands adequate responses to threats and, consequently, adequate evaluation of the effectiveness of response measures. The basic concept is implemented in practice evaluation of the security of objects of informatization, is the concept of certification tests. Under this concept implies the assessment of the protection of informatization objects certification path used means of information protection from unauthorized access. One of the most promising alternative solutions to the problem of adequate evaluation of the security of objects of informatization is a synthesis of characteristics of processes of information security on the object of informatization within the corresponding target function. This article shows the possibility of obtaining a numerical evaluation of the security of information objects with the use of mathematical modeling of information security threats, caused by illegal actions, and processes for responding to such actions. This approach will allow to evaluate the effectiveness of the various responses and on the basis of these assessments to justify the most effective system for ensuring security of objects of informatization.

Keywords— information security; threats; informatization objects; protected information systems; mathematical modeling; conformity assessment; security compliance; certification tests; attestation test; Orange book; e-banking

I. Introduction

Constant perfection of methods of unauthorized access to information, and significant damage to this kind of action resulted in a focused and systematic improvement of technologies of information security and mechanisms to address threats to information security. One of the main areas of improvement is to ensure the compliance of the characteristics of these mechanisms demands adequate responses to threats and, consequently, adequate evaluation of the effectiveness of response measures [1-3].

Obviously, such an assessment should be carried out systematically [5], on the basis of a comprehensive study of ways to protect the objects of informatization (information systems).

In accordance with the system approach investigation of mechanisms in responding to threats to the security of information of the objects of informatization (IO) connected with the security assessment of the IO, i.e., the capacity of these mechanisms to adequately respond to information security threats the IO.

II. The existing concept of evaluation of the security of the IO on the basis of certification tests

The basic concept is implemented in practice evaluation of the security of the IO is the concept of certification tests. Under this concept implies the security assessment of the IO certification path used means of information protection from unauthorized access. In accordance with the Governing document "Protection from unauthorized access to information. Terms and definitions" under the certification of information security means activities for confirmation of conformity of possibilities of means of information protection requirements of state standards, normative documents approved by Federal certification bodies within the competence of those bodies [4]. It should be noted that, in accordance with document certification study limited to description of the functions performed by protection mechanisms from unauthorized access to information, and qualitative characteristic of the contents of these functions corresponding to a certain class of security of information systems and computer technology, as well as a list of normative documents on this issue. Implemented in the methods of certification are to verify the claimed capabilities with the requirements (Tab.1). In accordance with the Governing document "Automated system. Protection against unauthorized access to information. Classification of automated systems and requirements on information protection" the conclusion about the ineffectiveness of the mechanism of protection of information in General is done in the case that at least one of the claimed functionalities (the document is similar to the Orange book).

The obvious advantage of this concept for assessing the security of the IO is the ease of estimation procedures. Shortcomings that limit its use are:

1) the lack of a formal interpretation of characteristics of threats to information security;

2) lack of formalized representation of the dynamics of the impact of threats to information security and processes for responding to such threats;

TABLE 1. THE CLAIMED CAPABILITIES FOR INFORMATION PROTECTION CLASSES THE PROTECTION OBJECTS OF INFORMATIZATION

Used means of information protection and requirements	**Classes of protection**				
	1E	***1B***	***1C***	***1B***	***1A***
1. Means of access control					
1.1. Identification, authentication and access control entities:					
to IO	+	+	+	+	+
to terminals, computer equipment (computer technology), the nodes of computer network, communication channels, external devices of computer technology	-	+	+	+	+
to programs	-	+	+	+	+
to data	-	+	+	+	+
1.2. Managing information flows	-	-	+	+	+
2. The means of registration and accounting					
2.1. Registration and accounting:					
entry (exit) of access subjects to (from) the system (network node)	+	+	+	+	+
the issuance of a printed (graphic) output documents	-	+	+	+	+
run (completion) programs and processes (tasks, tasks)	-	+	+	+	+
program access of subjects to access protected files, including their creation and deletion, transmission lines and channels	-	+	+	+	+
program access of access subjects to the terminals, computer technology, nodes in a computer network, communication channels, external devices, computer technology, programs and data	-	+	+	+	+
change of authority of access subjects	-	-	+	+	+
created by securable object access	-	-	+	+	+
2.2. Records media	+	+	+	+	+
2.3. Clearing (reset, depersonalization) deallocate regions of memory computer technology and external drives	+	+	+	+	+
2.4. Signaling attacks	-	+	+	+	+
3. Cryptographic tools					
3.1. Encryption of sensitive data	-	-	+	+	+
3.2. Encryption of information belonging to different entities (groups of entities) in different keys	-	-	-	+	+
3.3. The use of certified (certified) encryption	-	-	-	-	+
4. Means of ensuring the integrity of the working environment					
4.1. Ensuring the integrity of software and processed information	-	-	-	+	+
4.2. Physical security of computer equipment and media	+	+	+	+	+
4.3. The presence of the administrator (service) information protection in the information system	+	+	+	+	+
4.4. Periodic testing of the working environment	-	-	+	+	+
4.5. The availability of means of information recovery	+	+	+	+	+
4.6. The use of certified means of protection	-	-	+	+	+

