ISSN 2347 - 3983
Volume 8. No. 7, July 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter163872020.pdf
https://doi.org/10.30534/ijeter/2020/163872020

Study the Methods of Internal Audit of Information Security in Organizations

Irgashyeva Durdona Yakubgjanovna[1], Xolimtayevalqbol Ubaydullayevna[2]
[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan
durdona.ya@gmail.com
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan
iqbola.xolimtaeva@gmail.com

ABSTRACT

This article presents a typical approach of security analysis, criteria for assessing security controls of a computer network and methods for assessing information security in organizations, taking into account the model for assessing information security processes. To organize an internal audit of information security in organizations, an approach is proposed for describing an object and forming a model of an intruder.

Key words: Vulnerabilities, unauthorized access, internal audit, content, interpretability, measurability, Intruder model, Markov process.

1. INTRODUCTION

Currently, information security of computer systems for various purposes continues to be an extremely acute problem and task. It can be stated that despite the efforts of numerous organizations involved in solving this problem, the general trend remains negative. There are two main reasons for the growing number of high-impact information security incidents in large organizations, according to data:

- the growing role of information technology in supporting business processes, as a result of the increasing requirements for information security of automated systems;
- increasing complexity of information processes. This imposes increased requirements on the qualifications of personnel responsible for ensuring information security.

The choice of adequate solutions that provide an acceptable level of information security at an acceptable level of costs is becoming an increasingly difficult task.
The first reason is objective; it can be opposed only by the organization's ability to meet the increasing requirements in the field of information security.
To neutralize the impact of the second reason, it is necessary to monitor the compliance of the qualifications of the personnel responsible for providing information security and the tasks at hand, to obtain an objective assessment of the state of the information security subsystem.
To solve these problems, organizations of auditors in the field of information security are created, aiming to conduct an examination of the compliance of the information security system with certain requirements, assess the information security management system, and improve the qualifications of specialists in the field of information security. The status of such organizations can be both state and independent international organizations. The idea of conducting an information security audit and certification of an information system for compliance with certain requirements is not new. The attestation system usually emerges simultaneously with the adoption of information security standards.

2. TYPICAL APPROACH OF SECURITY ANALYSIS

At the moment, there are a number of international security analysis approaches specified in the following documents: Open Source Security Testing Methodology Manual (OSSTMM), NIST SP800-15, The Information System Security Assessment Framework (ISSAF, PCI DSS).
Generalizing them, it can conclude that a typical method of security analysis should include the following steps:

1. Study of the initial data about the tested network.
2. Analysis of the composition, structure and configuration of critical elements of the network infrastructure.
3. Scanning of external network addresses of the tested network from the Internet.
4. Internal scanning of network resources.
5. Analysis of the network configuration, servers and workstations of the network using specialized security controls.
6. Processing of the received test results.

Security controls are used when testing both the network and its protection system. During testing, the used protection mechanisms are checked, their resistance to possible attacks, and vulnerabilities are searched [1]. A typical network security testing scheme includes the stages of planning, gathering information, identifying vulnerabilities, conducting test attacks on the system, and documenting. The planning process defines the goals and objectives of testing.
At the stage of collecting information, the identification of available network devices, network topology, open ports, etc. is carried out.
Further, the collected data about services and their versions are compared with information about known vulnerabilities. At the stage of confirming vulnerabilities,

the possibility of gaining unauthorized access to the system is illustrated.

3. AN APPROACH FOR COMPARATIVE ANALYSIS OF COMPUTER NETWORK SECURITY CONTROLS

A modern means of monitoring the security of computer networks should provide a reliable toolkit that can effectively provide a complex process of monitoring network security with minimal intervention of a specialist in routine scanning tasks. As an environment for testing security controls, a typical network of some informatization object is selected, including a class ***C***subnet (Table 1).

