ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 10 , October 2017

Modeling the Processes of Violation Security on Monitoring System

Nasrullaev Nurbek Baxtiyorovich, Bekmurodov Ulugbek Bakhromugli,
Khaydarov Sardor Fayzullaevich

PhD student, Department of Providing Information Security, Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan
Senior lecturer, Department of Providing Information Security, Samarkand Branch of the Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan
Assistant, Department of Cryptology and Discrete Mathematics, Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan

ABSTRACT. In this article the principles of evaluating the effectiveness of the violator's actions in the critical infrastructure are given. The operational complex of modeling of processes of infringement of information security is presented and uncertainties of modeling of the infringer and ways of their elimination are researched. A mathematical model of the aggregated index of the effectiveness of the violator's actions is proposed, which removes a number of limitations of existing probabilistic models of random phenomena in the field of information security.

I. INTRODUCTION

Informatization of resources on the basis of modern technology has made the security of the information infrastructure one of the most acute problems of our time. The process of informatization causes the emergence of new types of threats to information security, aimed primarily at management and life support systems of objects that are most exposed to destructive information impacts. The actual list of threats to information security (IS)should be determined by the results of modeling the possible actions of the violation information security. At present, the methodology for assessing the level of the violator's potential and the effectiveness of his unauthorized actions (UA) is not sufficiently formalized. In fact, the level is determined expertly according to criteria known to them only.

II. DECOMPOSITION FOR SECURITY PROPERTY OF THE INFO COMMUNICATION SYSTEM

At present, the development of the direction connected with the study of the safety of resources is hampered by the lack of unified notions about the essence of the concept of information security. These technological systems have higher risk levels in comparison with traditional info communication system, up to the disruption of the system's operation, emission of harmful substances, techno genic catastrophes and human victims. Therefore, in addition to ensuring confidentiality, integrity and accessibility of information, it is also necessary to consider the issue of technological process of security in the info communication system (ICS), which has properties such as observability, controllability, identifiability (Fig.1.1).

Therefore, the purpose of protecting the technological process is to ensure the requirements for controllability, observability and processability of the process. If these requirements are not fulfilled, destructive actions on the ICS of the technological process related to losses are possible:

– control ability of the technological process, including control locking and / or unauthorized management;
– process observability: modification of process parameters and / or falsification of sensor measurements;
– system operability: an accident (shutdown) of the process and / or degradation of computing resources [1,2].

All destructive influences on the ICS of the technological process are produced by three reasons: violation of availability (denial of service) of critical information, violation of its integrity and confidentiality.

