UDC 004.43(031):681.3.01(02)
DOI: 10.15587/1729-4061.2022.269030

# APPLICATION OF THE PRINCIPLE OF INFORMATION OBJECTS DESCRIPTION FORMALIZATION FOR THE DESIGN OF INFORMATION PROTECTION SYSTEMS

**Vladimir Lutsenko**
PhD, Associate Professor,
Senior Researcher*
**Dmytro Progonov**
*Corresponding author*
E-mail: progonov@gmail.com
*Department of Information Security
National Technical University «Igor Sikorsky Kyiv Polytechnic Institute»
Peremohy ave., 37, Kyiv, Ukraine, 03056

***The development of information independence of the State requires the introduction of the latest technologies for analyzing, storing, processing, and transmitting information. The focus of this work is improving information security systems with limited access, in particular the development of new methods of designing such systems, which are characterized by minimal influence of the subject-designer on the design process. The object of the study is the methodology and means of designing systems for restricting and controlling physical access, as well as access to information at objects of information activity and information and telecommunication systems of Ukraine.***

***To exclude the influence of the subject of the designer, it is necessary to improve the design process itself. In this paper, the possibility of creating an automatic design system based on the representation of protection objects in the form of objects of a common structure has been mathematically proved. Such a structure combines both telecommunication objects and objects of information activity. Changes in the legislative, regulatory, and technical bases of information protection necessary for the implementation of the proposed system have been determined, in particular, granting the State Communications Committee of Ukraine new powers that ensure the balance of interests of the customer of protection systems and executors. The possibility of formalizing the representation of data on arbitrary objects of protection is shown. This representation makes it possible to create open library semantic databases with incomplete data on the object of protection.***

***A theoretical base has been built that makes it possible to determine the correspondence between the set of threats to the information security of the object and the unambiguous corresponding list of countermeasures. At the same time, information protection projects are distinguished by evolution and uniformity of choice of a set of means of protection to any threats to objects of arbitrary complexity***

***Keywords: databases with incomplete information, automatic designer of information security systems, object of protection of the general structure***

*Received date 03.10.2022*
*Accepted date 05.12.2022*
*Published date 30.12.2022*

***How to Cite:*** *Lutsenko, V., Progonov, D. (2022). Application of the principle of information objects description formalization for the design of information protection systems. Eastern-European Journal of Enterprise Technologies, 6 (9 (120)), 28–37. doi: https://doi.org/10.15587/1729-4061.2022.269030*

## 1. Introduction

Any project of an information security system (ISS) [1] or an integrated information security system (IISS) should determine the real security of protected objects in accordance with DSTU 3396.0-97 and DSTU ND TZI 3.7-003-05. There are no special problems with the documents of general access in the branches of legal norms, regarding the regulatory framework and methodological support. And in the field of technical protection of information (TPI), including for example, when creating a high-quality model of threats and designing protection systems, there is a significant imperfection. In general, this is due to an objective lag in the development of this direction. In Ukraine, ISS and IISS have not been developed as a methodology that is an element of the State Policy. That is, there are currently factors that indicate a technological crisis that predetermines the relevance of the topic. In particular, there is no completed design concept. Especially such design, which does not depend on the designer, that is, computer-aided design [1].

## 2. Literature review and problem statement

In the direction associated with the design of IISS, improvement can be achieved if we consider the creation of a system for protecting objects in the complex. At the same time, it is necessary to combine into a single process such stages as inspection and description of the object, design of a mature and financially minimized protection system, post-project audit, which is systematically considered in [2], or pre-project audit, which, due to its increased complexity, is considered fragmentary in many works, for example, [3–5].

A specialist in the development of ISS projects should be a specialist in technical and organizational protection systems, as well as in legal and legal issues. And technical protection involves the use of information technology, system analysis, modeling of complex systems, optimal search for solutions for fuzzy or incomplete data, the use of cryptography and steganalysis methods [6].

Developers of IISS systems are trying to develop new, progressive approaches to the creation of design tools for access restriction and information protection systems. For example, there is a well-known approach based on the evolutionary architecture of a complex information system [7]. This approach is configured to create a model of the object's behavior and its state. It is based on the representation of the method of creating a description of the object and the model of event management in the form of some image, which the author of [7] calls Statechart [8–10]. As events, current behavior is considered in a general sequence.