3) lack of a formalized model of security information, taking into account the peculiarities of the offender's actions as a source of threats [5].

These shortcomings lead to many errors in the justification of the ways and means of information security [4], which in turn necessitates the search for such approaches to the security assessment of the IO, which would provide the required adequacy assessment.

III. THE PROPOSED CONCEPT FOR ASSESSING THE SECURITY OF THE IO ON THE BASIS OF MATHEMATICAL MODELING

As the practice of conducting research in this direction, one of the most promising solutions to the problem of adequate evaluation of the security of the IO is a synthesis of characteristics of processes of information security for the IO within the corresponding target function (e.g. [6-11]).

As an example of such a system consider a system of the performance characteristics of responses to threats to the security of e-banking [12, 13].

The basis of the synthesis of this system based on the principle of the identity of the system structure characteristics of the effectiveness of such measures hierarchical representation of the functional model of the processes of responding to threats to the security of electronic banking. In turn, the functional model of the processes of responding to such threats is based on the functional model of illegal actions concerning the remote banking services (RBS), and that, in turn, based on the conceptual model of the offender.

Under these conditions, the model of the intruder is interpreted as a model of illegal actions in respect of the services of RBS. The major restrictions on the interpretation of this model are:

1) this kind of illegal action is a method of implementation of security risks of e-banking;

2) the source of the threats is an attacker;

3) for this kind of source is characterized by a single (during the study period) the impact on the environment of RBS;

4) once the impact on the environment of RBS is also done for reasons of stealth;

5) breach of security of e-banking is associated with the operation of illegal actions associated with the following operations:

– receiving confidential information of the bank clients;

– modification, or destruction of the information;

– blocking of the information security environment of the RBS in certain circumstances.

Target motivation are illegal actions on the modification or destruction of information clients of the bank.

The correspondence between the compositional characteristics of the grouping of States of a functional model of the processes of responding to threats to the security of electronic banking, the compositional characteristics of the grouping of States of a functional model of illegal actions in connection with the services, RBS and classification bases synthesized system characteristics are listed in Tab. 2, and the structure of the system in Fig. 1.

TABLE 2 COMPLIANCE COMPOSITE FUNCTIONAL BASIS OF MODELS OF STUDIED PROCESSES, BASES FOR CLASSIFICATION OF THE SYSTEM PERFORMANCE CHARACTERISTICS RESPONSES TO THREATS TO THE SECURITY OF OBJECTS OF INFORMATIZATION

Composite level	**Composite base grouping States functional models**		**Grounds for the classification of the system performance characteristics response**
	Illegal actions in respect of the services RBS	***Processes for responding to security threats in e-banking***	
1	the appearance of signs of illegal actions	identify signs of illegal actions	ability to identify signs of illegal actions
2	Stages of carrying out fraudulent operations in respect of the services RBS	definition of the stages of illegal actions	ability to identify stages of illegal actions
3	Illegal actions in relation to specific services	establishment of services of services exposed to security risks	opportunities for the establishment of ser-vices of services expo-sed to security risks
4	the objective function illegal actions	the objective function response	the effective response to security threats in e-banking