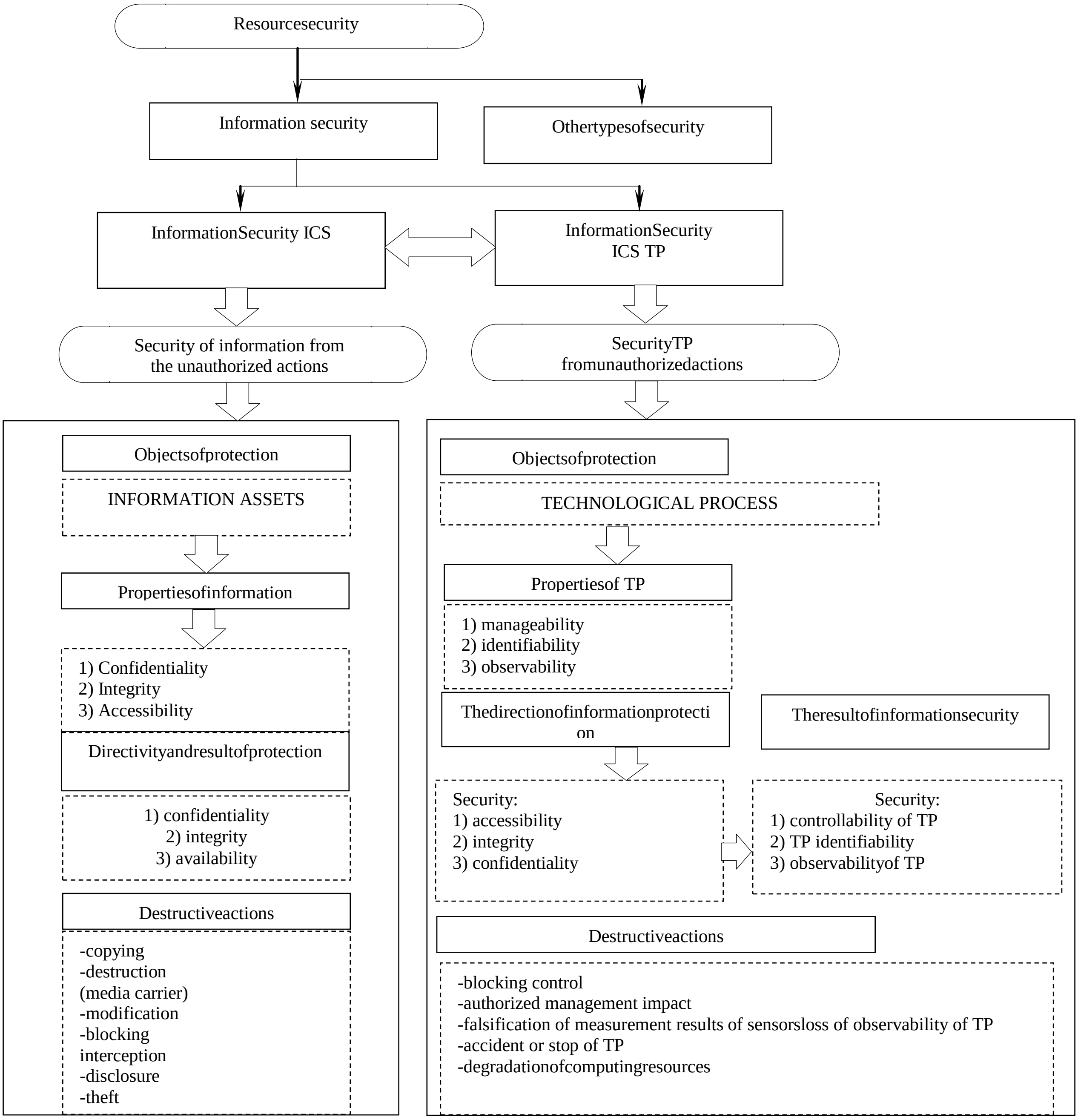

Fig.1.1. Decomposition of the security property of the info communication system of the technological process of resources.

Critically important information is the "technological" information fixed in the documentation for the technological process of the technological process, the destruction, blocking or distortion of which may lead to the disruption of the operation of theICS of the technological process, as well as information "about the ICS of the technological process and the technological process" The case of its theft can be used for destructive information effects on the ICS of the technological process. "Technological"information is:

– operational (dynamic) information (telemetry, telemeasurements, telecontrol) on the flow of a controlled process;

– archival (static) information (normative and technical documentation, process parameters and other archival information).

Guided by the basic principles and methods of qualimetry, it is suggested that the potential of the destroyer be characterized by a vector:

$$\mathrm{Y}^{\mathrm{P}}_{\langle \mathrm{D}\rangle} = \mathrm{Y}^{\mathrm{P}}_{\langle \mathrm{D}\rangle}(\mathrm{A}'_{\langle \mathrm{k}'\rangle};\ \mathrm{A}''_{\langle \mathrm{k}''\rangle};\ \mathrm{B}'_{\langle \mathrm{l}'\rangle};\ );\mathrm{k} = k'+k'', \mathrm{A}_{\langle k\rangle} =< A'_{\langle \mathrm{k}'\rangle} + \mathrm{A}''_{\langle \mathrm{k}''\rangle} > [2, 3, 4].$$