A set of models of possible behaviors (a library of possible behavior patterns) are also represented in the form of behavior images – Viewchart. At the same time, Viewcharts images are based on Statecharts and develop them at the same time. Creating a description of objects is carried out by using a set of tools called Statemate. Thus, the Statechart determines what the object was and what it will be. Viewchart, in fact, is a set of data representations (in the author's version – images) taking into account the tendency regarding the sequence of states of the object. Images can be histograms of states either in a time sequence or in a sequence of possible states that can be created either simultaneously or in a time sequence. With this approach, the creation of a design methodology is reduced to the creation of formalized, that is, mathematical tools (Statemate), used as functions of the relationship between possible Statecharts and existing Statecharts.

This approach to creating models of information protection is promising. But the quality indicators of the protection project remain uncertain if the project is based on such models. The protection project, at the same time, is not the final technological product but is one of the possible options for the final technological product. In addition, on such principles, we are not talking about the objectivity of decisions in the design, or about the optimization of the project in relation to any design parameter.

In general, these and other approaches lead to the possibility of formalizing the description of protection objects and can help in creating an automatic design system, or at least as computer-aided design tools.

A method of risk analysis and management, such as CRAMM, can be considered close (the UK Government Risk Analysis and Management Method, UK, 1985). It is a versatile tool for conducting IS surveys, analyzing risks, conducting an audit for compliance with the requirements of the British Government and BS 7799, developing a security policy and a plan for ensuring business continuity. But in this case, the CRAMM method may not be useful to us. The reason is that it cannot be used independently as a «designer» of the protection system, taking into account the results of its survey, and risk analysis.

The Cobra method is a means of risk analysis and conformity assessment of IS in accordance with BS7799 and GOST R ISO/MEC 17799-2005 standards in information technology. Risk assessment here is carried out quantitatively. Tools for consulting and security reviews are being implemented, there is a large database of threats and vulnerabilities. A large number of questionnaires are used, which leads to the subjectivity of decisions, especially if the survey statistics are insufficient and determining the degree of sufficiency is an ambiguous question.

The Risk Watch method (America) is implemented in the form of a software product and is a means of analyzing and managing risks. It uses different types of security audits, the choice of which is given to the user for consideration. But this method also does not make it possible to use security audit and independently, automatically design a protection system. That is, Risk Watch is also not a designer.

The Buddy System method of the company «Consultation Objective and Bi-Functional Risk Analysis» is an international methodology created according to the project of the European Union [11]. This is a method of risk analysis and conformity assessment of ISO 17799. The method is a software product that implements both quantitative and qualitative risk analysis. It has developed means of generating reports. Particular attention is paid to the risks associated with physical security violations. But the focus is on project management, not the design procedure.

If we consider these (as well as others, such as EBIOS, MEHARI, OCTAVE, CORAS, Vulture) implementations of analysis methods, it is necessary to determine the degree of adaptability of these implementations to the characteristics of Ukrainian users. At the same time, it is necessary to take into account the peculiarities of the legislation and standards of Ukraine, the peculiarities of relations between user organizations within the framework of the existing infrastructure, local and regional peculiarities in creating the structure of IS, requirements for working and reporting documentation, traditions. From this point of view, the product Buddy System is probably the closest to domestic requirements.

That is, all known methods are means of risk analysis, and not «designers». And their modification cannot create a new automatic «designer» due to the inconsistency of the standards of different States and the regulatory and methodological framework.

The result of the audit is often a certificate of compliance of the surveyed IS with the requirements of international standards. This provides a competitive advantage associated with greater trust from customers. At the same time, the standard GOST R ISO/MEC 17799–2005 is the basis for any work in the field of information security and audit but is not a design system [12].

It should be noted that in most cases, the developers of IISS design systems try to significantly improve each of the design stages separately, or to adapt to the requirements of international standards [6]. The creation of new approaches is hampered for objective reasons, the main of which are: the complexity of the task; financial restrictions of performers in the absence of state support; the need to attract qualified specialists from various technological industries. Therefore, it is necessary to develop a methodology for designing IISS, which makes it possible to minimize the influence of subjective factors, in particular, giving preference to IISS developers to certain solutions, while ensuring a given level of quality of the information security system.

