The main aspects of conformity assessment of DLP-systems used to ensure the security of significant objects of critical information infrastructure of the Russian Federation

V V Selifanov, P A Zvyagintseva, J A Isaeva and A S Goldobina
Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

Abstract. The main aspects of conformity assessment of significant objects of critical information infrastructure are considered. Information security tools used to ensure the security of significant objects of critical information infrastructure must necessarily undergo the conformity assessment procedure and its form is defined only for state and municipal information systems, as well as information systems of personal data. In all other cases, the subjects must determine the form, content and criteria of conformity assessment independently. The authors propose an approach to assessing the compliance of information security tools on the example of DLP-systems, allowing it to determine, as well as the analysis and synthesis of the procedure. This approach is harmonized with the international regulatory framework and is based on the latest methodological documents of the Federal Service for Technical and Export Control of Russia on operating systems.

1. Introduction
With the entry into force of the Federal law of the Russian Federation of 26.07.2018 № 187 «On the security of information infrastructure of the Russian Federation» [1], a new segment of information systems has appeared, in which information security is strictly required.

This segment combines a fairly large number of heterogeneous objects, which are divided into three groups:

- information system;
- automated process control systems;
- information and telecommunication networks [1].

Taking into account that violation of safety properties of such objects can lead to serious consequences of various scales [2], the requirements to the means of protection are set as strict as possible, including mandatory conformity assessment.

2. Problem statement
The analysis of requirements to safety of significant objects of information infrastructure of the Russian Federation [3] showed that conformity assessment could be carried out in the form of certification or tests (acceptance). Thus, requirements for certification are put forward also by other regulatory legal acts of the Russian Federation, for example, the Order of Federal Service for Technical and Export Control of Russian Federation № 17 [4].
In the case where there are no such requirements, as well as on-site already implemented means of information security subject of critical information infrastructure (hereinafter-CII) conformity assessment should be carried out independently at various stages of the implementation of organizational and technical security measures. The object of the study is the procedure of conformity assessment of DLP-system.

From the point of view of the Federal law «On technical regulation», conformity assessment is a direct or indirect definition of compliance with the requirements for the object, in this case DLP-system.

Analyzing the provisions of the requirements [3] researchers are faced with a number of problems that have no solution in the segment of documents regulating the security of significant objects of critical information infrastructure – the most problematic of which is the need for conformity assessment during testing and acceptance into operation.

On the one hand, everything complies with the provisions of the federal law "On technical regulation" [5] on the other hand the composition and content of the procedures are not defined, and most importantly, the criteria by which it is necessary to decide on the compliance or non-compliance of protection systems.

It should be noted that in accordance with the adopted approaches [1], [3] the subject of critical information infrastructure is directly responsible for ensuring the security of the object and, therefore, must obtain comprehensive evidence of the reliability of the protection system, taking into account the possible damage, as well as the costs of the evaluation procedure itself.

The place and role of the above procedures in the process of creating a cybersecurity system of critical information infrastructure objects is interesting, which can be represented as a sequence of the following steps [3], [6], [7], [8]: categorization (classification); identification and classification of critical assets; assign security and access management requirements that define a system’s cybersecurity architecture; development, implementation, testing and commissioning.

As can be seen, testing and commissioning are integral and equivalent stages of work in the creation of a cybersecurity system, which poses three tasks to researchers:

- defining the criteria that a cybersecurity system must meet;
- determination of the composition and content of conformity assessment procedures;
- development of conformity assessment methodology.

3. Theory

In order to understand what these requirements are, the subject of the CII will have to solve another non-trivial problem: determine the requirements for this type of protection as DLP-system, which are not defined by any of the regulators. This FfF that they must be set for the DLP system. Probably, it is possible to use the existing system of requirements based on ISO/IEC 15408 [9-11] standards actively used by the Federal Service for Technical and Export Control of Russian Federation.

When using the «General criteria» [9-17] the object of evaluation (hereinafter-OE), which in this case will be the DLP - system, is considered not in itself, but in the context of its environmental functioning. During the preparation for the conformity assessment should be allocated requirements for the environment of the OE, hereinafter referred to as aspects of the environment of functioning of the OE. Aspects of the environment of functioning of the OE contain the following components:

- security assumptions contain various security concepts for the environment in which the OE will be used or is intended to be used;
- security threats that include all threats to the security of information that require protection by OE or its environment;
- security policies that identify and, if necessary, explain all the provisions of the organization's security policy or the rules to which the OE must comply.
On the basis of the above-described security components, the security objectives for the OE and the operating environment are formulated, aimed at ensuring the confrontation of threats and the implementation of the provisions of the security policy.