From the perspective of the efficiency theory of purposeful processes, the vector $\mathrm{Y}^{\mathrm{P}}_{\langle \mathrm{D}\rangle}$is an indicator of the virtual quality of the results of the unauthorized actions. It includes three groups of components: $\mathrm{Y}^{\mathrm{P}}_{\langle \mathrm{D}\rangle} =<v, r, \tau>$characterizing virtual (possible) target effects, where v is a measure of the target effects (efficiency of the unauthorized actions), the cost indicator resources (the resource intensity of the unauthorized actions), τ - the cost of operating time (the efficiency of the unauthorized actions). Each of the components of the vector $\mathrm{Y}^{\Pi}_{\langle 3\rangle}$ depends on the vectors $\mathrm{A}'_{\langle \mathrm{k}'\rangle}, \mathrm{A}''_{\langle \mathrm{k}''\rangle}, \mathrm{B}'_{\langle \mathrm{l}'\rangle}$, where $\mathrm{A}'_{\langle \mathrm{k}'\rangle}$- operational technical characteristics (OTP) and parameters of the system of unauthorized persons (SUA) of the violator; $\mathrm{A}''_{\langle \mathrm{k}''\rangle}$-operational technical characteristics and the parameters of the process of organization of the unauthorized actions (POUA)or the technology of unauthorized use; $B'_{\langle l'\rangle}$- characteristics of the functioning conditions (CHFC)of the system of unauthorized persons [3]. Under the system of unauthorized persons, we mean a set of software hardware the unauthorized actions. Under the characteristics of the functioning conditions of the unauthorized actions, we mean a set of factors that affect the parameters and operational technical characteristics of the system of unauthorized persons (vector $A'_{\langle k'\rangle}$, as well as the characteristics of the process of organization of the unauthorized actions (vector , $A''_{\langle k''\rangle}$) and them obeslovlivayuschie possible (virtual) $Y^{P}_{\langle D\rangle}$results of the unauthorized actions.The use of an infringer by an intruder occurs in the conditions of active counteraction of the protection system of the attacked ICS TP. Therefore, under the application conditions $\mathrm{B}''_{\langle \mathrm{l}''\rangle}$.the violator of the system of unauthorized persons will be understood as the set of mechanisms for protecting the attacked ICS TP. These protective mechanisms affect the situation in which the system of unauthorized persons will have to perform the task, and thus determine the required $\mathrm{Y}^{\partial}_{\langle 3\rangle}(\mathrm{B}''_{\langle \mathrm{l}''\rangle})$ for the offender results of the unauthorized actions, i.e. $\mathrm{Y}^{\mathrm{P}}_{\langle \mathrm{D}\rangle} \in \{\mathrm{Y}^{\mathrm{R}}_{\langle \mathrm{D}\rangle}\}$,, where $\mathrm{Y}^{\mathrm{R}}_{\langle \mathrm{D}\rangle}$- $v^{T}, r^{\mathrm{P}}, \tau^{D} >$,where v^{R} is the required (minimally admissible) target effect v, r^{M} - maximum (maximum allowable) resource costs r, τ^{D}- directive (maximum permissible) time τ.The relation $\mathrm{Y}^{\mathrm{P}}_{\langle 3\rangle} \in \{\mathrm{Y}^{\mathrm{R}}_{\langle 3\rangle}\}$is a formal expression of the target of the intruder's. The purpose of the unauthorized actions is determined by the violation of the functioning of technological processes.

The efficiency index of the unauthorized actions will be described by the vector.

$$\mathrm{Y}^{\mathrm{IA}}_{\langle \mathrm{D}\rangle} = \mathrm{Y}^{\mathrm{IA}}_{\langle \mathrm{D}\rangle}\left(\mathrm{A}'_{\langle \mathrm{k}'\rangle}, \mathrm{A}''_{\langle \mathrm{k}''\rangle}, \mathrm{B}'_{\langle \mathrm{l}'\rangle}, \mathrm{B}''_{\langle \mathrm{l}''\rangle}\right), \textit{where } \mathrm{A}'_{\langle \mathrm{k}'\rangle} = \mathrm{A}'_{\langle \mathrm{k}'\rangle}(\mathrm{B}'_{\langle \mathrm{l}'\rangle}, \mathrm{B}''_{\langle \mathrm{l}''\rangle}),$$
$$\mathrm{A}''_{\langle \mathrm{k}''\rangle} = \mathrm{A}''_{\langle \mathrm{k}''\rangle}(\mathrm{B}'_{\langle \mathrm{l}'\rangle}, \mathrm{B}''_{\langle \mathrm{l}''\rangle}), \mathrm{B}_{\langle l\rangle} =< \mathrm{B}'_{\langle \mathrm{l}'\rangle}+\mathrm{B}''_{\langle \mathrm{l}''\rangle} >, l=l'+l''.$$

III. THE STRUCTURAL DIAGRAM OF THE OPERATIONAL COMPLEX FOR MODELING THE PROCESSES OF INFORMATION SECURITY VIOLATION

The structural diagram of the operational complex for modeling the processes of information security violation is shown in Figure 2.2.We will reveal the content of the main elements of the operational complex unauthorized actions violator in the ICS TP:

DOF - direction of the offender;
PCB- is the unauthorized actions process control body;
CUV- conditions of use by the violator of the system of unauthorized persons.

