# Conceptual Approach to the Risk Analysis of Information Technology Security

Roman S. Anosov[1], Sergey S. Anosov[1], Igor Yu. Shakhalov[2,3], Valentin L. Tsirlov[2,3]

[1] *STC Zarya, 9 2nd Brestskaya St., bld.1., Moscow, 123056, Russia*
[2] *NPO Echelon, 24 2nd Electrozavodskaya ul., Moscow, 107023, Russia*
[3] *Bauman Moscow State Technical University, 5/1 2nd Baymanskay ul., Moscow, 105005, Russia*

**Abstract**

This paper describes the risk-oriented approach to the development of information security systems. The author suggests a concept-based formal model of security risk assessment and analysis for information technologies. It is suggested that the set of mean values of the subject activity integral effects, which determine the degree of its activity compliance with the purposes and regulatory requirements in conditions of information security threats, as the risk level indicator. It is concluded that the system element of information security risk analysis is a set of information, technical, organizational and socio-economic indicators for risk assessment at individual stages of analysis. It is demonstrated that the suggested concept-based approach can be specified in detail in the form of mathematical models.

**Keywords**

Risk assessment, conceptual model, risk management, information technology

## 1. Introduction

The notion of risk is a key notion in the field of security in general and information security in particular [1]. On the one hand, the information security risk combines the range of issues related to the information security threats, including identification of the threat sources and vulnerabilities in protected information technologies, determination of the methods, probability, and potential implications of the threats. On the other hand, the risk is integrated into the processes of technical and economic analysis and decision-making related to the information security assurance, creation of facilities and organization of information technology security system, definition of its composition, architecture, and configuration.

Characteristic features of the information security risk assessment include:

- High dimensions and the resultant labor-intensiveness of the assessment process stemming from the large number of potential security threats and vulnerabilities in the protected information technologies.
- Need to assess the risk at every stage of the information technology life cycle starting from the product definition to its intended use and retirement;
- Need to assess the risk at various levels of the information technology management, including the risk management and information security audit.

The risk "deployment" process demonstrated in Figure 1 can be presented as the successive effect produced by security threats on:

- The processes going on in the information system;
- The processes of the subject's (data owner's) activity management;

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: an_rs@list.ru (A.1); serg-anosov@mail.ru (A. 2); is@cnpo.ru (A. 3); v.tsirlov@bmstu.ru (A. 4)
ORCID: 0000-0002-1786-1128 (A. 3); 0000-0003-2657-4179 (A. 4)

- The results of activity at the level of individual subjects and at the level of the activity field in general.

Relevant indicators are used at each of these risk “deployment” stages, for example:

- Probability of the incident occurrence, information security indicators: confidentiality, integrity, availability;
- Performance of the information system, ability of the information system to perform its tasks;
- Potential damage of the subject that can be caused by any disruption in its control process; probability of the damage occurrence.

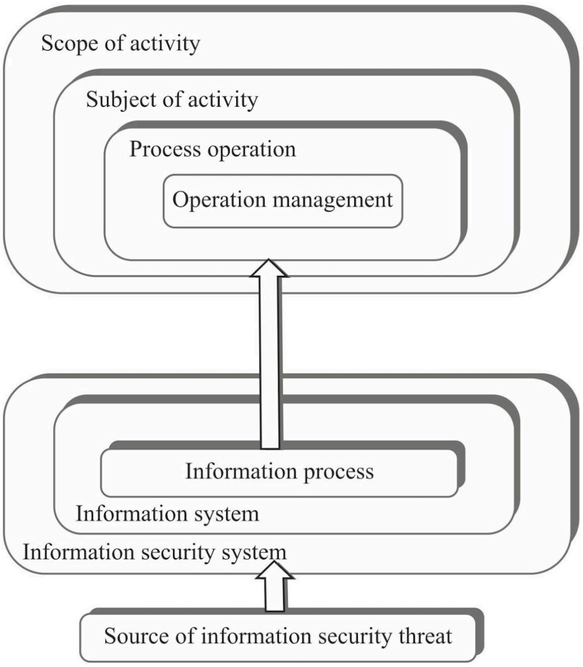

**Figure 1**. Structure of risk analysis process

High dimensions and multiple levels of the risk analysis task explain the wide practical application of qualitative (heuristic) methods used for its solution. However, the qualitative analysis methods do not fully suit the existing situation in the IT field which is characterized by the high significance of information infrastructure, intensive information confrontation, and high information security risks. An important activity aimed to improve the risk analysis efficiency is the application of formal (qualitative) methods of analysis based, in particular, on the results of formalization of various processes related to the information security assurance [2]. The formal access control model that provides a rigorous description of the information flows in the system is the classical representative of such methods [3-8]. Data flow diagrams (DFD), sequence charts of the Unified Modeling Language (UML), and tree formalism are used, for example, to model threats when developing secure applications [9, 10].