In order to achieve these goals, security requirements are imposed on the OE. There are two groups of requirements - these are the safety requirements for the safety functions of OE, and the requirements of confidence in the technology and process of development, operation and evaluation of the OE and are designed to ensure the adequacy of the implementation of safety mechanisms.

Existing DLP-systems allowed to develop the following concept:

- The main security threats that should eliminate DLP-system, marked with the prefix «SD»;
- The provisions of the security policies that must successfully function in a DLP system and is represented by the prefix «SP»;
- Assumptions the security of DLP-systems is represented by the prefix «SA».

**Table 1. Description of aspects of dlp-systems functioning environment**

| Designation | Description |
|-------------|-------------|
| SD. UNAUTHORIZED_ACCESS | An unauthorized user may attempt to gain unauthorized access to information processed by the DLP system by bypassing security mechanisms. |
| SD.ACCESS_CONTENT | An internal intruder may attempt to withdraw protected information from the information system |
| SP.ACCESS_DATA | DLP-system ensures the implementation of security policy operations with protected information |
| SP.MANAGE | The configuration and management of the DLP system must be provided by authorized administrators |
| SP.ACCESS | DLP system users must be allowed to work with the system |
| SA.NOEVIL | The initial installation and configuration of the DLP system is performed by an authorized system administrator |
| SA.LOCATE | The DLP system is within the controlled area |
| SA.SECCOM | The DLP – system environment must ensure that distributed parts of the DLP system communicate securely and remotely between the system components and the administrator. |
| SP.SECURITYINTERNET | The DLP-system environment must ensure that entities from an untrusted network (such as the Internet) can only access the OE via ftp |

The analysis of the identified aspects of the security environment made it possible to formulate FSR in ISO/IEC 15408-2 notations table 2.

**Table 2. Safety requirements functions**

| Functional safety requirements applicable to a DLP system the symbol of the family | Name of functional capability |
|-------------------------------------------------------------------------------------|-----------------------------|
| FMT_MOF                                                                             | Managing the various security features of the DLP system |
Functional safety requirements applicable to a DLP system the symbol of the family

| Name of functional capability |
|-------------------------------|
| FMT_MTD Data management of DLP system security functions |
| FMT_SMR Assigning security management roles |
| FAU_GEN Security audit data generation |
| FAU_SAR View security audit |
| FIA_UAU Authenticate users |
| FIA_ATD The definition of the user attributes |
| FIA_UID User identification |

Requirements of trust – in fact the requirements for the composition and content of the conformity assessment procedure. Also here it should be noted, rather accurate reference point set in point 29 of the Order of Federal Service for Technical and Export Control of Russia № 239 [3]:

In significant objects of category 1, information security means (hereinafter – ISM) are used not less than 4 classes of protection;
2 categories – not less than 5 protection class;
3 categories – 6 protection classes.

At the same time, each specified protection class corresponds to a certain level of estimated confidence given in State Standard ISO/IEC 15408-3 with additional components that allow to correspond to the levels of control of the absence of undeclared opportunities given in the guidance documents [18]. The list of such components installed in the protection profile of operating systems of type «A» [18] is given in table 3.

| Classes of trust | Trust components |
|------------------|------------------|
| Development      | ADV_ARC.1 Security architecture description |
|                  | ADV_FSP.4 Full functional specification |
|                  | ADV_IMP.2 Full display of the implementation view of the Safety Function of the Evaluation object and |
|                  | ADV_IMP_EXT.3 Implementation of OE |
| Guides           | AGD_OPE.1 User’s manual |
|                  | AGD_PRE.1 Подготовительные процедуры |
| Support life cycle | ALC_CMC.4 Support for generation, acceptance procedures and automation |
|                  | ALC_CMS.3 The scope of the Configuration Management presentation implementation |
|                  | ALC_DEL.1 Delivery procedures |
|                  | ALC_DVS.1 Identification of security measures |
|                  | ALC_FLR.1 Basic Troubleshooting |
|                  | ALC_LCD.1 Developer-defined lifecycle model |
|                  | ALC_TAT.1 Fully defined development tools |
|                  | ALC_FPU_EXT.1 Operating system software update procedures |
Let us formulate the method, stages, procedures and criteria for assessing the compliance of information security products according to State Standard R ISO/IEC 15408 [10-12] similarly [19].