It should be understood that the infringer (and implemented by him) in the info communication space for the protected party is represented in the form of dangerous processes - the processes of infringement of information security. These destructive processes together with the processes of defense (counteraction) form the so-called conflicting processes, and the study of the effectiveness of their counteraction to each other is an actual task.

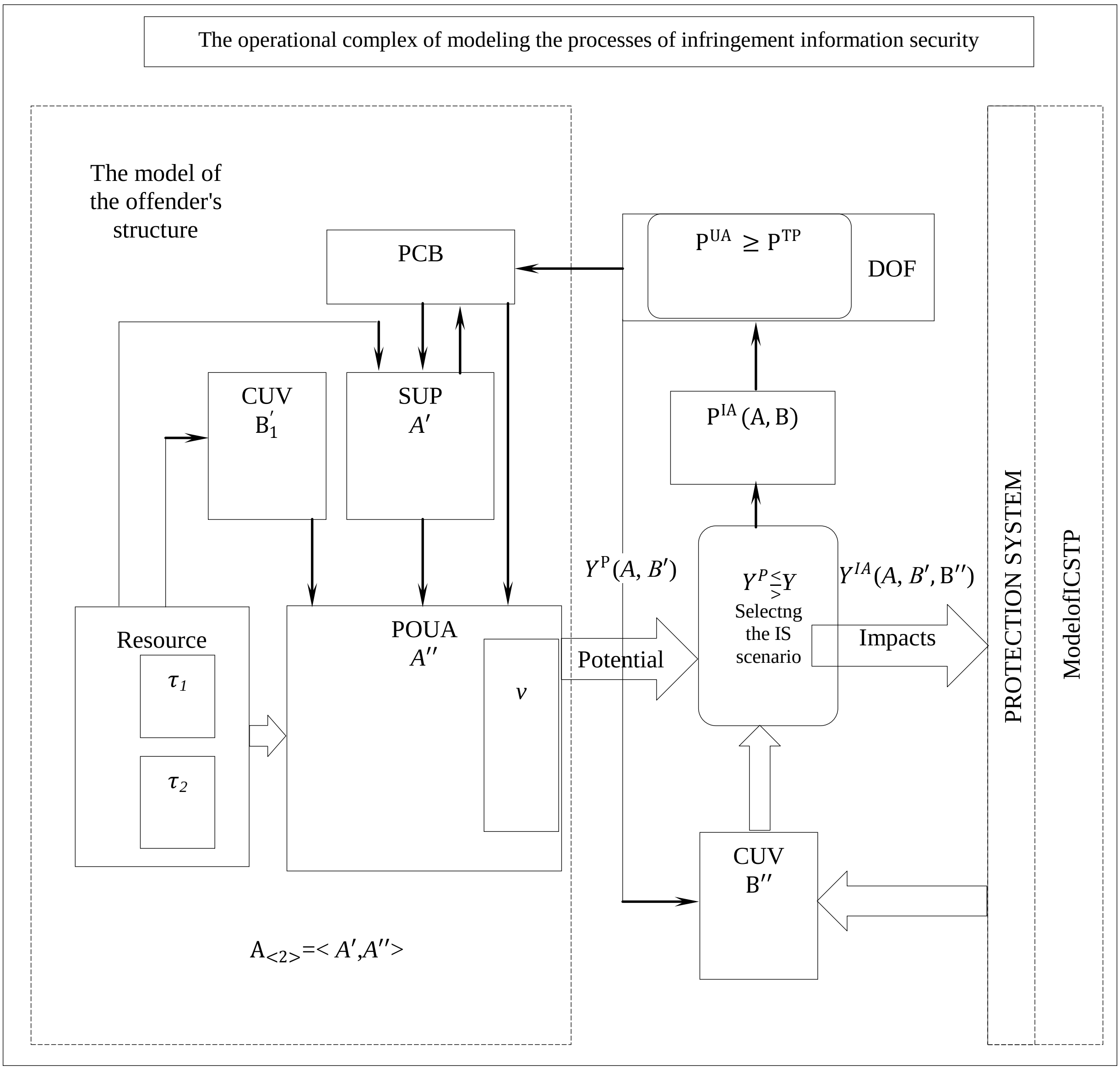

Fig. 2.2.Structural diagram of the operational complex for modeling the processes of infringement information security.