Papers [11, 12] use the tree and graph formalism to create the threat model. In papers [6, 13], the model of controlled threat occurrence process is developed, including the stages of protection system study and examination of protection facilities at the selected attack path and implementation of destructive effects. The dynamics of information security threat occurrence can be modeled using the Petri-Markov networks, which allows taking into account the parallelism and logical interrelation of threat occurrence processes. Markov models are also used to study the threats and to select the optimal set of information protection tools [14].

The formalism of individual processes associated with the information security assurance and specific stages of the risk analysis serve as the basis for system research. Thus, papers [15-22] describes the procedure for assessment of security risks in critical facilities that includes decomposition of the object into multiple components, determination of a set of associated threats, calculation of the risk-contributing potential of the object components considering the risk-reducing potential for protection measures. Paper [23] suggests a structured risk analysis using expert assessment and statistical data on information security incidents. In standard ISO/IEC/IEEE 24765[4], the hierarchy analysis method providing wide opportunities for the analysis of multilevel nested structures is used to assess the risk. Papers [24-28] deals with the issues of using fuzzy logic programming to evaluate the extent of damage arising from the threats to information security. The mathematical tools of Bayes networks are used in papers [29, 30] to build the intelligent (expert) automated system of threat analysis and risk evaluation. Paper [31] suggests using the immune systems and cognitive computing to reduce the risks.

## 2. Rationale for the formal model

The distinctive feature of this paper is the use of process approach [32, 33] to the risk analysis of information security based on the decomposition of the following processes:

- Process of the subject's activity in a specific field (industry);
- Information process in the subject's activity management systems;
- Life cycle process of the information technology and protection technologies.

The processes of the subject's activity are considered in the context of the structure described in Table 1.

**Table 1**
Generalized characteristics of the practical activity structure

| Name of level | Contents of level | Standard characteristics |
|---|---|---|
| Processes of the subject's activity | Process operations | Functional and technical characteristics of performed operations |
| | Production processes | Indicators of the product life cycle, resource-intensiveness, performance, quality, effectiveness, reliability, security |
| | Organizational and economical processes | Financial, employment, marketing indicators of the processes |
| Subjects of activity | Organizations, enterprises, institutions | Financial, employment, marketing indicators of the subjects |
| | Integrated structures | Performance indicators in accordance with the target programs, projects, and plans |
| Fields (industries) of activity | Health care, science, transportation, communication, power generation, banks, fuel and power, nuclear sectors, defense industry, aerospace sector, metals and mining, chemical industry | Social, political, economic, environmental significance, importance for the national defense, national security and public order |

The activity is regarded as a set of $\boldsymbol{P}$ elementary processes. Evey i-th elementary process is characterized by a set of positive effects $\boldsymbol{S}_i^+$ expressing the degree to which a functional purpose of the process is achieved and a set of negative effects $\boldsymbol{S}_i^-$ expressing the resource-intensiveness of the process and side consequences (not relating to the functional purpose) associated with its implementation.

Each level of activity is a system of serial/parallel elementary processes (operations) formalized by the graph theory methods. The graph edge corresponds to elementary process $P_i$ and the neighboring vertices correspond to the set of input $\boldsymbol{S}_{i\lhd}$ and the set of output effects $\boldsymbol{S}_{i\rhd}$ of this process:

$\boldsymbol{S}_{i\lhd} = \{\boldsymbol{S}_{j\rhd}^+, \boldsymbol{S}_{k\rhd}^+, \dots, \boldsymbol{S}_{l\rhd}^-, \boldsymbol{S}_{m\rhd}^-, \dots\}$, where indices $j, k, \dots, l, m \dots \in \mathbb{N}$, $j, k, \dots, l, m \dots < i$ are the indices of the processes $P_j$, $P_k$,…, $P_l$, $P_m$,…, whose output effects determine the output effect of the i-th process;