If (1) - many component requirements the credibility of the information security requirements for facility assessment 

\[ K = \{ k_1, k_2, \ldots, k_n \} \]  

(1)

Lot \( K \) it is formed using one of the predefined trust assessment levels (TAM) or protection classes. For each component of the trust requirement \( k_i \), defined set of actions (2).

\[ A = \{ a_{i1}^{(i)}, a_{i2}^{(i)}, \ldots, a_{in}^{(i)} \} \]  

(2)

\((n_i- the number of actions of an appraiser for components \( k_i \)), which must be performed by the appraiser (testing laboratory) to confirm compliance of the OE with the presented component \( k_i \).

For each action, evaluator \( a_j^{(i)} \) there is a lot (3)

\[ g_j^{(i)} = \left\{ g_{j1}^{(i)}, g_{j2}^{(i)}, \ldots, g_{jm}^{(i)} \right\} \]  

(3)

of steps of evaluation - the smallest structural unit of work for evaluation \((m_j^{(i)}- the number of steps of estimation to actions of the appraiser \( a_j^{(i)} \)). The development of evaluation steps is performed by experts of the testing laboratory on the basis of the «General safety assessment methodology» presented in State Standard R ISO/IEC 18045-2013 [10], taking into account the features of the OE.

Under the method of developing the evaluation steps will understand the display (4)

\[ M : \Sigma \times A \rightarrow G \]  

(4)

A function \( M \) on the basis of the actions of the appraiser \( a_j^{(i)} \) and information about the implementation (of evidence developer) OE \( \Sigma \) generates a set of evaluation steps \( G_j^{(i)} \), performed to check the satisfaction
of OE many $K$ component requirements of trust for security. As a rule, the function $M$ for this OE $\Sigma$ is a bijective map [21] [22].

The operator of correctness of performance of action of the appraiser (5) for OE $\Sigma$ call

$$a_{j}^{(i)} \in A^{(i)},$$

$$F_{g}: \sum A \rightarrow \{0, 1\};$$

$$F_{g}(\sum a_{j}^{(i)}) = \begin{cases} 1, & \text{if the evaluation steps are successful} \\ 0, & \text{otherwise} \end{cases}$$

The conformity assessment procedure is a set of four objects (8) where: $K$ - many component requirements of confidence to safety requirements for OE $\Sigma$; $M$ – development method the steps of evaluation; $F_{g}$ – the operator of correctness of performance of action of the appraiser.

$$B = \{\Sigma, K, M, F_{g}\}.$$ (8)

Conformity assessment procedure (in the form of certification tests) provides for three stages: planning, evaluation, analysis and execution of evaluation results [20]. At the planning stage, the tasks of obtaining and analyzing the initial data for the assessment are solved. On the basis of the performed analysis, many actions (2): of the appraiser and the corresponding assessment steps are formed.

Evaluation of the ISM is carried out using a set of evaluation steps. The analysis and presentation of evaluation results involves a comparison of actual and benchmark results. As a result of the analysis, we obtain a set of ordered pairs of the form is (7)

$$(a_{j}^{(i)}, F_{g}(\sum a_{j}^{(i)})).$$ (9)

For OE $\Sigma$, the compliance with the component of the trust requirement is declared $k_{i}$, if during the execution of a set of actions of the appraiser, $k_{i}$, if during the execution of many actions of the evaluator (7) positive results are obtained for each of them (8):

$$\sum_{a_{j}^{(i)}}^{n} F_{g}(\sum a_{j}^{(i)}) = n_{i}.$$ (10)

According to the results of the evaluation, a technical evaluation report is issued. For OE declared compliance with the requirements of confidence in the security of information (1), if (9)

$$\forall i \in [1, n] \sum_{a_{j}^{(i)}}^{n} F_{g}(\sum a_{j}^{(i)}) = n_{i}.$$ (11)

At the same time, the method and procedures for assessing compliance with these requirements are generally consistent [13], what allows us to assert the identity of the confirmed level of trust DLP-system the most relevant documents of the Federal Service for Technical and Export Control of Russia in the field of requirements means information security for the fourth class of protection used for their certification.

It should be noted, that for the procedures and functions discussed above, it is necessary to allocate the following to the stages of creating a subsystem for ensuring the safety of significant objects of critical information infrastructure, while the following should be taken into account:

DLP-system is only one of the components of the security system, and its operation is highly dependent on other components;

The nature of work in the course of testing a Significant object of critical information infrastructure is slightly different from the procedures described in state standard R ISO/IEC 18045-2013 [18].