Table 1. Criteria for assessing security controls of a computer network

Criteria	Number of points
Port scan	
Correctly identified port openings	+1
Wrong port state detection	-1
OS identification	
Accurate OS identification	+3
Correct family identification	+1
Returning a list of possible families containing the correct answer	0
Incorrect OS identification	-1
Service identification	
Accurate service identification	+3
Exact identification of the service family	
Unidentified service	-1
Misidentified service	-3
Identifying vulnerabilities	
Exactly identified vulnerability	+2
False alarm	-1
Existing but identified vulnerability	-2

Security controls are installed inside the network perimeter, which provides access to all computers on the network and thereby allows you to get the most complete report on their security status. In the course of the comparative analysis, the assessment of the quality of identification of services, applications, vulnerabilities, analysis of the interface convenience and completeness of reporting are carried out [2].

Ease of work was assessed taking into account the following factors:

- the ability to create test profiles;
- the ability to rescan individual services;
- the quality of the submitted report;
- availability of additional functions, according to security assessment.

4. ASSESSMENT OF INFORMATION SECURITY BASED ON INDICATORS

A defining element of the process of conducting an audit of information security of organizations and systems is a model for assessing information security processes. The assessment model specifies a list and a reference model of the processes to be assessed for the information security audit object, determines the information security audit criteria and information security indicators, a method for evaluating processes using indicators, and a method for displaying the assessment results. The basis of the assessment model is the list and model of the evaluated processes and a set of indicators that are used to collect data and determine the degree of achievement of the process attributes of the established information security audit criteria.

An assessment model is considered in the form of a structure linking the information security measurement needs defined by the information security audit objectives with the corresponding processes. The assessment model describes how information security is quantified and how they are converted into indicators that provide a basis for making decisions about the degree of information security compliance with the established information security audit criteria, the degree of correctness of the organization's information security system processes. In general, the model for assessing the processes of ensuring information security of an organization can be represented by the structure shown in Figure.1.

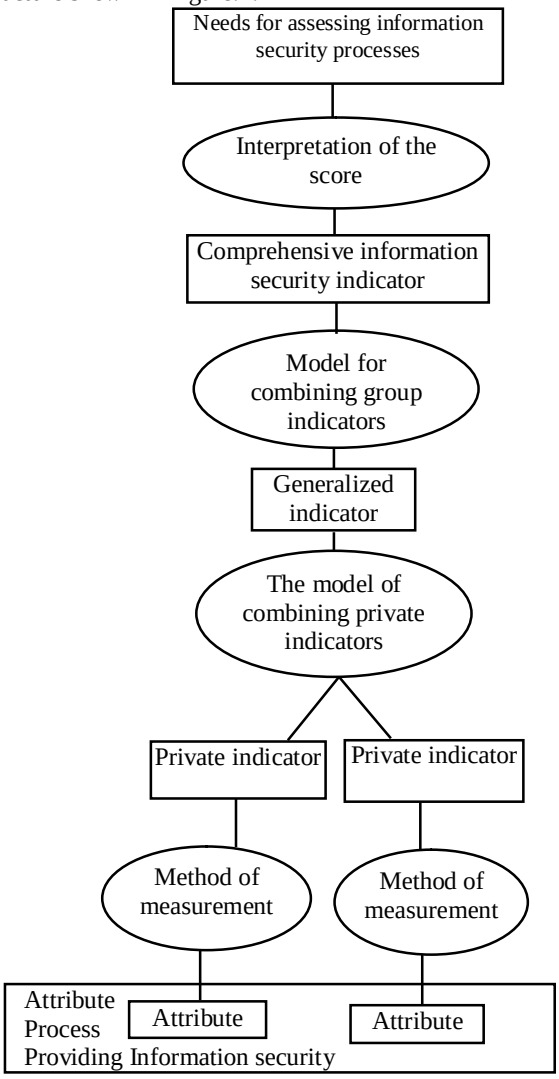

Figure 1: An assessment model for the organization's information security processes

An assessment model is considered in the form of a structure linking the information security measurement needs defined by the information security audit objectives with the corresponding processes. The assessment model describes how information security is quantified and how they are converted into indicators that provide a basis for making decisions about the degree of information security compliance with the established information security audit criteria, the degree of correctness of the organization's information security system processes. In general, the model for assessing the processes of ensuring information security of an organization can be represented by the structure shown in Figure.1.