## 3. The aim and objectives of the study

The aim of this work is to create a methodology for objectively effective design of information security systems circulating at information activity objects (IAO) and information and telecommunication systems (ITCS). This creates the prerequisites for the development of a new methodology for designing ISS or IISS.

To accomplish the aim, the following tasks have been set:

– to define the concept of structures of objects of protection for the description of objects of any complexity, from individual allocated premises (AP) to ITCS and IAO structures of regional-territorial scale, for example: object, district, city, regional, etc.;

– to propose changes in the list of clusters of protective equipment that will make it possible to describe objects of any complexity in a single way, regardless of restrictions or prohibitions on the use of these means of protection;

– to provide a basis for possible variants of the structures of objects of protection of the general structure (OPGS) and formulate rules for choosing means of protection for them;

– to prove the uniformity in determining the links between threats, counteractions and structures of objects when using restrictions and prohibitions in the means of protection.

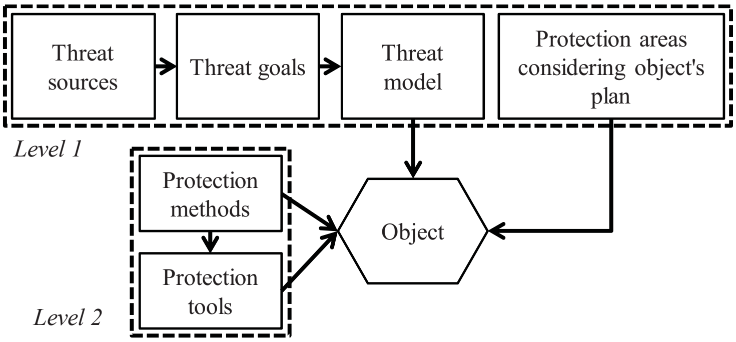

Fig. 1. The sequence of decision-making in the design of information security systems and integrated information security systems

## 4. The study materials and methods

The object of the study is the process of creating systems for restricting and controlling physical access, as well as access to information at the objects of information activity and in the information and telecommunication systems of the State. When conducting the study, a common representation of the sequence of design stages as two logical levels of decision-making is used, as shown in Fig. 1.

Meaningfully, at level 1, the possible actions of the intruder are determined in determining the threats to the object, which, in turn, determine the possible directions of protection. At level 2, possible counteractions from the side of the object are determined.

At the same time, a separately automated system (AS) as an ITCS body, and separately an IAO that does not contain ITCS in its composition, are represented in their totality in the form of some complex object we will call «the object of protection of the overall structure».

The main idea in the implementation of the design stages of the objects of protection of the general structure (OPGS) is to compile lists (Names) of factors that create threats and collectively represent the Image of Threats, and the corresponding lists (Names) of areas of protection, which similarly constitute the Image of Protection. The next step is to determine the specific methods and means of protection according to the Image of Protection, that is, to create an Image of the Protected Project. At first glance, the task is not difficult, but it is so provided that these lists (Names) are objectively unambiguous, regardless of the specific author of the project. Then it would be possible to put the Image of Threats in accordance with the Image of Protection and then the Image of Protection in accordance with the Image of the Protected Project. This correspondence would mean the possibility of creating rules for the transition from one stage to another (the definition of relationships between stages is possible, for example, in the form of directed graphs, or mathematically in the language of finite automata FSM, etc.

In the language of the Euler-Ven formulas, possible OPGS (the basis of OPGSS) are defined as shown in Fig. 2.

It is also possible to represent a description of the variants of the structures of OPGS according to Table 1.