$\boldsymbol{S}_{i\rhd} = \{\boldsymbol{S}_i^+, \boldsymbol{S}_i^-\} = f_s(\boldsymbol{S}_{i\lhd}, \boldsymbol{U}_i, \boldsymbol{E}_i)$, where $\boldsymbol{U}_i$ is the set of control parameters of the $i$-th process, $\boldsymbol{E}_i$ is the set of environmental parameters influencing the $i$-th process, $f_s(*)$ is the operation of transforming the set $\{\boldsymbol{S}_{i\lhd}, \boldsymbol{U}_i, \boldsymbol{E}_i\}$ into the set $\boldsymbol{S}_{i\rhd}$.

The principle of activity decomposition into elementary processes implies the determination of activity nodes (time moments or process cycle events) where it is possible to identify uniquely the occurring effects meeting at least one of the following conditions:

[4] "ISO/IEC/IEEE International Standard - Systems and software engineering -- Vocabulary," in ISO/IEC/IEEE 24765:2010(E) , vol., no., pp.1-418, 15 Dec. 2010, doi: 10.1109/IEEESTD.2010.5733835.

The effects are essential for further activity in accordance with its technology (also in order to form control actions);

The effects are essential in terms of compliance with regulatory requirements.

The accepted approach to presentation of the practical activity as a system of elementary processes is based on the following assumptions:

1) At the level of process operations (Table 1), each i-th elementary process is considered to be an indivisible entity;

2) The course and result of i-th elementary process depend only on the set of input effects and set of control parameters;

3) At other levels of activities, starting from the level of production processes, a certain sequence of processes of the preceding level to which assumptions 1)…2) apply is considered as the elementary process.

Presentation of practical activity as a system of elementary processes and effects is illustrated by Figure 2.

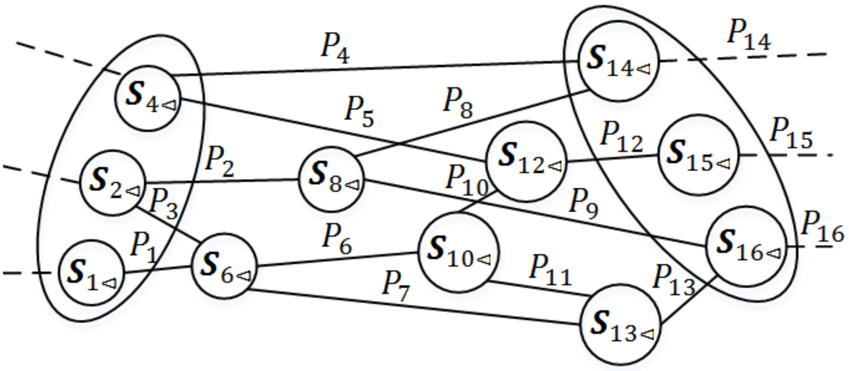
$P_4$
$P_{14}$
$\boldsymbol{S}_{14\triangleleft}$
$\boldsymbol{S}_{4\triangleleft}$
$P_5$
$P_8$
$P_{12}$
$P_{15}$
$\boldsymbol{S}_{12\triangleleft}$
$\boldsymbol{S}_{15\triangleleft}$
$P_2$
$\boldsymbol{S}_{2\triangleleft}$
$P_3$
$\boldsymbol{S}_{8\triangleleft}$
$P_{10}$
$P_9$
$P_{16}$
$\boldsymbol{S}_{16\triangleleft}$
$P_1$
$P_6$
$\boldsymbol{S}_{10\triangleleft}$
$\boldsymbol{S}_{1\triangleleft}$
$\boldsymbol{S}_{6\triangleleft}$
$P_{11}$
$P_{13}$
$P_7$
$\boldsymbol{S}_{13\triangleleft}$