5. INFORMATION SECURITY AUDIT OF ORGANIZATIONS AND SYSTEMS

A measurement method is a logical sequence of operations that is used to measure attributes in relation to a specific scale. Operations can include activities such as counting events or observing the passage of time. The same measurement method can be applied to many attributes.

The kind of measurement method depends on the nature of the operations used to measure the attribute. Two types can be defined:

1) subjective - a quantitative definition that includes a person's judgment;
2) objective - a quantitative definition based on calculations.

Possible examples of measurement methods include interviewing, observation, questionnaire survey, knowledge assessment, testing, data sampling. Some measurement methods can be implemented in many ways [3]. The measurement procedures used reflect the specific implementation of the measurement method in a given organization, in a given system.

The measurement method converts the value of a measured attribute into a value on a measurement scale. The type of scale depends on the nature of the relationship between the values on the scale. Examples of scale types:

- nominal: measurement values are categorical. For example, classifying defects by type does not imply order among the categories;
- ordinal: measurement values are ranked. For example, the severity distribution of defects is a ranking;
- interval: measurement values have equal distances corresponding to the same attribute values.A null value is not possible;
- ratio scale: dimension values have equal distances corresponding to the same attribute values, where a zero value corresponds to a zero attribute.

It is considered an assessment model based on indicators of the functioning of processes of the organization's information security system. Performance indicator$\boldsymbol{W}$process is a measure of the degree to which the actual result of the process corresponds to the required.

The main requirement when choosing a performance indicator is the compliance of the indicator with the process goal, which is displayed by the required result$\boldsymbol{Y}^{\mathrm{TP}}$.

For describing the correspondence of the real result$\boldsymbol{Y}$the required process, it is formally defined a numerical function on the set of results of the process:

$$\boldsymbol{P} = \boldsymbol{p}(\boldsymbol{Y}, \boldsymbol{Y}^{\mathrm{TP}}) \quad (1)$$

which is a conformance function showing the degree to which the process goal has been achieved. Thus, the indicator of the functioning of the process can be represented as:

$$\boldsymbol{W} = \boldsymbol{p}(\boldsymbol{Y}, \boldsymbol{Y}^{\mathrm{TP}}) \quad (2)$$

6. INTERNAL AUDIT OF INFORMATION SECURITY OF ORGANIZATIONS AND SYSTEMS

However, in order for the function (1) to be considered as an indicator of functioning, in addition to the requirement of compliance with the process goal, it must meet the following requirements: content, interpretability and measurability. Content means that when evaluating an indicator, all essential characteristics and properties (attributes) of the process are taken into account.

Interpretability is essential to understanding the results of the assessment. Measurability means that there is a measurement method for an indicator that provides reliable data and a trusted way of measuring.

If the process is assessed by a certain number of its attributes, then a vector indicator of functioning is introduced, combining particular indicators:

$$\boldsymbol{W_0} = < \boldsymbol{W_1}, \boldsymbol{W_2}, \dots, \boldsymbol{W_m} \quad (3)$$

where

$\boldsymbol{W_i j} = \boldsymbol{1}, \boldsymbol{m}$ determined by (2) with staging instead of$\boldsymbol{y}$,$\boldsymbol{Y}^{\mathrm{TP}}$quantities$\boldsymbol{y}$,

$\boldsymbol{Y}^{\mathrm{TP}}$private characteristics (attributes) of the process, i.e.$\boldsymbol{W} = \boldsymbol{p}(\boldsymbol{y_i y}^{\mathrm{TP}}), \boldsymbol{j} = \boldsymbol{1}, \boldsymbol{m}$.

