Critical Information Infrastructures Security Modeling

Sergey Erokhin, Andrey Petukhov, Pavel Pilyugin
Moscow Technical University of Communications and Informatics
Moscow, Russia
esd@mtuci.ru, anpetukhov@yandex.ru, paul.pilyugin@gmail.ru

Abstract—**The paper discusses the modeling of various aspects of the security of critical information infrastructures (CII) in the assumption of creating a reference model of CII security in the future. The features of CII in terms of goals and safety criteria based on the analysis of various regulatory and methodically established definitions and descriptions of CII are established. The contradictions arising in the attempts to use the traditional methodology of information security in relation to CII are shown. The problems of using the methods and models of classical risk analysis are discussed, in particular, the impossibility of applying the concept of residual risk to the formation of CII safety objectives. The conclusion is made about the expediency of basing these goals on the exhaustion of possible protective measures (controls and activities), the concept of asymptotic safety management of CII , which guarantees the trend of security growth without its current assessment. Changes in the role and place of the threat model in ensuring the security of CII related to the lack of evidence of the completeness of this model are considered. The attractiveness of using the SDL technique for forming elements of the threat model in the conditions of a specific CII is indicated. The structure of the future reference model of safety of the CII including definition of the purposes and criteria of safety (including functional), multilevel static model of functioning of the CII (including security factors), a dynamic model of the spread of security incidents within the CII, the typology of the result of aggressive manifestations of the CII functioning environment (threat model) and the model (methodology) of the spread of protective activities within the information infrastructure.**

I. Introduction

Critical information infrastructures (CII) in different spheres of activity, in different countries can be attributed to completely different objects, but despite this, all these objects have a number of common features that determine the specifics of the CII from the point of view of security, including with regard to modeling methods.

Analysis of the current results of the Russian and international regulation of procedures for ensuring the safety of CII shows that they are determined not through their properties, but through a situation (incident) when something happened to them, i.e. in the normal, non-emergency state, they may not differ from the "non-critical" infrastructures. The definition of CII includes the state of the environment (state, people, nature, etc.), which may not be involved in the functioning of the CII , including not affecting the security of the CII . In particular, foreign sources [1] define critical infrastructure as a set of systems and assets that are so vital to the state that the destruction of such systems and assets will have detrimental effects on national security. CII includes public and private owners, operators and other entities related to IT and responsible for its condition (as a subject of CII management).

This point of view leads to some object and subject duality of ideas about the safety of CII . Object duality is expressed in the fact that the safety of the CII is considered in the form of a set of situations including the state of both the object and the environment of its functioning. Object states can be irreversible or even correspond to the total loss of the object, the state of the environment can be safe or emergency (correspond to the incident). Each situation is generated by a certain state of the object, it is its cause, but in the situation there is also the state of the environment that arose under the influence of the object, so the level of criticality (significance) of the CII, strictly speaking, depends on the security of the environment. All situations corresponding to a security incident constitute a set of criticality.

Damage resulting from security incidents, applies to certain "recipient" (recipient) of the damage (the CII-recipient). The elements of the set of criticality associated with a CII-recipients but the subject duality is that the recipient does not necessarily manages CII security. In other words, there are many recipients of CII and many subjects of CII security management, and these sets are, in General, different. It follows that the model of high-level entities of "Common criteria" [2], which believes that owners of information assets manage security risks, should be supplemented in the case of CII.

The categorization of CII solely on the scale and nature of the damage [3] also distorts the traditional role of the risk model, taking into account the intensity of the threat. In General, such categorization before several incidents occur is somewhat conditional, since there are no mechanisms for calculating the residual risk (it is impossible to justify its acceptable level and the concept of residual risk disappears in practice). Apparently, in order to somehow compensate for this fact, there are new directions of the use of standards and techniques in the management of safety of CII , for example, in [4] for the first time specified technologies that are prohibited in significant objects of CII , for example, remote access of persons who are not employees of the subject of management of CII (in particular, this means that outsourcing of CII service, including the developer, formally can be carried out only in person).