In essence, the potential $Y^{P}_{\langle D \rangle}$characterizes the intrinsic structure of the intruder and can be analytically represented differently: in the form of a pair <Str, Par>, where Str is the structure of the intruder, Par is the value of its parameters $A'_{\langle k' \rangle}, A''_{\langle k'' \rangle}, B'_{\langle l' \rangle}$. Knowledge of the structure and the Par parameters allows us to classify the enemy according to various criteria. Therefore, the characteristics of the offender will be described by the vector <Str, Par, Clas>, where class is the criterion for classifying the offender. Applying a different combination of the parameters$A'_{\langle k' \rangle}, A''_{\langle k'' \rangle}, B'_{\langle l' \rangle}$it is possible to classify the intruder in a number of aspects [4,5]. For example, with respect to the parameter $A''_{\langle k'' \rangle}$- the

type of the offense imputed by the intruder, by the parameter $B'_{\langle l'\rangle}$- the type of remote connection to the ICS TP. Therefore, in the course of the information security audit, it is first of all necessary to determine the class of the offender, and then to assess its potential.
The process of modeling an intruder includes uncertainties:
Type 1. Mathematical structure of the intruder - uncertainty of the potential of the offender $\hat{Y}^{P}(\hat{A},\hat{B})$.
Type 2. The criterion of choice by theoffenderofthescriptis unauthorized actions - $\hat{Y}^{P} \overset{\geq}{\underset{<}{-}} \hat{Y}^{IA}$
Type 3. The index of the quality of the results of the unauthorized actions–

$$\hat{Y}^{P} \overset{\geq}{\underset{<}{-}} \hat{Y}^{IA}$$

Duetothefact that both the violator and the system have to be protected from it under uncertainty, the values of the parameters of the vectors$\widehat{A}_{\langle k\rangle}$and $\hat{B}_{\langle l\rangle}$turnouttobe random (Q is the symbol of the random variable), and, consequently, and the vectors $\hat{Y}^{P}$and$\widehat{Y}^{UA}_{\langle D\rangle}$ likewisewillalsobe random.
Moreover, the pre-admissible values $\hat{Y}^{\partial}_{\langle 3\rangle}$of the vector $\hat{Y}^{P}$, depending on the defense system , $\widehat{B}''_{\langle l''\rangle}$attacked bythe ICS, are a priori random, The attacker himself and the goal of the operation, set by him, are unknown.
There solution of the uncertainties of the first and second types allows us to construct a model of the violator, and the removal of uncertainties of the second and third types is a model of the processes of infringement of information security of the ICS. Figure 2.3 shows a schematic diagram illustrating the relationship of the above uncertainties. The uncertainty diagram