The introduction of a vector performance indicator imposes additional requirements: the minimum number of particular indicators and completeness.

The requirement for the minimum number of particular indicators is associated with the desire to reduce the complexity of the assessment, however, while maintaining the completeness of the coverage of the characteristics and properties (attributes) of the process. Usually a vector indicator is introduced in cases where the goal of the process is achieved by solving several tasks, the efficiency of solving each of which is estimated by the corresponding private indicator$\boldsymbol{W_i}$, $\boldsymbol{j} = \overline{\boldsymbol{1}, \boldsymbol{m}}$.The size of the vector indicator is determined by the number of process attributes evaluated. Private indicators can have different dimensions. Therefore, when forming a generalized indicator, it is necessary to operate with the normalized values of indicators, which is required for their comparison. The value of a particular indicator can be presented as a percentage or shares.

Measuring information security can be based on imperfect information, therefore determining the accuracy or significance of the indicators is an important component of presenting the actual value of the indicator [4]. The accuracy of the indicators depends on the chosen measurement method, the source of the data, and the reliability of the data provided.

Subjective measurement methods depend on expert interpretation of process attributes. The accuracy of the estimates can be increased if, in addition or instead of them, the numerical values of the parameters of the information security processes are used. For example, to evaluate a particular indicator, a calculation method can be used, which consists in determining the proportion of

employees whose professional skills are assessed and whose professional suitability is assessed regularly.

Private indicators can be presented in the form of questionnaire questions, as implemented, for example, in the document NIST Special Publication 800-26 "Security Self-Assessment Guide for Information Technology Systems" and in BSIPAS56.

In this case, particular indicators are included in the metrics in the context of sources and evidence of information security auditthe method of calculating the indicator and,for example, can be presented in the form of a table (Table 2).

Table 2: Privatemetric

Parameter	Description
Private indicator of information security	Are all roles in the organization personalized and responsibilities established for their performance?
Measurement method	The proportion of roles that are personalized and for the performance of which responsibility is established
Information security self-assessment evidence	Are all roles that exist in the organization documented? Are employees responsible for performing roles specified in the relevant instructions? Is there documentary evidence that employees have been made aware of their role-playing responsibilities (for example, signing orders)? How many roles are personalized and for their execution established responsibility? How many roles are there in the organization?
Calculation method	The number of roles that are personalized and for the execution of which the responsibility / number of roles existing in the organization is established
Sources of evidence of information security assessment	Credit information security policy organizations. Role Provisions. Assignment of Responsibility Provisions. Orders for appointment, distribution of responsibilities between employees of the organization. Job (role) instructions of employees
Indicator	The goal for this indicator is to achieve

The more indicators that allow using calculations to evaluate the attributes of interest of processes, the higher the objectivity of evaluating processes with subjective measurement methods can be. With the help of private indicators of information security, the attributes of the processes of the information security system are assessed, and with the help of generalized indicators of information security, the processes of the information security system are evaluated. A private metric aggregation model is an algorithm or calculation that connects private metrics according to a specific rule.

The rule should be based on understanding or on assumptions about the expected relationship between the particular indicators.

Such a rule can be the allocation of significant particular indicators with the assignment of significance coefficients to them. The significance of particular indicators is determined by the degree of influence of the process attribute on the result of the process. In this case, the generalized indicator is calculated as follows:

$$\boldsymbol{W_0 = \sum a_i x W_i}, \quad (4)$$

where$\boldsymbol{a_i}$ −coefficients of significance of particular indicators$\boldsymbol{W_i}$;

$$\boldsymbol{\sum_{i=1}^{m} a_i = 1} \quad (5)$$

$\boldsymbol{m}$ −number of private indicators$\boldsymbol{W_i}$in the generalized indicator$\boldsymbol{W}$.

The model for combining private indicators can be built on the basis of the theory of utility, when the method of folding the vector (generalized) indicator using the preference system is used.