II. Criteria of CII security

Initially, information security had three objectives-confidentiality, accessibility and integrity. This triad is related to the concept of security almost half a century ago, which stated that information security is a technique that controls who can use or modify the computer or the information contained therein: unauthorized use, modification and blocking of use [5]. Over time, this principle has been enshrined in various regulations, arguing that any security incident can be reduced to a violation of one or more of these three criteria.

The imperfection of this approach has long been known, in the process of development of information technology there were whole classes of incidents that can not be associated with a violation of the traditional criteria of the triad. Attempts to update the criteria space, bringing it in line with the modern problems of information security, led to the expansion of the nomenclature of criteria (for example, Parker's hexade [6]) or took into account the relationship of criteria with the state of information and protection activities (for example, McCamber's cube [7]). In all cases, these solutions do not go beyond their conceptual apparatus of the actual information technology, and the elements of the resulting criterion space are formulated in terms of information assets (data and processes).

To date, the information security strategy of a typical office or traditional automated system, as a rule, identifies as a priority criterion the confidentiality of information, the second priority is integrity, and the last – availability.

In the context of CII, the priority of these tasks is changing. Security in such systems primarily affects accessibility – that is, ensuring and maintaining the health of all components. In the second place is usually integrity, and the lowest priority is given to confidentiality, because the data circulating in the system are often " raw " and without further analysis within the context are not valuable.

The priority of the criteria, integrity, and availability relative to confidentiality again highlights the fundamental circumstance fundamentally distinguishes CII in a number of other types of implementation of information technologies. This is because the security objectives of the CII clearly go beyond the information infrastructure itself and are determined by aspects of the operation of the entire critical facility. Violation of the criteria of integrity and availability, particularly in paths of control, have a direct and immediate negative impact on the functioning of the critical object, while a violation of the confidentiality of such exposure, typically, is not. Therefore, in traditional systems, such as office systems, security objectives are defined in terms of information assets and confidentiality is among the criteria of the leading place, and for CII , where security objectives are associated with sustainable and trouble-free operation of the object, this statement is usually unfair.

In certain circumstances, the integrity of the system may have the highest priority (although individual components or the system as a whole will be prioritized according to these requirements under specific operating requirements). In determining the direction of such requirements (i.e. the goals and objectives of security), regulatory sources on CII, along with the use of traditional formulations, focus on the structure and content of security objectives for CII . For example, in [4] the goal-setting is concentrated in paragraph 16 ("security tasks") and includes four tasks (goals), the first of which is absolutely general and applicable to any type of information technology implementations (and not only for CII):

- "prevention of illegal access to information processed by a significant object, destruction of such information, its modification, blocking, copying, provision and distribution, as well as other illegal actions in relation to such information" [4] (it is noteworthy that the illegal "provision" and "distribution", i.e. factors of confidentiality, are mentioned in the last place)

The other three tasks (goals) explicitly use different from the traditional safety criteria directly related to the efficiency of the object functioning:

- "prevention of information impact on software and software and hardware, as a result of which the operation of a significant object may be disrupted and (or) terminated;
- ensuring the functioning of a significant object in the design modes of its operation under the influence of threats to information security;
- ensuring the possibility of restoring the functioning of a significant object of critical information infrastructure» [4]

In the process of identifying the boundaries of effective application of the regulatory framework of security CII and analysis of the above formulations, it is found that there is no mention of the traditional criteria of security (confidentiality, integrity and availability) or other characteristics of the state of information assets. These formulations extend the state space of information assets to the state space of the most critical object. Security criteria are established among the characteristics of functioning invariant to the events of the information space. Moreover, these formulations (for example, concerning disaster recovery processes) extend not only the space on which the criterion is defined, but also the time of such determination, since they assume the properties of a critical object for a period of some duration after the incident (recovery period).