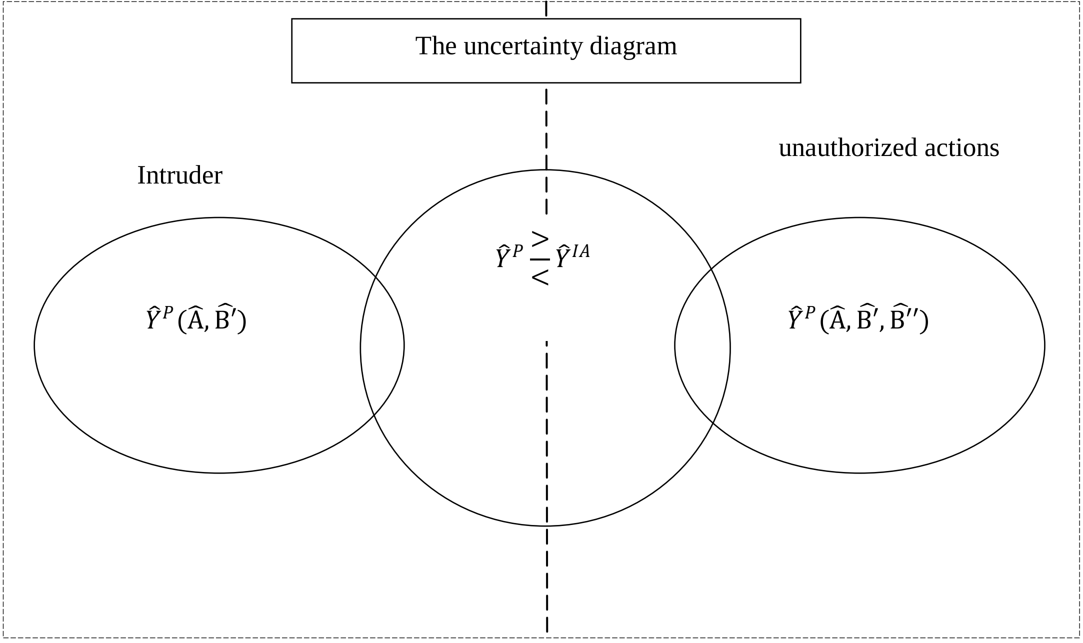
The uncertainty diagram
Intruder
unauthorized actions
$\hat{Y}^{P}(\widehat{A},\widehat{B}')$
$\hat{Y}^{P} \overset{\geq}{\underset{<}{-}} \hat{Y}^{IA}$
$\hat{Y}^{P}(\widehat{A},\widehat{B}',\widehat{B}'')$

Fig. 2.3.Schematic diagram illustrating the relationship of uncertainties of the modeling process of the intruder and his actions.

The uncertainties that the researcher faces in modeling the offender's actions are discussed in more detail below.

First, the introduction of uncertainty in the mathematical structure of the violator, described by the vector$\hat{Y}^{P}_{\langle D\rangle}$, allows you to reflect in the simulation the actual incompleteness of information about the destroyer.
The extreme case of uncertainty is unstructurability, tha tis, the impossibility of constructing an appropriate model of the violator belonging to one or another type of mathematical structure. To remove this "structural" uncertainty, it is possible to offer a technology for masking information resources of ICS TP. This technology allows:

- detectthehiddenchannelsoftheunauthorizedintrusiononinformationresources;
- Form reflexive control of the intruder with the help of a deceptive information – computing environment, the parameters of which are described by the vector$\widehat{B}'^{*}_{\langle l'\rangle}$.

The purpose of masking is the identification (building a model) of the offender, that is, determining the values of the parameters$\widehat{A}^{'}_{\langle k^{'}\rangle}, \widehat{A}^{''}_{\langle k^{''}\rangle}$. and forming vector $\hat{Y}^{P}_{\langle D\rangle}$. This is achieved by creating a falseideaof the offender about the object of attack by substituting $\widehat{B}^{'}_{\langle l^{'}\rangle}$ on $\widehat{B}^{'*}_{\langle l^{'}\rangle}$. As a consequence, the possibility of a comprehensive study of the structureisbeingrealized; estimatingthepotential$\hat{Y}^{P}_{\langle D\rangle}$; determinethelistoftheirprotectivemeasures , $\widehat{B}^{''}_{\langle l^{''}\rangle}$.

Secondly, there is an uncertainty in the assignment of basic sets and relations on the basis of which the model of the violator is built. To determine the quantitative measure of such uncertainty, one can use the stochastic approach (stochastic structures), based on the fundamental provisions of probability theory and mathematical statistics, or an approach from the position of the theory of fuzzy sets (fuzzy structures).

The idea is to investigate the uncertainty of the choice of the offender of one or another scenario of the implementation of the unauthorized actions [6]. For this approach, the problem of determining the potential $\hat{Y}^{P}_{\langle 3\rangle}$isnotput, since the values of the parameters$\widehat{A}^{'}_{\langle k^{'}\rangle}, \widehat{A}^{''}_{\langle k^{''}\rangle}$ areunknown.

It is proposed to evaluate the violator in the types$U = \{U_i\}_{i=1}^{N}$.