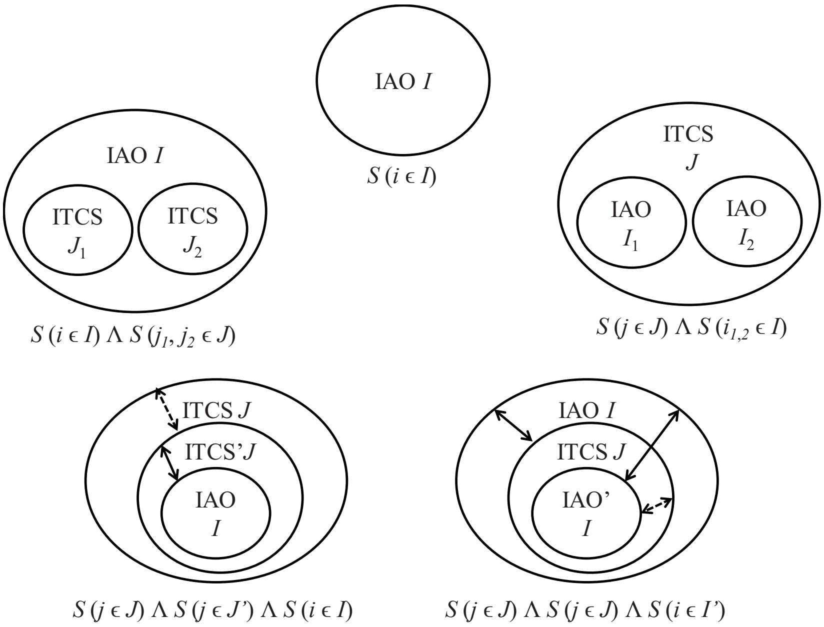
IAO $I$
$S\ (i \in I)$
IAO $I$
ITCS $J_1$
ITCS $J_2$
$S\ (i \in I) \wedge S\ (j_1, j_2 \in J)$
ITCS $J$
IAO $I_1$
IAO $I_2$
$S\ (j \in J) \wedge S\ (i_{1,2} \in I)$
ITCS $J$
ITCS'$J$
IAO $I$
$S\ (j \in J) \wedge S\ (j \in J') \wedge S\ (i \in I)$
IAO $I$
ITCS $J$
IAO' $I$
$S\ (j \in J) \wedge S\ (j \in J) \wedge S\ (i \in I')$

Fig. 2. The basis of possible variants of the structures of OPGS of arbitrary complexity

Table 1

Variants of the structures of the object of protection of the general structure

| No. | A variant of the structure of the object of protection of the general structure |
|---|---|
| 1 | IAO, which does not fit in its composition ITCS |
| 2 | IAO, which includes ITCS, or several ITCS, including a public network (as an INTERNET network or telephone network) |
| 3 | ITCS, which includes IAO, or several IAOs intended for maintenance of ITCS for its functional purpose, or also intended for auxiliary functional purposes (office premises, warehouses, technological and industrial premises, etc.) |
| 4 | OPGS, which are defined as the main ITCS, which also includes the subordinate ITCS' which includes the IAO with its own purpose defined for this purpose (the breaking line of the arrow in Fig. 2), which does not carry the functional responsibilities characteristic of the main ITCS (continuous line of the arrow in Fig. 2). Such OPGS are called hybrid OPGS of the first type |
| 5 | COPGS, which are defined as the main IAO, which also includes ITCS with its own purpose defined for this purpose (continuous line of the arrow in Fig. 2), and IAO' as part of this ITCS. Moreover, this subordinate IAO' either carries (continuous line of the arrow in Fig. 2) or does not carry (the breaking line of the arrow in Fig. 2) the functional responsibilities characteristic of the main IAO – hybrid OPGS of the second type |

The OPGS structures should be formed taking into account their location within some infrastructure level. For example, within the structure of an enterprise, institution, etc., located within a district, or more branched within a city, region, or even on a national scale that is not related to the local location.

Such structures include all IAO, regardless of their purpose, scale, and complexity. In addition, it becomes possible to create a methodology for constructing ISS or IISS of any complexity. On such principles, it becomes possible to create a computer-aided design system. That is, the entire design process receives the fundamental possibility of automation using a single universal method.

From that moment on, it became possible to formulate definitions and rules that should be carried out in the design of ISS and IISS. Moreover, such definitions and rules form the basis for a formalized description of the properties and logical relationships between the components of the projects of any ISS. And threats with appropriate DF and possible counteractions (that is, methods and means of protection), taking into account the current state of the object, form its description. This description is considered as an image of the object.

That is, the concept of the image of an object as a means of its formal description is introduced.

The following concepts are included in the library of definitions for which the object is described and the links between the basic components of ISS projects are included:

– list $I$ of elements $i \in I$, which make up the object;

– the state of the set of these elements $S(I)$;

– list of destabilizing factors $F$ as some $f$ function $F=f(S(I))$;

– a list of means and methods of protection for each individual case.