Based on the above, and also based on the provisions of state standard R 0043-3-2014, it should be noted that the most optimal procedure for assessing compliance with ISO/IEC 15408 standards in the framework of the order of the Federal Service for Technical and Export Control of Russia № 239 – is certification of information security requirements, within the framework of which, confirmation of compliance of means of information protection to the requirements provided in point 29 of this document is carried out.
This step is not required for the greater part of the significant objects of critical information infrastructure, but its use will improve the reliability of the results.

4. The findings and conclusions
The paper presents an approach to conformity assessment on the example of DLP-systems, allowing it to determine, as well as its analysis and synthesis for use in significant objects of critical information infrastructure. This approach is harmonized with the international regulatory framework and is based on the latest methodological documents of the Federal Service for Technical and Export Control of Russia on operating systems.

The proposed method of formation of procedures and criteria for certification tests of the ISM through the "General criteria" can be useful in the development of private methods of verification of mechanisms and subsystems of information security.

References
[1] 2017 Federal law dated 26.07.2017 № 187 «On the security of the critical information infrastructure of the Russian Federation»
[2] 2018 The decree of the RF Government dated 08.02.2018 № 127 «About the approval of rules of categorization of objects of critical information Infrastructure of the Russian Federation, as well as a list of indicators of criteria for the importance of critical information infrastructure of the Russian Federation and their values»
[3] 2017 The order of the Federal Service for Technical and Export Control of Russia from 25.12.2017 № 239 «About the approval of requirements for safety of significant objects of critical information infrastructure of the Russian Federation» Retrieved from: https://minjust.consultant.ru/documents/38914
[4] 2013 The order of the Federal Service for Technical and Export Control of Russia from 11 February's 2013 г. № 17 «About the statement of requirements for protection of the information which is not the state secret containing in the state information systems».
[5] 2015 Methods for Testing & Specification; Risk-Based Security Assessment and Testing Methodologies, European Telecommunications Standards Institute, ETSI EG 201 015, 2015.
[6] 2019 CloudFlare «Zero-trust security: What's a zero-trust network?» 2019
[7] Bellovin S M 2019 Layered Insecurity IEEE Security & Privacy 17 03 96-95
[8] 2002 Federal law dated 27.12.2002 № 184 of "On technical regulation" 2002
[9] 2012 State standard R ISO / IEC 15408-1-2012 Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 1. Introduction and General model.
[10] 2013 State standard R ISO / IEC 15408-2-2013 Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 2. Functional safety components.
[11] 2013 State standard R ISO / IEC 15408-3-2013 Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 3. Components of security trust.
[12] Markov A S and Tsirlov V L 2017 Structural content of information security requirements Monitoring of law enforcement 1 53- 61
[13] Grishchenko L A 2018 Assessment of trust in the security of information technologies Questions of science and education 7 62-6
[14] Demidov D 2017 A systematic approach to describing the source code of a cloud platform with assured security 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) pp 31-6
[15] Mukhanov A, Petukhov A, Pilugin P 2018 «Common Criteria» and Software-Defined Network (SDN) Security International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC) pp 1-6
[16] Chen H, Bao D, Gao H, Cheng J 2016 A Security Evaluation and Certification Management Database Based on ISO/IEC Standards 12th International Conference on Computational Intelligence and Security (CIS) pp 249-53

[17] Recchia L, Procopio G, Onofrii A, Rogo F 2014 Security Evaluation of a Linux System: Common Criteria EAL4+ Certification Experience IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (Naples, Italy) pp 77-81

[18] Methodical document of Federal Service for Technical and Export Control of Russia. «Protection profile of type "A" operating systems»

[19] Barabanov A V, Grishin M I, Markov A S, Tsirlov V L 2013 Formation of information security requirements for DLP-systems Radioelectronics Issues 2 67-76

[20] State standard R ISO / IEC 18045-2013 Information technology. Methods and means of security. The methodology of evaluation of information technology security

[21] Barabanov A V, Grishin M I, Markov A S 2011 Formal basis and metabasis of conformity assessment of information protection means of Informatization objects Proceedings of the Institute of engineering physics 3 82-8

[22] Markov A S, Tsirlov V L, Barabanov A V 2012 Methods for assessing the inconsistency of information protection means ed A S Markov (Moscow: Radio and communications) p 192