**Figure 2**. Presentation of practical activity as a system of elementary processes and effects

On the Figure you can see that the ellipses denote the example of emphasizing the adjacent process states of the next level of activity, e.g.: $\boldsymbol{S}_{2\triangleleft} = \boldsymbol{S}_{3\triangleleft}$, $\boldsymbol{S}_{4\triangleleft} = \boldsymbol{S}_{5\triangleleft}$, $\boldsymbol{S}_{6\triangleleft} = \boldsymbol{S}_{7\triangleleft}$, $\boldsymbol{S}_{6\triangleleft} = \{\boldsymbol{S}_{1\triangleright}, \boldsymbol{S}_{3\triangleright}\}$, $\boldsymbol{S}_{8\triangleleft} = \boldsymbol{S}_{9\triangleleft}$, $\boldsymbol{S}_{10\triangleleft} = \boldsymbol{S}_{11\triangleleft}$, $\boldsymbol{S}_{12\triangleleft} = \{\boldsymbol{S}_{5\triangleright}, \boldsymbol{S}_{10\triangleright}\}$, $\boldsymbol{S}_{13\triangleleft} = \{\boldsymbol{S}_{7\triangleright}, \boldsymbol{S}_{11\triangleright}\}$, $\boldsymbol{S}_{14\triangleleft} = \{\boldsymbol{S}_{4\triangleright}, \boldsymbol{S}_{8\triangleright}\}$, $\boldsymbol{S}_{16\triangleleft} = \{\boldsymbol{S}_{9\triangleright}, \boldsymbol{S}_{13\triangleright}\}$.

Thus, the activity is formalized by a sequence of states of the elementary process system in the effect space $\{\boldsymbol{S}^{+}, \boldsymbol{S}^{-}\}$. The states of one activity level can be nested into the states of another level by scalarizing the effects of the preceding level or operating the state vector (without transforming the effect vector of preceding level into the scalar effect of the next level. As the result, it becomes possible to perform successive generalization of the effects of individual process operations as far as the activity effects of the subject and industry on the whole. In the set of the subject's (industry's) activity effects, it is possible to distinguish the subset of integral effects $\boldsymbol{S}_{\Sigma} \subset \{\boldsymbol{S}^{+}, \boldsymbol{S}^{-}\}$ whose size is used to assess the degree of the activity compliance with the defined purposes and specified requirements.

The information processes underpinning the practical activity control take place in the context of information systems and, more broadly, in the context of the information infrastructure (Table 2).

**Table 2**
Generalized characteristics of information infrastructure

| Name of level | Contents of level | Standard characteristics |
|---|---|---|
| Information processes | Organizational and economical, production, and technological information | Parameters of practical activity control |
| | Publicly available information, trade secrets, personal data, proprietary information for restricted use | Properties of information (confidentiality, integrity, availability, reliability etc.) |
| Information life cycle | Creation, processing (transformation), transmission, storage, destruction (deletion) | Indicators of corresponding information operations |
| Information infrastructure | State information systems, facilities of critical information infrastructure, automated control systems, personal data information systems, public information systems, information and telecommunication networks | Indicators of protection from unauthorized access, vulnerability of information systems, tools, and technologies (vulnerability of software, network protocols, availability of technical leakage channels, organizational defects etc.) |
| | Information protection systems, security systems | Organizational protective measures, information security software and technical facilities, security features of protection facilities, indicators of immunity to attacks. |
| Life cycle of information infrastructure facilities | Conceptual development, basic engineering design, development of detailed design documentation, commissioning, operation, modernization, decommissioning | Indicators of resource-intensiveness, confidence indicators (including the levels of check for the absence of vulnerabilities and undocumented features) |
| Information security threats | Anthropogenic, industry-related, natural hazards (intentional and non-intentional actions of a person, degradation of technical system reliability, weather conditions etc.) | Characteristics of information security threats, expertise, motivation, resources (potential) of information security violator |

Information operations are the procedural analogue of the process operation of practical activities in the information processes. They are performed by computation and communication information systems in compliance with preset algorithms and protocols and are aimed to solve the following tasks (refer to Figure 3):

Implementation of the abstract model of practical activity in the state space ***S***;

Formation of control parameters ***U*** ensuring the target path of the practical activity process in the state space ***S*** considering the environmental conditions.

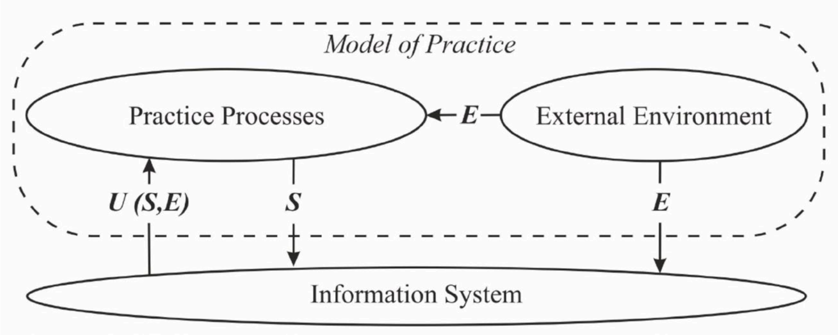

**Figure 3**. Illustration of practical activity control principle

In the Figure you can see that ***S*** is the state of practical activity processes, ***E*** are the environmental parameters, ***U*** are control parameters.