Given the fact that the implementation of the functions respond to the attacker is a reaction to unlawful acts in the formation of the characteristics of the timeliness of response to this kind of threat conditions timely response are [14, 15]

$$t_{(y)} < t_{(o)} \tag{1}$$

$$t_{(o)} < t_{(y)} + \tau_{(y)} \tag{2}$$

$$t_{(o)} + \tau_{(o)} \leq t_{(y)} + \tau_{(y)} \tag{3}$$

where: $t_{(y)}$ is a point in time the onset of the threat, $\tau_{(y)}$ – time implementation of threat $t_{(o)}$ – time detection of threats, $\tau_{(o)}$ – time to respond to the threat. The adequacy of the assessment of the values $\tau_{(y)}$ and $\tau_{(o)}$ is the systemic nature of evaluation mechanism.

With the random nature of the values that make up the conditions (1) to (3), the expression for E characteristics timeliness in responding to threats to the security of electronic banking can be represented as a probability [14]:

$$E = P(t_{(y)} < t_{(o)}, t_{(o)} < t_{(y)} + \tau_{(y)}, t_{(o)} + \tau_{(o)} \leq t_{(y)} + \tau_{(y)}) \tag{4}$$

Thus, it is clear that the method of evaluation of security of IO by organizing and modeling the characteristics of the processes of information security on these objects and devoid of the shortcomings to the assessment of security of IO on the basis of certification tests.

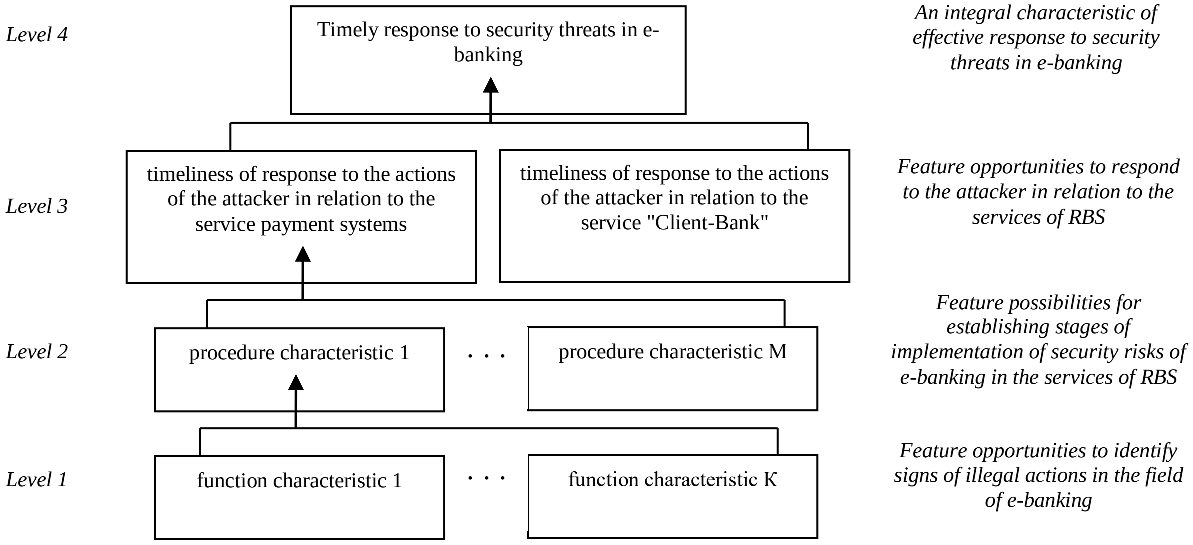
Level 4
Timely response to security threats in e-banking
An integral characteristic of effective response to security threats in e-banking
Level 3
timeliness of response to the actions of the attacker in relation to the service payment systems
timeliness of response to the actions of the attacker in relation to the service "Client-Bank"
Feature opportunities to respond to the attacker in relation to the services of RBS
Level 2
procedure characteristic 1
. . .
procedure characteristic M
Feature possibilities for establishing stages of implementation of security risks of e-banking in the services of RBS
Level 1
function characteristic 1
. . .
function characteristic K
Feature opportunities to identify signs of illegal actions in the field of e-banking

Fig. 1. The Structure of the System Performance Characteristics Response the Security Threats of E-Banking

IV. CONCLUSION

A method of evaluating the security of objects of Informatization on the basis of certification tests has a number of drawbacks that can be eliminated when using the proposed approach to this evaluation through mathematical modeling. This method allows to obtain an adequate assessment of the effectiveness of information security at the Olympics in a wide range of parameters of the security threat information and apply the protection mechanisms.