– The corresponding possible threats of IW and in the "mechanism of choice" $\zeta(\ \eta^{i}_{j}\ )$ ofthescenariooftheconcretethreat$\eta^{i}_{j} \in U_i$. That is, as a model of the offender, his profile <U, ζ> is considered. Before choosing$\zeta(\eta^{i}_{j})$ scenario, theintrudercounters:

– Process of studying the specifics of the ICS TP and identifying the vectors$\widehat{B}^{'}_{\langle l^{'}\rangle}and\widehat{B}^{''}_{\langle l^{''}\rangle}$;

– When comparing $\hat{Y}^{P} \overset{\geq}{\underset{<}{}} \hat{Y}^{IA}$ anddeterminingthepermissiblevalues $Y^{\partial}_{\langle 3\rangle}$ ($B^{''}_{\langle l^{''}\rangle}$) ofthevector $Y^{P}_{\langle 3\rangle}$ of the potential possibilities.

It seems obvious that it is irrational to talk about the stochastic nature of IA since the intruder does not make his choice at random. His choice is purposeful and conditioned by a certain criterion of choice.

Then we can say that the "selection mechanism" $\zeta(\eta^{i}_{j})$ ischaracterizedbythe presence of some unknown (random) factors. In this case, it is necessary to introduce an assumption - the information security auditor knows a lot of typical information technology threats and scenarios for their implementation. This access is completely justified, since the list of typical information technology threats is really known.

We will distinguish three types of possible situations. To the first type we refer the situation when the set of threats and the criterion for choosing ζ are known. In this situation, the profile are broken, it is only possible to quickly organize the appropriate protection. This type includes a situation in which a lot of threats U are known, and the criterion for choosing ζ is unknown. In this case, the process of managing security is similar to the process of the game. The solution of these problems can be solved using a special section of mathematics.

However, game theory, like a mathematical apparatus, suffers from conceptual incompleteness. So, in a real conflict, the list of possible threats U and the scenarios for their implementation is just unknown, and the best solution for the violator in a conflict situation is often to go beyond the known scenarios of system of unauthorized persons.

The third type includes situations where a lot of U threats, or rather the scenarios for their implementation, are unknown. In this situation, the protection system should be able to quickly suppress unknown unauthorized attempts to timely configure the protection mechanisms and / or counter impacts. To this end, the protection system should be endowed with a principally new property that allows it to promptly anticipate the realization of unknown threats U and prepare them in time.

Thirdly, the level of uncertainty (randomness) of the quality index of the results of the unauthorized actions $\hat{Y}^{UA}_{\langle D\rangle} = \hat{Y}^{UA}_{\langle D\rangle}\left(\widehat{A}_{\langle k\rangle}, \hat{B}_{\langle l\rangle}\right)$, usingtheprofile<U,ζ>, It is characterized by the probability P^{IA}_{D}ofachievingthegoal of the operation, and is an indicator of the effectiveness of the unauthorized actions. Indeed, the vectors $\widehat{A}_{\langle k\rangle}$, $\widehat{B}^{'}_{\langle l^{'}\rangle}$ a, therefore, and$Y^{P}_{\langle D\rangle}$renderturnoutto be random. Moreover, the admissible values $\hat{Y}^{IA}_{\langle D\rangle}$ofthevector$\hat{Y}^{P}_{\langle D\rangle}$are also a priori random,

$$\begin{cases}\hat{Y}^{P}_{\langle D\rangle} = Y^{P}_{\langle D\rangle}\left(\widehat{A}_{\langle k\rangle}, \widehat{B}^{'}_{\langle l^{'}\rangle}\right),\\ \hat{Y}^{IA}_{\langle D\rangle} = Y^{IA}_{\langle D\rangle}\left(\widehat{B}^{''}_{\langle l^{''}\rangle}\right).\end{cases}$$

Since under real conditions the suitability criterion of the unauthorized actions takes on the form $G_{Ц}$:$\hat{Y}^{P}_{\langle D\rangle} \epsilon, \hat{Y}^{\partial}_{\langle 3\rangle}$then$P^{IA}_{D} = P(\hat{Y}^{P}_{\langle D\rangle} \epsilon, \{\hat{Y}^{IA}_{\langle D\rangle}\})$.Apparently, thefactof the suitability of the results of an operation is a random event. Therefore, the measure of achievement of the target by the offender is a probabilistic characteristic.

To calculateP^{IA}_{D} , it is sufficient (but not necessary) to determine conditions for the realization of threats that are favorable for the offender with a profile <U,ζ>.Under the conditions of the implementation of the ICT, it is understood that the infringehas information:

- On the structure and characteristics of ICS;
- About the presence of vulnerabilities of the software And hardware and protection system.