The unification rule can also be based on the system of preferences of some particular indicators over others, which makes it possible to evaluate the process, focusing on the preferred particular indicators.

For example, if the established preference system indicates a preference for a particular indicator$\boldsymbol{W_1}$over $\boldsymbol{W_2}$and$\boldsymbol{W_2}$over$\boldsymbol{W_3}$ ($\boldsymbol{W_1 > W_2 > W_3}$), then the process, assessed by the generalized indicator, can have a rating equal to the most preferred particular indicator.

A generalized metric aggregation model is also an algorithm or calculation that connects generalized metrics according to a specific rule. This rule can also be based on a preference system.

In this case, the assessment of the set of processes will reflect the assessment of the preferred generalized indicators. As a result of combining generalized information security indicators, a complex indicator will be obtained that reflects the information security of an organization and (or) system.

At choosing and forming private, generalized and complex indicators, for example, the following criteria should be taken into account:

- feasibility of data collection;
- availability of human resources to collect and manage data;
- ease of data collection;
- the degree of interference in the activities of personnel;
- availability of appropriate tools;
- ensuring confidentiality;
- potential resistance from data providers;
- ease of interpretation of the indicator by consumers and evaluators.

The interpretation of assessment results is an explanation linking the quantitative assessment of indicators with the need to measure network traffic in information security processes in the language of consumers of measurement results [5]. Such an interpretation may reflect, for example, a violation of information security properties, possible negative consequences for the organization's activities or the functioning of systems based on the results of assessment.

7. ORGANIZATION OF INTERNAL AUDIT OF INFORMATION SECURITY IN ORGANIZATIONS

To conduct an internal audit of information security, it is proposed in accordance with the following approach:

- description of the research object;
- formation of a model of the intruder;
- forming a threat model;
- assessment of significant threats;
- forecasting and assessing incidents based on subjective destabilizing factors;
- assessment of incidents by objective destabilizing factors;
- formation of requirements for the improvement or creation of an information security system.

Thus, we define the set of objects of the information system, formally presented in the form $s_i \in S$, where S –set of information system objects, $i \in 1 \ldots n$, and n –total number of objects. In general, the stage of describing the object of research is shown in Figure 2.

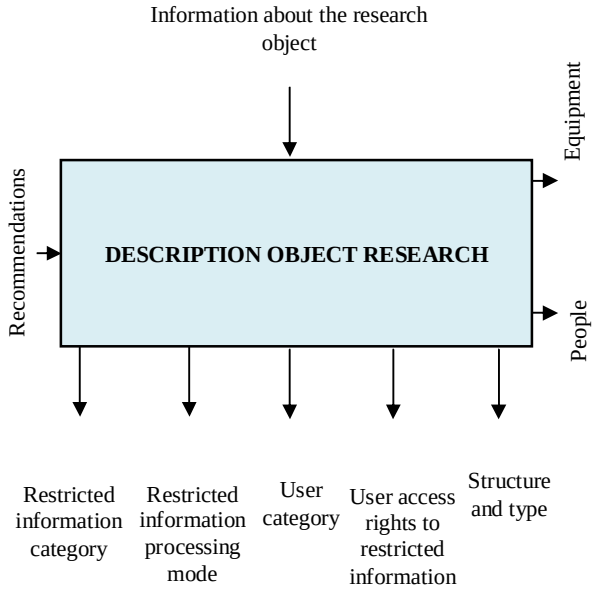

Figure 2: Scheme for describing object research

The information obtained as a result of the description of the information system is used in the formation of a model of violators. As output data, templates of violators as an object of attack are obtained. Each offender is characterized by different indicators, including the purpose of the attack, the target of the attack, the means of attack, etc. In general, the intruder's model is shown in Figure 3.