In General, the security of a CII is understood as "the state of protection of a CII, ensuring its stable functioning when carrying out against its computer attacks" [4]. This definition takes the security of CII beyond the actual information security, "capturing" the space of functional security. Therefore, when modeling the safety of CII it is impossible to speak only about information security, the concept of functional safety should be involved-part of the security of the critical object, which depends on the correct functioning of the safety-related electrical control systems, security systems, etc., based on other technologies.

III. Asymptotic security management

Other fundamental differences between safety objectives and the related system of criteria and other methodological grounds are also characteristic of CII .

In any definition (description) of the concept of CII and or related categories, there is a clear postulate on the principle inadmissibility of the incident leading to the accident. At the same time, we are not talking about any acceptable (minimum) levels of trust, robustness or other characteristics of "incident resistance" characterizing the residual risk that is caused. there are at least two reasons: the absence or fundamental rejection of mechanisms for calculating damage (human casualties, irreversible environmental consequences, etc.) and the inability to justify the very minimum level of "incident resistance", which can be said to have ensured safety. Therefore, the inadmissibility of an emergency incident under any circumstances is expressed explicitly or implicitly as a security goal of the CII.

However, there is another important fact-the difference between the subjective probability of an incident from zero (if it were not, the CII would not fit its definition). This difference from zero gives rise to the concept of the recipient of the CII, which allows for the occurrence of an incident, but does not allow for a mechanism for calculating damage. For the same reason, a security management entity seeking to avoid the possibility of an incident is always confident that such a possibility exists. Therefore, the CII safety simulation should take into account the following limitations:

- it is generally incorrect to determine the security risk of the CII and therefore to manage it in the traditional sense;
- it is even more incorrect to establish an acceptable level of residual risk for the CII and, especially, to use it as a safety purpose;
- the subjective probability of an incident must be zero (inadmissibility of an incident), but it will never be zero according to the definition of the CII.

In these circumstances, security management can be in some sense "asymptotic" in nature, abandoning the assessment and management of risks in an explicit form, to guarantee a steady approximation of the subjective probability of an incident to zero. Perhaps this methodology will be the most attractive for the CII.

In the context of abandoning the concept of residual risk, the assessment of the threat intensity is abolished, and it becomes impossible to analyze the degree of reduction of this threat as a result of security measures. The threat model is primitivized to a binary state ("there is a threat - there is no threat"). It is impossible to imagine the statement that there is no threat initially, or that some threat is completely eliminated by security measures (there is no concept of materiality or insignificance of the threat in these conditions). All the known methodology of threat modeling explicitly or implicitly include the dogma, asserting the sufficient completeness of a model, no one is concerned about (could be due to the impossibility of) a proof of this completeness.

Without this dogma, the goal of CII safety management is not to achieve some level of security (to balance risks with costs, to bring some derivative measure (risk, trust, economic indicators) to a given level or to optimize such characteristics). The aim of ensuring the safety of the CII is to exhaust the potential of protection (to do everything possible) regardless of the content and direction of aggressive manifestations and subject to known and limited capabilities of protective activities. And then, the target state of security is defined not in terms of threats and entities harmonized with them (offender, asset, vulnerability, etc.), when we argue that some (claiming to be exhaustive) set of actual threats is compensated by us, but directly in terms of our activities-activities (claiming all the same exhaustive completeness).

A significant fact is that in any methodical standard of CII there is no categorical dependence of decisions on structure and an origin of threats. Therefore, it can be assumed that either it is necessary to abandon the methodology based on threat modeling, or to use the correct mechanism of proof of exhaustive completeness for the threat model used. In the first case, it is necessary to concentrate not on threats, but on protective activities and implement all those measures, the effectiveness of which is positive, solving the non-trivial task of ensuring the formal completeness of the initial nomenclature of activities and metrization of their effectiveness depending on the conditions, including compatibility of application. In the second case, the deep question of the original axiomatics, on the basis of which it is possible to build a proof of the presence or absence of a threat, has not yet been solved.