The values of control parameters $\boldsymbol{U} = f_u(\boldsymbol{O}^+, \boldsymbol{Q}^{o+}, \boldsymbol{O}^-, \boldsymbol{Q}^{o-}, \boldsymbol{C}, \boldsymbol{T}^o)$ are determined by such information process characteristics as:

- Set of information operations $\boldsymbol{O}^+$ provided by the information process algorithms (protocols);
- The probability that the i-th foreseen operation will be performed, $Q_i^{o+} \in \boldsymbol{Q}^{o+}$;
- Set of unforeseen (abnormal) operations $\boldsymbol{O}^-$ which can be performed in the information system under the influence of internal factors or environment;
- The probability that the i-th unforeseen operation will be performed, $Q_i^{o-} \in \boldsymbol{Q}^{o-}$;
- Quality parameter (degree of completion) of the i-th operation $C_i \in \boldsymbol{C}$;
- Duration of the i-th operation implementation $T_i^o \in \boldsymbol{T}^o = \{\boldsymbol{T}^{o+}, \boldsymbol{T}^{o-}\}$.

The set of values of information process characteristics $\boldsymbol{H} = \{\boldsymbol{O}^+, \boldsymbol{Q}^{o+}, \boldsymbol{O}^-, \boldsymbol{Q}^{o-}, \boldsymbol{C}, \boldsymbol{T}^o\}$ can be put into correspondence with the set of characteristics (properties) peculiar to the processed information including such classical properties as confidentiality, integrity, availability.

The standard procedural approach to the information process analysis suggests its presentation on several layers. Thus, the following layers are considered in computational information systems: application programming language, operating system, instruction set architecture, microarchitecture, digital logic layer. In communication information systems, such layers include the application layer, presentation layer, session layer, transport layer, network layer, channel layer, and physical layer. In databases, the conceptual, logical, and physical presentation layers are distinguished, each of which uses specific data presentation models.

The elementary information operation $O$ of the information process is considered in this model as a set including the input data $V$, instruction $I$ for the input data processing, and the operation execution result $W$: $O = \{V, I, W\}$ (Figure 4).

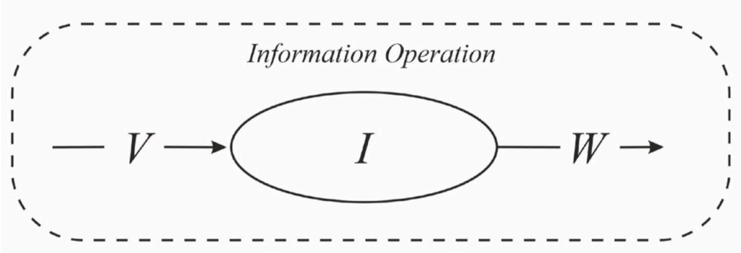

**Figure 4**. Information operation model

Structurally, the information process is defined by the precedence relation (or consequence relation) $\Xi$ specified on the set of information operations $\boldsymbol{O}$: i-th operation $O_i$ precedes the j-th operation $O_j$, $O_i \Xi O_j$, if the result of the i-th operation execution is used as the input data for the j-th operation. In general, instruction $I$ of the operation can depend on the results of one or several preceding operations, which is formally specified by the influence relation $\phi$ in the set $\boldsymbol{O}$: i-th operation $O_i$ influences the j-the operation $O_j$, $O_i \phi O_j$, if the result of the i-th operation execution determines the instruction of the j-th operation.

The information processes are implemented using the information technology system described in Table 3.