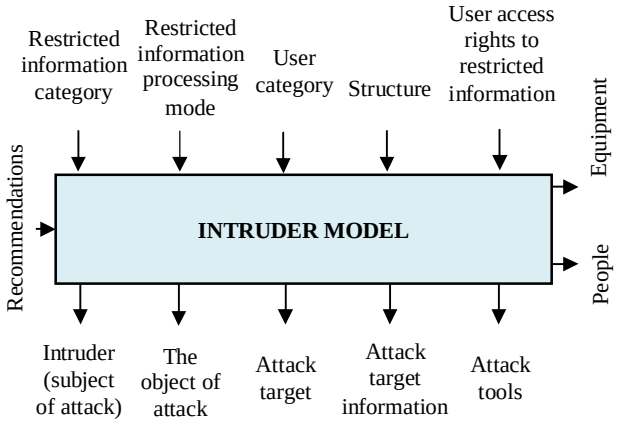

Figure 3: Intruder's model

Based on the violator model, three main classes of information security violators can be distinguished:

B −internal offenders who have the right to access the controlled area and the organization's information system (employees);

R −internal offenders who have the right to access the controlled area, but do not have access to the organization's information system (partners, clients);

Q −external offenders who do not have the right to physical access to the controlled area and to the organization's IP (hackers, criminal structures).

At the stage of forming the threat model, data from the intruder's model is received at the input, and at the output, destructive actions are generated for each object for each intruder [6-7]. From all possible destructive actions, many threats to information security are formed – $\{X\}$. In general terms, the threat model is shown in Figure 4.

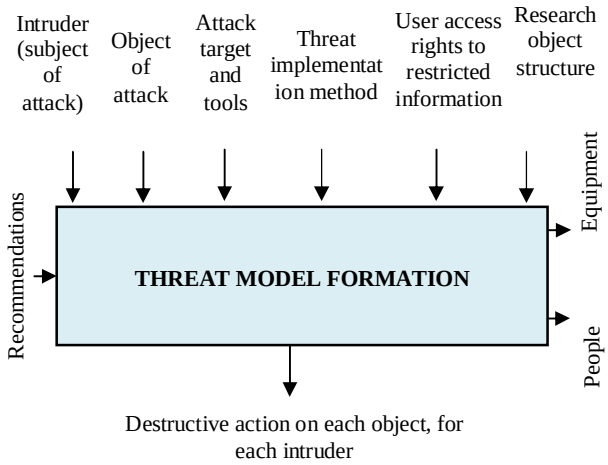

Figure 4: Threat model formation

At the stage of assessing significant threats, it is determined:

- probabilityofthreatrealization;
- the degree of influence of threats.

Probability of implementation of security threats$\boldsymbol{P_{X_j}}$, with scope$\boldsymbol{P}$ = [0,1] and many basic values$\boldsymbol{T_P}$={very low, low, medium, high, very high}=$\{\boldsymbol{a_{X_1}}, \boldsymbol{a_{X_2}}, \boldsymbol{a_{X_3}}, \boldsymbol{a_{X_4}}, \boldsymbol{a_{X_5}}\}$, is determined on the basis of expert assessments, taking into account the competence coefficient of each expert and an assessment of the consistency of expert opinions.

The degree of influence of information security threats$\boldsymbol{L_{Y_j}}$expertly assessed with scope$\boldsymbol{L} = [\boldsymbol{0}, \boldsymbol{1}]$and many basic values$\boldsymbol{T_L}$ = {light impact, moderate impact, heavy impact, critical impact, destructive impact} =$\{\boldsymbol{a_{Y_1}}, \boldsymbol{a_{Y_2}}, \boldsymbol{a_{Y_3}}, \boldsymbol{a_{Y_4}}, \boldsymbol{a_{Y_5}}\}$.

Significance of information security threat in information security strategy$\boldsymbol{F_{V_j}}$with scope$\boldsymbol{F} = [\boldsymbol{0}, \boldsymbol{1}]$and many basic values$\boldsymbol{T_L}$ = {insignificant, small, medium, large, destructive}= $\{\boldsymbol{a_{V_1}}, \boldsymbol{a_{V_2}}, \boldsymbol{a_{V_3}}, \boldsymbol{a_{V_4}}, \boldsymbol{a_{V_5}}\}$, graded according to the fuzzy statement system$\widetilde{\boldsymbol{L^1}}$.