There is a practice (at least internationally) of creating and using a common language to describe, understand and manage CII-risks, both external and internal [1]. Its purpose is to facilitate the process of identification and prioritization of activities to compensate for the risks of CII. Attention is drawn to the fact that not the threats of risks are identified, and not even the risks themselves, but the activity of their compensation. In this language, the initial entities are not classified as threats or even attack scenarios, but as types and subtypes of security measures. Since the development of such a language corresponds to the movement towards the creation of a reference model of CII, the question arises: is the form of identification of risks as manifestations of threats the only possible, and is it possible to identify risks without specifying the threat and vulnerability, for example, by linking it directly to the type of protective activity (or its absence)?

IV. Security threats modeling

In any case, in order to answer these questions, it is necessary to have an adequate understanding of the threatening danger. In any particular case, there are features of the structure and form of such representation and the common element is always the typology of the manifestation of danger, the nomenclature of identified and qualified types of such manifestation, external (aggressiveness of the environment) and internal (imperfection of the object) events and situations that cause damage (the so-called proactive aspect of security management [8] - threat model).

Threat modeling methodologies tend to focus on several types:

- declarative (base model method)
- support for risk analysis (feasibility assessment methods)
- the subject of the decomposition (how the data flows and process flows)
- harmonization of high-level entities (common criteria methods)

Declarative methods of forming threat models suggest the presence of regulated information and procedural resources to support the various stages of modeling (basic model). Methods of this type use speculative systematization of threats based on the assumption of the internal content of the threat. The low level of constructability of such a scheme, the lack of links with the features of the used assets and information technologies, the General nature of expert assessments limit the use of declarative techniques in real conditions.

Methods of the second type represent the gradual process of the attack modelling and analysis of threats aimed at preparing data for multidimensional risk analysis. This process involves the harmonization of security objectives and technical requirements for information processing and transmission procedures at each stage. As a result, the dynamic, adaptable and extensible identification of threats, the enumeration of their nomenclature and the procedure for assessing the feasibility are carried out. At the same time, the range of threats and their characteristics are formed on the basis of requirements that establish a certain, pre-permissible level of residual risk for each category of information assets. Obviously, this makes this approach inapplicable for critical information infrastructure objects.

Technologies of the subject of decomposition are distinguished not so much methodological innovations, many of fine tools and instruments to visualize the processes of decomposition. This ensures a correct evolutionary transition from one level of threat modeling to another. Threat modeling begins with the creation of a representation of the analyzed application or infrastructure, and then in this representation the components of its parts are allocated, i.e. the decomposition of the subject of analysis is carried out. Declarative methods of forming threat models suggest the presence of regulated information and procedural resources to support the various stages of modeling (basic model). Methods of this type use speculative systematization of threats based on the assumption of the internal content of the threat. The low level of constructability of such a scheme, the lack of links with the features of the used assets and information technologies, the General nature of expert assessments limit the use of declarative techniques in real conditions.

One common way to visualize a formal threat modeling process is to use data flow diagrams (DFD) [9]. Initially, there were only four elements in DFD: data flows, data warehouses, data modification processes, and external data modification factors - interactors. But, when the management of information security has become the prevailing ideology of the calculus of trust (the"common criteria"), the DFD procedure complements another definition of "trust boundary", specifically for modeling threats.

The idea of harmonization of threats is implemented in the concept of information security management taking into account the requirements and conditions (for the object of management and for the environment of its functioning) on the basis of an assessment of confidence in the means of implementation of these conditions and ways to meet these requirements ("calculation of trust"). The basic statement of this concept is [2]. One of the key provisions of this document establishes the set and relationship of the original concepts ("high-level entities") in the field of information security. These relationships show that the essence of the "threat" interacts with the entities "risks", "assets", "threat agents" and "vulnerabilities". Harmonization reveals these relationships and allows to include their content in the threat model, therefore threats are modeled not by themselves, but in the context of interacting entities.