The methods for assessing the potential of the violator and the effectiveness of its impact are conceptual in nature. Therefore, in the course of monitoring, expert assessments of the offender in types U of possible threats of information security, which he is able to perform, are widely used. Accordingly, the intruder model should determine the intruder's preferences for choosing potentially attacking actions - the elementary events of infringement of information security, from which various scenarios for the realization of the threat of unauthorized attacks are formed. That is, the security administrator faces the task of minimizing the power of the set U. In the formulation of this problem, the following assumptions can be made about the availability of data [7]:

- level of knowledge and competence of the offender;
- the initial location of the intruder in ICS, whichdeterminesthelistofresourcesavailabletohumanthebasisofsomeformalmodel;
- initial rights of the in fringer, limiting a lot of unauthorized actions, on the basis queried conditions for the implementation of the unauthorized actions.

One can distinguish priori $N^A$and a posteriori $N^P$of the intruder model. The first type is the model, the list of parameters and their values are determined without reference to the structure of the research ICS. Its structure is determined by hypotheses put forward by auditors on the basis of available a priori data. As a result, the a priori model of the offender, taking into account his preferences for the choice of potentially possible attacking actions, is as follows:

$$N^A = <Z, H, K, G>,$$

Where Z is the initial knowledge of the intruder about each attacked resource and the access rights that this violator has; H - resources to which the intruder has physical or remote accesses before the attack begins; K - the level of competence of the offender, that is, classes or lists of available attacking actions, both based on vulnerabilities of varying criticality, and on various methods of collecting information; G - the main objectives of the violation, for example, violation of controllability, observability or identifiability of TP.

Tomodeltheactions of the violator, an adequate mapping of its structure, it will be necessary to develop a model ontological model for representing knowledge about violators. Further, for example, during the analysis of the state of the information security, "saturate" it with expert data (hypotheses) about the offender with reference to a particular ICS TP, thereby forming BZ^N knowledge base about the offender.

The proper functioning of the technological process depends on the quality of the work of many other production processes, the violation of which is the target of the offender's misconduct. Then we can say that the output of the developed operational complex is a set of stochastic super indicators that correspond to the set of goals of the offender's IDS. In a complex, these super indicators give some sort of integral indicator-indicator. The physical meaning of this indicator is characterized by the quality of the system of protection against the intruder; a relative evaluation of the security of the ICS TP and a measure of the uncertainty of the situation in which the violator operates.

The study of the dynamics of the values of the indicator taken by him during the operation of the operational complex will later reveal both the fact of the presence of the intruder in the ICS TP and the scenarios of the unauthorized actions available to him.

IV. CONCLUSION

It should be noted that the prognostic capabilities of the operational complex allow investigating the intruder at the current time and also to generate new models of the intruder ahead of time, to investigate their capabilities and offer various options for protection.

REFERENCES

[1]. Gorniak, S., Ikonomou, D., Saragiotis, P. et al., Priorities for Research on Current and Emerging Network Trends. European Network and Information Security Agency. 2010.

[2]. Marin, G.A., "Network security basics", *Security & Privacy, IEEE*, vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.

[3]. K. Benton, L. J. Camp, and C. Small, "OpenFlow Vulnerability Assessment," in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 151–152.

[4]. S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN Security: A Survey," in IEEE SDN for Future Networks and Services (SDN4FNS), 2013, pp. 1–7.

[5]. D. Li, X. Hong, and J. Bowman, "Evaluation of Security Vulnerabilities by Using ProtoGENI as a Launchpad," in Global Telecommunications Conference (GLOBECOM 2011). IEEE, 2011, pp. 1–6.

[6]. Kotenko and E. Doynikova, "Security assessment of computer networks based on attack graphs and security events," Bali, Indonesia, LNCS, vol. 8047. Springer-Verlag, April 2014, pp. 462–471.

[7]. WilkoHenecka, Stefan Kogl, Ahmad-Reza Sadeghi, Thomas Schneider, and ImmoWehrenberg. TASTY: Tool for Automating Secure Two-Party Computations. In *ACM Conference on Computer and Communications Security (CCS)*, 2010.