$\widetilde{L^1}$

$$= \begin{cases} \widetilde{L_1^{(1)}}: < IF\ \mathrm{E}_{11}\ OR\ \mathrm{E}_{12}\ OR\ \mathrm{E}_{13}\ OR\ \mathrm{E}_{21}\ OR\ \mathrm{E}_{22}\ OR\ \mathrm{E}_{31}\ Then\ F_{V_j}\ is\ a_{V_1} >; \\ \widetilde{L_2^{(1)}}: < IF\ \mathrm{E}_{14}\ OR\ \mathrm{E}_{23}\ OR\ \mathrm{E}_{32}\ ORИ\ \mathrm{E}_{41}\ Then\ F_{V_j}\ is\ a_{V_2} >; \\ \widetilde{L_3^{(1)}}: < IF\ \mathrm{E}_{15}\ OR\ \mathrm{E}_{24}\ OR\ \mathrm{E}_{33}\ OR\ \mathrm{E}_{42}\ OR\ \mathrm{E}_{51}\ Then\ F_{V_j}\ is\ a_{V_3} >; \\ \widetilde{L_4^{(1)}}: < IF\ \mathrm{E}_{25}\ OR\ \mathrm{E}_{34}\ OR\ \mathrm{E}_{43}\ OR\ \mathrm{E}_{52}\ Then\ F_{V_j}\ is\ a_{V_4} >; \\ \widetilde{L_5^{(1)}}: < IF\ \mathrm{E}_{35}\ OR\ \mathrm{E}_{45}\ OR\ \mathrm{E}_{55}\ OR\ \mathrm{E}_{44}\ OR\ \mathrm{E}_{54}\ OR\ \mathrm{E}_{53}\ Then\ F_{V_j}\ is\ a_{V_5} >; \end{cases} \quad (6)$$

where

$\boldsymbol{E_{ji}}$ −statements like: <$\boldsymbol{P_X is a_{X_j} and L_Y is a_{Y_j}}$.

Thus, it is defined:

- many significant threats that an intruder can implement in the information system$x_{ij} \in \{X\}$, where$i \in 1 \dots kj \in 1 \dots m$, and$m$– total number of information security threats [8] and$k$– total number of information security violators;
- many significant threats to information security for each of the objects of the information system$x_{jS_i}\{X\}$and for each of the intruders$x_{i,jS_i} \in \{X\}$;
- many significant threats to information security for each object of the information system and for each intruder belonging to the classes:
  - confidentiality$\{K\} - k_{jS_i}, k_{i,jS_i} \in \{K\} \subset \{X\}$;
  - integrity$\{C\} - c_{jS_i}, c_{i,jS_i} \in \{C\} \subset \{X\}$;
  - availability$\{D\} - d_{jS_i}, d_{i,jS_i} \in \{D\} \subset \{X\}$.

The data obtained as a result of the stage of assessing significant threats are used at the next stage - forecasting and assessing the number of incidents by subjective destabilizing factors, which is proposed to be carried out according to the following approach:

- building a directed graph;
- construction of a matrix of transition probabilities;
- formation of the vector of intensity of the implementation of threats;
- formation of the vector of the initial state of the system;
- deterministic modeling of the Markov chain is carried out;
- simulation of the protocol of the Markov process is carried out;
- simulation modeling of the Markov process is carried out;
- the results are processed.

One of the key points of the forecasting methodology is the simulation of the Markov chain. At the first step of simulation, a uniform distribution is generated in the interval (0; 1) a random number R and the initial state of the Markov process is determined X0, at the zero step, that is, at the moment of time$\boldsymbol{t} = \boldsymbol{0}$:

$\boldsymbol{X_0 = min\{i = 0, 1, 2 \dots i - 1: R \le a_0^{(0)} + a_1^{(0)} + \dots + a_K^{(0)}\}}$. It is believed$\boldsymbol{k = X_0}$.