But the application of even this developed standard in the case of critical information infrastructure objects causes some difficulties. The main source of them is that the result of an information security incident is described by dividing the set of object states into subsets of acceptable and unacceptable States, and the security criteria change abruptly when the state of an object changes from one subset to another. Moreover, in general, security criteria can have the same value for object States from different subsets. Finally, one of the possible states of an object can be the termination of its existence as a result of an incident, which in some cases makes any assessment of safety criteria meaningless.

Among the approaches that harmonize threats with other high-level entities (vulnerabilities, assets and threat agents), the SDL (Security Development Lifecycle) methodology [10] attracts attention, which includes the method of listing "threats per element". In general, it involves several stages, but in the context of the topic of security of critical objects of interest are charting and listing threats.

When charting, you typically use the DFD data flow charting tools (including the trust boundary element). The element of "trust boundary" shows that the elements located on different sides of this boundary function at various levels of authority.

To enumerate threats in SDL, you can use the "stride threats per item" method, after accepting elements of some universal list as the initial item [11]:

- **S**poofing of user identity (spoofing subject),
- **T**ampering (intervention and modification),
- **R**epudiation (disclaimer),
- **I**nformation disclosure (leakage and disclosure),
- **D**enial of Service,
- **E**levation of privilege (capture and elevation of privilege)

Attention is drawn to the proximity of the wording of this classification of threats to the actual security criteria [6], which indicates a high level of generalization of the initial nomenclature of threats, and gives grounds to count on the appropriate level of completeness of the model. The method assumes that all threats can be grouped from the STRIDE list, and that each type of DFD-elements correspond to certain threat classes [10]. The methodology continues to evolve, for example, the issue of the role and possibilities of disclaimers (received and sent messages) in attacks on logbooks (data stores) in order to remove them is still debatable.

As will be shown below, the knowledge required to simulate the safety of CII must contain, not so much information about the aggressive potential of the environment, as about the channels of its implementation, i.e. about the sequences of events and states within which the causal chains of the incident spread are implemented, from its occurrence to the fact of damage.

Elements of such chains can be considered as vulnerabilities, but in the case of CII vulnerabilities are methodically subordinate, because in CII vulnerability can only be in three States: eliminated, eliminated (short-term state) and unknown. Therefore, the harmonization of threats in the modeling of CII is aimed at identifying unknown threats.

Methodological solutions are included in the SDL does not directly operate with the category of damage and not pursue the goal of minimizing the residual risk. They are aimed at achieving the completeness of the threats taken into account, thereby creating prerequisites for the exhaustion of the potential of protective actions. At the same time, SDL fully retains the "harmonizing" properties, allowing to consider the manifestations of the threat in the context of a specific element of information technology (asset), in specific conditions and taking into account a specific source. In addition, SDL inherent "evolutionary" properties that allow for the decomposition of interacting entities, specifying scenarios for the threat (attack), without violating harmonization. Thus, we can conclude about the suitability and feasibility of SDL methodology for modeling threats to the security of CII.

V. A Distributed security modeling

Static multilevel models of the main types of CII are used for the analysis, design and management of CII safety. These models are used for a structured description of the space where functional and information processes take place, and the procedures for managing these processes are performed. For the safety of the static model CII are important precisely because they are the source of the terms, conditions, and limitations of emergence and spread within the level and between levels of "faults" CII, leading to an emergency incident.

One of the first to claim such a role was the so-called reference model [12], which defines five functional levels, but what is usually meant by CII occupies three lower levels. This model was created to describe the arbitrary functioning, but, due to the high level of its conceptuality, it was practically not used in an independent and non-detailed form. In the future, it has found its application as a basis for more developed and specialized security models.

The Kishi physical architecture hierarchy model proposed and developed in [13] describes the physical components combined via networks. Theoretically, it is quite suitable for modeling the safety of CII, but for this it is necessary to provide detailed specifications of the functioning of the elements of the architecture and the interaction of these elements with each other. The preparation and maintenance of such specifications is very time-consuming, especially for interfaces between levels. This fact significantly limits the use of the model.