OPGS as a subset $Y_i$ of the totality of known methods and means is the set $Y$ that uses the sample $F$ as its argument, i. e. $Y_i=f(F_i(S(I)))$, where $_i$ is a sign of belonging to a particular case of IAO or ITCS.

The above makes it possible to implement the procedure for determining the list of DF($F_i$) and the procedure for determining the means and methods of protection $Y_i$ as a sequence of two procedures (two stages of design). At the first stage, the list of threats to OPGS is determined, and at the second stage, the search for technical means and methods of ZI is carried out. Different authors represent the concept of DF and the concept of threats in different ways, that is, identify them or divide. If we identify DF and their causes as threats, then on their basis it is possible to determine the groups of violations that can be determined with the implementation of threats. If we separate DF and their causes, then the concepts of DF and DF sources are introduced. At the same time, most often for ITCS, the causes of DF include the human factor, technical devices, mathematical support, the technology of AS functioning, the external environment. DFs include the possible result of the action of causes, in the form of quantitative insufficiency, qualitative deficiency, failures, errors, natural disasters, malicious actions, and side effects. But for OPGS in the form of IAO, such definitions are not logical. Therefore, unity in the design approach requires the definition of DF actually as a source of DF, and it is proposed to define both DF and the appropriate formulation of descriptions of non-DF threats as threats. Then the terminology and meaningful meaning of threats and DF becomes one for any OPGS structure. In addition, with this approach, when creating a model of the ISS project, unity is ensured in the description of DF and threats both for the structure of the system of protection of OPGS through technical channels and for the structure of the system for protecting OPGS from unauthorized access (UAA).

With such principles, a further task is to describe a new method of creating transitions from DF to threats at the level of creating a model of threats and determining the directions of protection. And the transition from threats to specific means of protection in accordance with certain areas of protection is carried out in projects at the level of implementation of counteractions.

To solve this problem, it should be provided for the use of design tools using memory elements with a sample of the content of the request (associative memory, AM). This is necessary for the organization of databases (DB) of descriptions of elements of IAO $i \in I$, their state $S(I)$, the list of DF($F=f(S(I))$) and decisions on means and methods of protection $Y_i=f(F_i(S(I)))$.

## 5. Results of the study of the possibility of creating an automatic design system for the protection of objects of arbitrary complexity

### 5. 1. The concept of structures of objects of protection and the description of such structures

In general, the protection system by structure should correspond to the structure of the object of protection, that is, the structure of the hierarchical distributed AS of class 3, similar, for example, to the «Frontier» system for AS [13]. Then the general structure of the IS system is a set of complexes of protective equipment (CPE) of certain levels, as is shown in Fig. 3.

If we combine the above requirements, then the rules for the formation of ISS and IISS for OPGS can be formulated for cases given in Table 2.

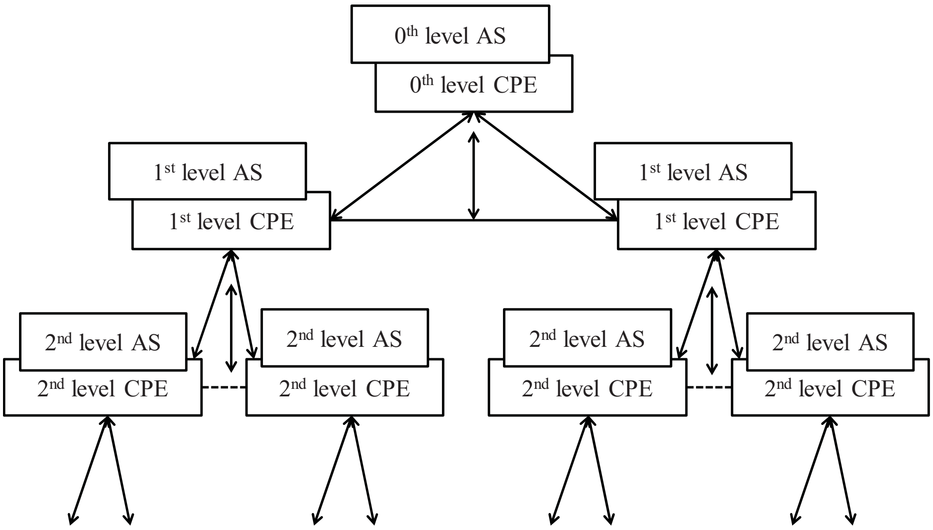

Fig. 3. Multi-level complex of protective equipment

Table 2

Rules for the formation of an information security system and an integrated information security system