**Table 3**
Standard information technology system

| Life cycle stage | Contents of the information technology | Subjects determining the contents of information technology |
|---|---|---|
| Conceptual design | Determination of the goals, objectives, and functions of the information system | Customer |
| Basic technical design | Structure implementation: composition, architecture (topology), software and hardware configuration | Developer, regulator |
| | Functionality implementation: algorithms, protocols, operations | |
| Implementation | Development of operational documentation, organizational and administrative documentation | Developer |
| | Software and hardware integration | Integrator |
| | Implementation of organizational structure | Customer, developer, regulator |
| | Personnel training | Customer, operator |
| Operation | Support | Developer |
| | Implementation of performance characteristics | Operator, industry-related and natural factors |
| | Implementation of information processes | Personnel, users |

This information technology system is a means of influencing the H characteristics of information processes by the subjects A determining its content. Subject A is considered a source of threat if its actions have the potential to cause an information security incident – occurrence of one or several unintended information operations out of the set $\boldsymbol{O}^{-}$ – or affect the effectiveness of foreseen operations implementation assessed in compliance with the indicators of set $\{\boldsymbol{C}, \boldsymbol{T}^{\boldsymbol{o}+}\}$. It is convenient to show the correlation between the threats and the information technologies by which the threats can be implemented (Table 4) using a binary matrix $(m_{i,j})$: $m_{i,j} = 1$, if the j-th information technology can be used to implement the i-th threat; $m_{i,j} = 0$, if the j-th information technology cannot be used to implement the i-th threat.

**Table 4**
Ways of threats occurrence

| Access objects | Types of impact | Vulnerabilities |
|---|---|---|
| | **Physical access** | |
| Controlled area | Penetration | Organizational defects |
| Personnel | Social engineering | |
| Hardware and equipment | Special impacts | Limited resistance to physical fields |
| | Natural impacts | Limited resistance to natural factors |
| | Industry-related impacts | Limited reliability |
| | Mechanical impacts | Limited strength |
| Operating environment of hardware and equipment | Interception of physical fields (signals) | Technical leakage channels |
| | **Logical access** | |
| Network environment | Intrusion (cyber-attack) | Vulnerabilities of network protocols and data communication channels |
| Operating environment | Programming and mathematical impacts | Vulnerabilities of software algorithms and soft hardware |
| Data | Reading, modification, writing, deletion | Incomplete and/or incorrect access control |

The probabilistic nature of information security threats occurrence and implementation, as well as the system of protective technologies used to resist the threats (Table 5) determine the probabilistic nature of information process parameters $\boldsymbol{H}$ and, consequently, control parameters $\boldsymbol{U}$ and effects of practical activity $\boldsymbol{S}$. The use of protective technologies is aimed to prevent the mean values of integral effects $\overline{\boldsymbol{S}}_\Sigma$ from falling beyond the limits of permissible range $\overline{\boldsymbol{S}}_\Sigma^*$ in the presence of information security threats.

**Table 5**
System of standard protective technologies

| Objectives | Protective technologies | Problem-solving methods |
|---|---|---|
| Development of protection system | Tools for protection from unauthorized access;<br>Antivirus protection tools;<br>Cryptographic protection tools;<br>Tools of information availability assurance | Formal access control models; formal models of integrity and availability;<br>Discrete programming methods |
| Organization of the protection system operation | Identification and authentication;<br>Access control;<br>Antivirus protection;<br>Integrity assurance<br>Availability assurance;<br>Equipment protection;<br>Personnel training | Operation analysis methods |
| Protection system configuration management | Security monitoring (analysis) tools;<br>Management tools for information security events;<br>Intrusion detection systems;<br>Data leak protection tools | Optimization methods;<br>Game theory methods |
| Information security management | Security audit;<br>Incident management;<br>Asset management;<br>Risk management | System analysis methods |

## 3. Conclusion

The suggested model briefly outlines the stages of the information security risk “deployment”. The set of mean values of the subject’s activity integral effects $\overline{\boldsymbol{S}}_\Sigma$, which determine the degree of its activity compliance with the purposes and regulatory requirements in conditions of information security threats is used as the risk level indicator. Using $\overline{\boldsymbol{S}}_\Sigma$ as the risk level indicator allows taking into account both the extent of potential consequences of the information security threat occurrence and the probability of occurrence of such consequences. The risk is analyzed in accordance with the suggested model by solving successively the following tasks:

1) Analysis of threats to information security and development of a threat model. This task investigates the sources of threats, causes and probability of their occurrence; possibility and ways of the threat occurrence considering the applied information technologies are studied.

2) Analysis of the threat consequences by information indicators. This task investigates the impact of information security incidents on the efficiency of processes implemented by information technology, as well as on the quality of the information system operation on the whole.