REFERENCES

[1] Benslimane Y., Yang Z., Bahli B. Information Security between Standards, Certifications and Technologies: An Empirical Study. In Proc. of the 2016 International Conference on Information Science and Security (ICISS), IEEE, 2016, pp. 1-5. DOI: 10.1109/ICISSEC.2016.7885859.

[2] Sedinić I., Lovrić Z. Influence of established information security governance and infrastructure on future security certifications. In proc. of the 2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija, Croatia, 2013, pp. 1111–1115.

[3] Wargo C.A., Frye G.E., Robinson D.W. Security Certification and Accreditation analysis for UAS Control and Communications. In Proc. of the 2009 Integrated Communications, Navigation and Surveillance Conference, IEEE, 2009 Pages: 1 - 12 DOI: 10.1109/ICNSURV.2009.5172850.

[4] Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, Journal of Theoretical and Applied Information Technology, 2016, vol. 88, No 1, pp. 77-88.

[5] Hambolu Q., Yu L., Oakley J., Brooks R.R., Mukhopadhyay U., Skjellum A. Provenance threat modeling. In Proc. of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2016, pp. 384 – 387. DOI: 10.1109/PST.2016.7906960.

[6] Ekanem B.A., Essien N. Identifying fault-prone modules in software for diagnosis and treatment using eeporters classification tree. Computer Sciences and Telecommunications. 2010. N 3. P. 88-98.

[7] Fay J. Contemporary Security Management.3th ed. Butterworth-Heinemann, 2010. 480 p.

[8] Iskhakov S.Yu., Shelupanov A.A., Meshcheryakov R.V. Simulation modelling as a tool to diagnose the complex networks of security systems. Journal of Physics: Conference Series. 2017. V. 803. N 1. P. 012057.

[9] Kostogryzov A. Modeling software tools complex for evaluation of information systems operation quality (CEISOQ). Lecture Notes in Computer Science. 2001; 2052; 90-101. DOI: 10.1007/3-540-45116-1_12.

[10] Kostogryzov A., Krylov V., Nistratov A., Popov V., Stepanov P. Mathematical models and applicable technologies to forecast, analyze, and optimize quality and risks for complex systems. In: The ICTIS 2011: Multimodal Approach to Sustained Transportation System Development - Information, Technology, Implementation - Proceedings of the 1st Int. Conf. on Transportation Information and Safety, ASCE, 2011, pp. 845 – 854. DOI: 10.1061/41177(415)107.

[11] Kostogryzov A.. editor. Probabilistic Modeling in System Engineering. InTech, 2018.

[12] Sychev A., Revenkov P., Dudka A. Bezopasnost ehlektronnogo bankinga *[Security of e-banking]*. M.: Alpina Pablisher, 2017. 320 p. *(In Russ).*

[13] Revenkov P., Berdyugin A. Expansion of the Operational Risk Profile in Banks Under Increase of DDoS-threats. Voprosy kiberbezopasnosti *[Cybersecurity issues]. 2017. N 3 (21). P. 16-23.* DOI: 10.21681/2311-3456-2017-2-16-23.

[14] Skryl S., Sychev A., Afonin I., Barkalov Y., Karpychev V. Ocenka ehffektivnosti mer reagirovaniya na ugrozy bezopasnosti ehlektronnogo bankinga: koncepciya i vozmozhnosti realizacii. Pribory i sistemy. Upravlenie, kontrol, diagnostika *[Instruments and Systems: Monitoring, Control, and Diagnostics]*. 2017. N 12. P. 33-40. *(In Russ).*

[15] Skryl S., Sychev A., Gromov Y., Meshcheryakova T., Arutyunova V. Matematicheskoe predstavlenie pokazatelya svoevremennosti reagirovaniya na ugrozy bezopasnosti kompyuternoj informacii v usloviyah prostejshej modeli narushitelya. Inzhenernaya fizika *[Engineering Physics]*. 2016. N 4. P. 29-35. *(In Russ).*