| For hierarchically distributed OPGS | | For single-level distributed OPGS |
|---|---|---|
| OPGS is built starting from a higher level of the structure, anticipating the hierarchical nature of the structure being created or examined | OPGS is built starting from a lower level of structure, and the future hierarchical nature of the overall structure of the OPGS is uncertain | |
| The structure of TP at the higher level IISS should include all general requirements for the technical specifications of the lower levels of the CPE TP | IISS for individual OPGS of a certain level are created independently of each other and without taking into account the future hierarchical structure of OPGS | TP and IISS project are created for each OPGS independently of each other |
| The composition of TP on the IISS of the lower levels cannot include any requirements that are not in the composition of the vehicle on the IISS of the zero level | When a fragment of the IISS of the next, higher level appears, the TP on its OPGS and the protection project is created as a set of TP points and IISS projects of lower-level objects | The points of TP and IISS projects of any OPGS should not have contradictions with any points of TP and the projects of IISS of other OPGS |
| The IISS project for the highest level of the OPGS should include IISS projects of all lower-level protection objects as their components | TP and IISS projects of higher-level objects may include items specific to the OPGS of a given level, provided that they do not have contradictions with the TP and IISS defined for any lower-level OPGS | The TP and the points of the IISS projects that are specific to the structure of OPGS are added to its TP and IISS project in the form of a separate item, that is, they cannot be included as a sub-item in the existing list of items defined for other OPGS of this structure |

It should be noted that the TP and IISS project for OPGS of each subsequent level should contain all the points of TP and IISS projects that were defined for all OPGS of previous, lower levels, including those specific to this list, for the previous level (Table 2).

### 5. 2. Formation of clusters of protective equipment using the structures of protection objects

The image of threats $Y$ determines the directions of protection but to determine the means of protection, it is necessary to rely on the possibilities of countering threats, namely on the database of possible means of protection that make up the image of the database. We define the database of possible means of protection with the image $Z$. Thus, the separation from the database of means of protection (set of means) of the part of equipment that is necessary for servicing the current OPGS is the task of determining the corresponding subset $Z_i \in Z$. A subset $Z_i$ is an image of the means of protection of the current OPGS. The corresponding image of the threats of the current OPGS is a subset $Y_i \in Y$.

The set of protection means as an image of $Z$ consists of four clusters (images of subsets) of means. These include active $Z(A_i)$ and passive $Z(P_i)$ protection means, prohibition (restrictions) in the use of certain means $Z(N_i)$ and cryptographic means $Z(K_i)$, indicated in Fig. 4.

Thus, the image of all possible means $Z$ consists of four images $Z(A,P,N,K)$. The initial conditions for the use of protective equipment in the $\{Z(A,P,N,K)\}$ design is the image of all possible means, and the final result of the design is the image corresponding to the current OPGS means $Z(A_i,P_i,N_i,K_i)$. In this definition, the symbol $i$ means the correspondence of the images of the means of protection to the image of threats $Y_i \in Y$ of the current OPGS.

Considering the procedure for determining the means of protection as a search procedure in the terminology of FSM, the initial state is defined by the image $Y_i \in Y$, the final state is the image $Z(A_i,P_i,N_i,K_i)$, and the transition tool from the initial to the final state is the algorithm of AM operation as a predicate of AM. It is necessary to determine the conditions under which the procedure is possible for the transition from the initial to the final state, that is, the existence of a quantifier [14]:

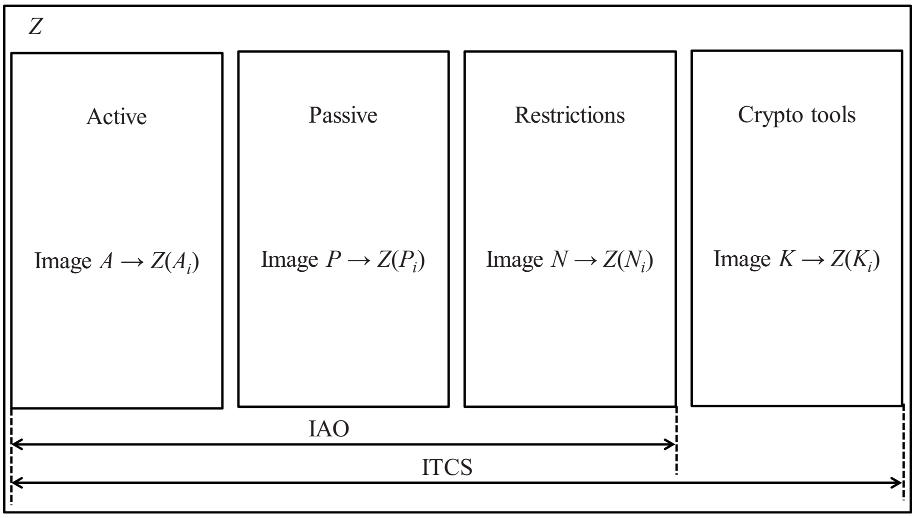

Fig. 4. Clusters of protection tools for the object of protection of the general structure

$$\forall(Y_i \in Y)\exists(Z(A_i,P_i,N_i,K_i)) = TRUE.$$

To do this, consider options for possible images of subsets of protective equipment $(Y_i \in Y) \to Z(A,P,N,K)$ for OPGS of arbitrary architecture.

$$Z(P) \leftrightarrow \neg Z(A) \wedge \neg Z(K), \quad (1)$$

$$Z_1(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge$$
$$\wedge\left[Z(P) \vee (Z(P_j) \notin Z(P))\right], \quad (2)$$

$$Z_2(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge Z(P), \quad (3)$$

$$Z_3(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge Z(P) \wedge Z(K), \quad (4)$$

$$Z_4(A_i) \in Z(K) \leftrightarrow \neg Z(N) \wedge \neg Z(P), \quad (5)$$

$$Z(P) \leftrightarrow \neg Z(A) \wedge Z(K), \quad (6)$$

$$Z(K) \leftrightarrow \neg Z(A) \wedge \neg Z(P), \quad (7)$$

where the symbol j emphasizes belonging only to that part of the *j*-th active means that make it possible to compensate for the lack of passive means $Z(P_j) \notin Z(P)$. This expression that highlights the image $Z(A,P,N,K)$ as an event that occurred as a result of the event that created the state $(Y_i \in Y)$ emphasizes that the images of threats are an argument for the future appearance of the image of the means of protection $Z(A,P,N,K)$.

### 5. 3. The procedure for determining the structures of objects of protection and their relations with a set of means of protection when building an information security system

Expressions (1) to (7) make sense provided that some rules, prohibitions, and restrictions are introduced, which are given in Table 3. That is, the rules of prohibition and restriction $N$ are a priori defined for any object in the form of a final specification. Thus, $Z$ is converted from an argument to a defined parameter, i. e. $\{Z(A,P,K), N=\text{const}\}$.

Table 3

Prohibitions and restrictions on the use of active protective equipment

| No. | Prohibitions and restrictions on the use of methods of active means of protection in the development of IISS systems |
|---|---|
| 1 | Active means $Z(A)$ are used only when it is proved impossible to use passive means Z(P), or when the already involved passive means $Z(P)$ are objectively unable to provide the necessary specified result of protection, which can be illustrated by the general expression $Z_1(A_j) \in Z(A)$=TRUE$\leftrightarrow Z(P_j \notin P)$. Under this condition, the expression $Z(P_j) \notin Z(P)$ is given in formula (2), and the symbol *j* emphasizes that the sample $Y_i$ with the symbol *i* is not related to the formation of such a forbidden sample $Z(P_j)$. Then it becomes clear that the numbers 1, 2, 3, and 4 in the definition of $Z_1(A_j)$, $Z_2(A_j)$, $Z_3(A_j)$ and a $Z_4(A_j)$ from formulas (2) to (5), respectively, mean the following cases:<br>– $Z_1$ – the case when active means are used without passive (or certain passive did not provide the desired result) and without crypto methods;<br>– $Z_2$ – the case when active methods are used together with passive ones in the absence of crypto methods and the absence of prohibitions on active ones;<br>– $Z_3$ – the case of using active methods together with passive and cryptographic;<br>– $Z_4$ – the case when the active methods are combined exclusively with cryptographic ones.<br>The meaning of formula (1) determines the case when only passive methods are involved, and the content of the formula (7) determines the case of involvement in the protection of exclusively cryptographic methods |
| 2 | Prohibitions and restrictions $Z(N)$ apply only to active methods of protection. In general, active methods of protection have the following disadvantages:<br>the use of active methods of protection leads to insurmountable unmasking features of the object;<br>– the presence of active protection means violates the electromagnetic compatibility of the technical means available at the facility;<br>– under the conditions of multichannel reception of interception means and long-term accumulation of information intercepted by means of an information attack, the possibility of isolating informative components from the protected signals remains and the probability of positive or negative consequences of the attack is not determined;<br>– under the conditions of using active protection to close the surrounding space with a radio channel, medical indicators of presence are negative;<br>– in the presence of crypto protection, radio noise does not make sense |
| 3 | Ensuring the necessary and sufficient value of the entropy coefficient of noise quality, which is formed by active means of protection, requires reliable proof |