3) Analysis of the threat occurrence consequences by organizational and technical indicators. This task includes the study of the effect the quality of information system operation produces on the control of automated processes in production and organizational activities.

4) Analysis of the threat consequences by social and economic indicators. This task is solved by investigating the influence of production and organizational activity effectiveness on integral indicators $\overline{\boldsymbol{S}}_\Sigma$ characterizing the degree of the activity compliance with its purposes and regulatory requirements.

5) Development of an information security system. This task is performed to investigate the possibility, ways, and facilities for achieving admissible values $\overline{\boldsymbol{S}}_\Sigma^*$ by countering the threats to information security. Comparative assessment of the information security system development alternatives is carried out based on the complex indicator $\{\overline{\boldsymbol{S}}_\Sigma^*, F\}$, including the life cycle cost $F$ of the information security system.

The essential element of the information security risk analysis is the complex of information, technical, organizational, social, and economic indicators that ensure the risk evaluation at specific stages of analysis.

## 4. References

[1] Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

[2] Markov A., Rautkin Y., Luchin D. and Tsirlov V., "Evolution of a radio telecommunication hardware-software certification paradigm in accordance with information security requirements," 2015 International Siberian Conference on Control and Communications (SIBCON), 2015, pp. 1-4, doi: 10.1109/SIBCON.2015.7147139.

[3] Anisimov V.G., Zegzhda P.D., Anisimov E.G., Bazhin D.A. A risk-oriented approach to the control arrangement of security protection subsystems of information systems. Automatic Control and Computer Sciences. 2016. V. 50. No 8. P. 717-721.

[4] Kostogryzov A.I., Stepanov P.V., Nistratov A.A., Nistratov G.A., Zubarev I.V., Grigorev L.I. Analytical modelling operation processes of composed and integrated information systems on the principles of system engineering. Journal of Polish Safety and Reliability Association. 2016. V. 7. No 1. P. 157-166.

[5] Kostogryzov A.I., Stepanov P.V., Nistratov G.A., Nistratov A.A., Grigoriev L.I., Atakishchev O.I. Innovative management based on risks prediction. In: Information Engineering and Education Science. 2014. P. 159-166.

[6] Petrenko A.A., Petrenko S.A., Makoveichuk K.A., Olifirov A.A. Methodological recommendations for the cyber risks management. In: CEUR Workshop Proceedings. (DLT 2020 - Selected Papers of the 5th International Scientific and Practical Conference Distance Learning Technologies). 2021. P. 234-247.

[7] Markov A., Barabanov A., Tsirlov V. Models for Testing Modifiable Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, Chapter 7, pp. 147-168. DOI: 10.5772/intechopen.75126.

[8] Markov A., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, Chapter 10, pp. 213-231. DOI: 10.5772/intechopen.75232.

[9] K. Labunets, F. Massacci, F. Paci, S. Marczak and F. M. de Oliveira, "[Journal First] Model Comprehension for Security Risk Assessment: An Empirical Comparison of Tabular vs. Graphical Representations," 2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE), 2018, pp. 395-395, doi: 10.1145/3180155.3182511.

[10] M. J. M. Chowdhury, "Security risk modelling using SecureUML," 16th Int'l Conf. Computer and Information Technology, 2014, pp. 420-425, doi: 10.1109/ICCITechn.2014.6997358.

[11] P. Ongsakorn, K. Turney, M. Thornton, S. Nair, S. Szygenda and T. Manikas, "Cyber threat trees for large system threat cataloging and analysis," 2010 IEEE International Systems Conference, 2010, pp. 610-615, doi: 10.1109/SYSTEMS.2010.5482351.

[12] J. Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 148-153, doi: 10.1109/SmartCloud49737.2020.00035.

[13] Kalinin M., Krundyshev V., Zegzhda P. Cybersecurity risk assessment in smart city infrastructures. Machines. 2021. V. 9. No 4. pp. 437–442. DOI: 10.3390/machines9040078.

[14] E. V. Larkin, V. V. Kotov, A. N. Ivutin and A. G. Troshina, "Petri-Markov model of interruptions," 2017 6th Mediterranean Conference on Embedded Computing (MECO), 2017, pp. 1-4, doi: 10.1109/MECO.2017.7977249.