A random variable is generated W, having an exponential distribution with the parameterλ_i. It is believed$T_0=W$, where$T=(T_0,T_1,\dots,T_n)$ – moments of process jumps.

In the next step$\boldsymbol{l = 1, 2, \dots, n}$a uniform distribution is generated in the interval (0;1) random number$R$and the initial state of the Markov process is determinedX_l, at$l$–thstep, that is, at time$l$:

$\boldsymbol{X_l = min\{j = 0, 1, 2 \dots j - 1: R \le p_{i,0} + p_{i,1} + \dots + p_{i,j}\}}$. It is believed $k=X_1$.

A random variable is generated W, having an exponential distribution with the parameterλ_i. It is believed $T_l = T_{l-1} + W$. Go to step$l$+1.

At the output of the simulation of the Markov process, a matrix is obtained, the rows of which correspond to the amount of simulation of the Markov process, and the columns - to the moment in time$\boldsymbol{t}$. At their intersection is the number of the state of the system at the moment of time.

8.CONCLUSION

In conclusion, it should be noted that at analyzing the assessment of information security in organizations, taking into account the model for assessing information security processes, anapproach is proposed for describing an object and forming a model of an intruder to organize an internal audit of information security in organizations.

REFERENCES

[1] Calder, **Information Security Based on ISO 27001/ISO 27002 - A Management Guide** (2nd ed.), Zaltbommel: Van Haren Publishing, 2009.

[2] Springer Heidelberg Dordrecht London NewYork Library of Congress Control Number: 2009943513 © Springer-Verlag Berlin Heidelberg 2010 **Handbook of Information and Communication Security**. ISBN 978-3-642-04116-7.

[3] Wong JinKee, MohdFadzi Abdul Kadir, Fauziah Ab Wahab, AznidaHayatiZakaria@Mohamad, Mohamad Afendee Mohamed, Ahmad Faisal AmriAbidin@Bharun. **Mitigating Risk of Spectre and Meltdown Vulnerabilities**. International Journal of Emerging Trends in Engineering Research. Volume 8. No. 3, March 2020, Indexed in Scopus. – P. 2395-2401.

[4] M. Suduc, M. Bizoi and F. G. Filip, "**Ethical Aspects on Software Piracy and Information and Communication Technologies Misuse**", Preprints of IFAC SWIIS Conference, Bucharest, 2009.

[5] GulomovSherzodRajaboevich, XoshimovaCharosSaidaminovna, GaniyevaToxiraIrkinovna, Djurayeva Shoxista

Tagirovna. **Analysis of Methods for easuring Available Bandwidth and Classification of Network Traffic**. International Journal of Emerging Trends in Engineering Research. Volume 8. No. 6, June 2020. Indexed in Scopus. – P. 2753-2759 https://doi.org/10.30534/ijeter/2020/87862020

[6] P.Z. Manrique de Lara and D. V. Tacoronte, "**Supervising Employee Misuse of Information Systems in the Workplace: An Organizational Behavior Study**",Empresa global y mercados locales: XXI Congreso Anual AEDEM. 1, Madrid: Universidad Rey Juan Carlos, 2007, pp. 31-43

[7] Atymtayeva, L.B., G.K. Bortsova, A. Inoue and K.T. Kozhakhmet, 2012. **Methodology and ontology of expert system for information security audit**. Proceedings of the 6th International Conference on Soft Computing and Intelligent Systems and 13th International Symposium on Advanced Intelligence Systems, Nov. 20-24, IEEE Xplore Press, Kobe, Japan, pp: 238-243.

[8] Suduc, A.M., M. Bîzoi and F.G. Filip, 2010. **Audit for information systems security**. Inform. Econom, 14: pp.43-48. https://doi.org/10.3182/20100712-3-FR-2020.00010