Against the background of others, the zoning model (Perdue) stands out for its universality [14], which is a rational symbiosis of the two mentioned models (reference and physical architecture) and is widely used for the analysis of control and security systems of CII . The zoning model is a multi-level scheme of CII and can be a platform for analysis of threats, vulnerabilities, risks and countermeasures (controls and activities) taking into account the management, information and support functions of CII . In addition, it develops, for example, in its original form, the model covers the entire CII without division into" critical "and" non-critical " parts, and in practice such division may be necessary, and for this purpose a special intermediate level – demilitarized zone- is added to the model..

It is important to emphasize that a common feature of static CII models is the use as the main instrumental technique of "stratification" (stratification) of the object – the allocation of the hierarchy of management, information and support functions of CII and the placement of similar entities involved in the performance of these functions at a fixed level. The subject of analysis in the framework of such a model is the interaction of these entities both within the appropriate level and with the adjacent higher and lower levels.

Therefore, looking ahead, it is natural to assume some analogy for the architecture of a promising communication platform of the future reference model of CII security. Within the framework of such a" stratified " architecture of the communication platform, it makes sense to talk about at least two circuits (levels) of communication services: the control loop of the communication infrastructure (including routing of data flows) and the loop of the transport data transmission, ensuring the delivery of data (the results of the functions of the CII) to the access points to these data.

In addition, we note the effectiveness of the use of DFD-techniques for the specification of the functioning of the elements of the zoning model and the interaction of these elements with each other both within the same level and with the adjacent higher and lower levels. The thesis that each type of DFD-elements correspond to certain classes of threats allows at each level of the static model, taking into account specific devices, systems, communications to identify and specify security factors specific only for this situation.

There is a causal extent (a non-deterministic chain of events and states) between elements of threat potential and the occurrence of damage. This is not really an attack scenario, if only because the latter is more deterministic in terms of control and more tied to the timeline. In the context of CII, we are not so much interested in the sources of harm (elements of the threat potential) as in the form and properties of the harm realization. CIIsafety considers the possibility of additional risks in the implementation of protection and provides not only the elimination (weakening) of the threat factors, but also the activity in the development process and the final manifestation of the danger (the moment of direct occurrence of damage, regardless of the threat that caused it).

Dynamic models of the analysis of such cause-and-effect chains provide an opportunity to study and control the processes of occurrence and spread of security incidents in the space of information assets of the CII. An extensive review of such models is given in [15]. The analysis of the known practical methods of modeling these processes throughout their life cycle and throughout the space of factors and circumstances affecting them showed that with the help of such models it is possible to effectively control the causal chain of the incident.

The fundamental distribution of security factors and the spread of security activities beyond the information infrastructure require addressing the issues of placement and interaction of security activities in the CII. In order to complete the formation of the CII security management circuit, it is necessary to provide IT with a method of distributing protective measures over the space of CII information assets in accordance with the trajectories of information security incidents. The determining prerequisite is that it is not possible to provide the necessary safety properties by the use of a single countermeasure or technique.

In this case, the question of the actual composition of activities (protective measures, controls) is not so acute, because there are sources, normative or constructive-methodically supporting and providing extensive nomenclature of activities, the completeness of which (nomenclature) is not in doubt. In these circumstances, it is advisable to discuss only the details of activities in the Annex to the specific implementation of the CII . The problem of effective (adequate and conflict-free) placement of activities in accordance with the adopted (multi-level static) model of the CII and the identified (dynamic) model of the spread of unacceptable deviations (incident) comes to the fore).

One of the most developed strategies to solve this problem is the use and application of the concept, involving the use of a large number of countermeasures in a step form (division into levels) [16]. The meaning of this concept is that after the penetration of the attacker through one of the protective levels, he meets with a new, perhaps fundamentally different protection of the attacked object. This hybrid multi-layer security strategy implements a comprehensive approach to security across the entire CII.