[15] Massel A., Gaskova D. Identification of critical objects in reliance on cyber threats in the energy sector. Acta Polytechnica Hungarica. 2020. V. 17. No 8. P. 61-73. DOI: 10.12700/APH.17.8.2020.8.5.

[16] Olifirov A.V., Makoveichuk K.A., Petrenko S.A. Integration of cyber security into the smart grid operational risk management system. CEUR Workshop Proceedings. 2019. V. 2522, pp. 132-144.

[17] Petrenko S.A., Makoveichuk K.A. Ontology of Cyber Security of Self-Recovering Smart GRID. CEUR Workshop Proceedings, 2017. V. 2081, pp. 98-106.

[18] V. Mokhor, S. Honchar and A. Onyskova, "Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 19-22, doi: 10.1109/PICST51311.2020.9467957.

[19] Butusov I., Romanov A. Methodology of security assessment automated systems as objects critical information infrastructure. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2018. No 1(25), pp. 2-10. DOI: 10.21681/2311-3456-2018-1-2-10.

[20] Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Kunakov E.P., Drolova E.Y. Implementation and auditing of risk management for the oil and gas company. In: Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. 2017. P. 539-543.

[21] Livshic I.I., Podolyanets L.A. Models of complex industrial facilities assessment based on risk approach. International Review of Management and Marketing. 2016. V. 6. No 5. P. 125-135.

[22] Kalashnikov A.O., Anikina E.V. Management of risks for complex computer network. Communications in Computer and Information Science. 2020. V. 1337. P. 144-157.

[23] A. Kozlov and N. Noga, "Some Method of Complex Structures Information Security Risk Assessment in Conditions of Uncertainty," 2020 13th International Conference "Management of large-scale system development" (MLSD), 2020, pp. 1-5, doi: 10.1109/MLSD49919.2020.9247662.

[24] I.V.Anikin, "Using fuzzy logic for vulnerability assessment in telecommunication network," 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 2017, pp. 1-4, doi: 10.1109/ICIEAM.2017.8076444.

[25] P. B. Khorev and M. I. Zheltov, "Assessing Information Risks When Using Web Applications Using Fuzzy Logic," 2020 V International Conference on Information Technologies in Engineering Education ( Inforino ), 2020, pp. 1-4, doi: 10.1109/Inforino48376.2020.9111767.

[26] N. Khokhlov, S. Kanavin and A. Rybokitov, "Modeling Information Security Infringements in Mobile Self Organizing Network of Communication Using Fuzzy Logic and Theory of Graphs," 2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA), 2019, pp. 60-63, doi: 10.1109/SUMMA48161.2019.8947572.

[27] Markov A., Markov G., Tsirlov V. Simulation of Software Security Tests by Soft Computational Methods. In Proceedings of the VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security' (IWCI 2019). (March 17-24, 2019 in Irkutsk, Baikalsk, Russia). Advances in Intelligent Systems Research vol. 169. Pp. 257-261. DOI: 10.2991/iwci-19.2019.45.

[28] Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization's information security. Business Informatics, 2017, no. 1(39), pp. 68-77. DOI: 10.17323/1998-0663.2017.1.68.77.

[29] E. D. Shishkina, "Bayesian networks as probabilistic graphical model for economical risk assessment," 2015 XVIII International Conference on Soft Computing and Measurements (SCM), 2015, pp. 24-26, doi: 10.1109/SCM.2015.7190400.

[30] N. Poluektova, T. Klebanova and L. Guryanova, "Risk Assessment of Corporate Infocommunication Systems Projects Using Bayesian Networks," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2018, pp. 31-34, doi: 10.1109/INFOCOMMST.2018.8632150.

[31] Sergei Petrenko, "2 Mathematical Framework for Immune Protection of Industry 4.0," in Developing a Cybersecurity Immune System for Industry 4.0 , River Publishers, 2020, pp.67-176.

[32] Anosov R., Anosov S., Shakhalov I. Formalized Risk-Oriented Model of the Information Technology System. Voprosy kiberbezopasnosti [Cybersecurity issues], 2020, No 5(39), pp. 69-76. DOI: 10.21681/2311-3456-2020-05-69-76

[33] Anosov R., Anosov S., Shakhalov I. Conceptual Model Of Information Technology Security Risk Analysis. [Cybersecurity issues], 2020, No 2 (36), pp. 2-10. DOI: 10.21681/2311-3456-2020-2-02-10.