Thus, we place protective activities throughout the causal chain of occurrence and development of the incident:

- exclude potentially dangerous fragments from the technology and supply the technology with infrastructure-architectural protective components and properties (static multilevel model)
- reduce the preconditions of unacceptable processes (threat model)
- provide an impossibility even in the case in the framework of the KII invalid transition of the object into an invalid state (dynamic model of the development of the incident))

VI. Summary

The initial statement of the security problem for traditional approaches is:

- for the declarative approach, effective (primarily cost-effective) implementation of the regulatory framework of security solutions.
- for a risk-based approach, achieving an acceptable level of residual risk is effective (primarily in the economic sense).
- for the calculation of confidence, the justification of the legality of assessment of that trust.

None of these approaches is fully able to ensure the safety of critical objects because it is impossible:

- be satisfied with the notion of declaratively acceptable residual risk
- limit yourself (without internal critical analysis) to normative nomenclatures of solutions
- it is unproven to accept any dogma of the completeness of the hazard (threat) model).

As part of the future reference safety model, it is advisable to provide for the CII:

- definition of safety objectives and criteria, taking into account:
  - expansion of KIWI security issues beyond the information infrastructure
  - involvement of functional safety methods and solutions;
  - features of CII related to risk analysis of implemented protective measures (activities and controls)
  - possibilities of the concept of asymptotic safety management;
- a static model for the operation of the CII , including safety factors reflecting the conditions of the" life cycle " of the incident;
- dynamic model of distribution incidents in the information infrastructure
- threat model that reflects the typology of the result of aggressive manifestations of the CII environment
- model (methodology) of the spread of protective activities within the information infrastructure, providing multistage (layered) counteraction to the spread of the incident throughout the depth of the CII

References

[1] Framework for Improving Critical Infrastructure Cybersecurity. // National Institute of Standards and Technology, USA, April, 16, 2018

[2] GOST R ISO/IEC 15408-1-2013 "Information technology. Methods and means of security. Criteria for evaluating the security of information technology. Part 1. Introduction and General model.

[3] Decree of the Government of the Russian Federation № 127 dated 08.02.2018 "On approval of the rules of categorization of objects of critical information infrastructure of the Russian Federation, as well as a list of criteria for the importance of objects of critical information infrastructure of the Russian Federation and their values." 20 sec.

[4] The Order of FSTEC of Russia No. 239 of 25.12.2017 "About the approval of Requirements to safety of significant objects of critical information infrastructure of the Russian Federation" (it is Registered in the Ministry of justice of Russia 26.03.2018). 28 p.

[5] Saltzer J. H., Schroeder M. D. The Protection of Information in Computer Systems URL: http://www.acsac.org/secshelf/papers/protection_information .pdf.

[6] Pender-Bey G. The ParkerianHexad: The CIA Expanded. URL: http://www.zigthis.com/145/parkerianhexad (дата обращения: 30.03.2016).

[7] McCumber J. Information Systems Security: A Comprehensive Model // Proceeding of the 14th National Computer Security Conference, NIST, Baltimore, MD, 1991.

[8] Andrey Petukhov. Information base of management of cybersecurity of critical infrastructures. XI InternationalScientificConference "InformationSocietyTechnologies" (Moscow, March 15-16, 2017).)

[9] Abi-Antoun, Marwan, Wang, Daniel and Torr, Peter, Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security, ASE'07, 2007. Atlanta, Georgia, USA

[10] Shostack, Adam (2014). "Threat Modeling: Designing for Security". John Wiley & Sons Inc: Indianapolis.

[11] «The STRIDE Threat Mode». Microsoft. 2016.

[12] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration — Part 1: Models and Terminology

[13] NIST Special Publication 800-82 Revision 2 «Guide to Industrial Control Systems (ICS) Security», May 2015. 247 c.

[14] ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems

[15] GOST R ISO/IEC 31010-2011 Risk Management. Risk assessment methods

[16] Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna, 1996