The shortcomings and limitations of active protection, given in paragraph 2 of Table 3, fully confirm the content of the restrictions given in paragraph 1 of Table 3.

Passive means of protection here include means of protection against leakage by channels of indirect electromagnetic radiation and guidance (PEMVN) and acoustic, as well as measures and means of protection against UAA to information carriers. The combination of $Z(P)$ with protection against UAA does not create contradictions with the general methodology of TPI.

If we consider the five types of structures of IAO, given in Table 1, then the application of expressions (1) to (7) to each of them makes it possible to systematize the images of protective equipment for different structures of objects:

1. For structure 1, according to Table 1, from the general range of expressions (1) to (7), passive means and passive means in the presence of permitted active means of type $Z_2$ are distinguished.

$$Z(A_i,P_i,N_i,K_i)= \\ =\begin{cases} Z(P)\leftrightarrow \neg Z(A)\wedge \neg Z(K), \\ Z_2(A_j)\in Z(A)\leftrightarrow \neg Z(N)\wedge \neg Z(K)\wedge Z(P). \end{cases}$$

It is possible to combine these two expressions according to the formula of logical connections, which gives the expression:

$$Z(A,P,N,K)=Z(P)\vee\left\{Z(P)\wedge\left[Z_2(A_i)\wedge \neg Z(N)\right]\right\}.$$

2. For structure 2, according to Table 1, it is possible to use the permitted active type $Z_2$ means in the presence of passive or passive means and means of cryptographic protection.

$$Z(A_i,P_i,N_i,K_i)= \\ =\begin{cases} Z(P)\leftrightarrow \neg Z(A)\wedge Z(K), \\ Z_2(A_j)\in Z(A)\leftrightarrow \neg Z(N)\wedge \neg Z(K)\wedge Z(P) \end{cases}$$

or:

$$Z(A,P,N,K)=Z(P)\wedge\left[Z_2(A_i)\vee Z(K)\right].$$

3. For structure 3, according to Table 1, it is possible to use passive methods of protection combined with cryptographic and permitted active type $Z_2$ ones in the presence of passive methods.

$$Z(A_i,P_i,N_i,K_i)= \\ =\begin{cases} Z(P)\leftrightarrow \neg Z(A)\wedge Z(K), \\ Z_2(A_j)\in Z(A)\leftrightarrow \neg Z(N)\wedge \neg Z(K)\wedge Z(P). \end{cases}$$

4. For structure 4, according to Table 1, it is possible to use passive methods of protection combined with cryptographic and permitted active ones of the type $Z_2$ in the presence of passive methods. And this coincides with the use of protection methods for structure 3.

5. For structure 5, according to Table 1, two options are possible. If the IAO does not have a general purpose with the main IAO, then it does not have a general purpose with ITCS. That is, the IAO is a separate object of protection, and it is possible for it to use the methods of protection specified for structure 1. If the IAO', being part of the ITCS, has a general purpose with the main IAO, then the purpose of the IAO' coincides with the purpose of the ITCS, and it is possible for it to use the methods of protection specified for the 3rd structure. Since $Z(A_i, P_i, N_i, K_i)$ for structure 3 appears to be a combination of means used as means of protection for structures 1 and 2, the general expression of logical relationships for the set of structures under consideration takes the form:

$$Z(A,P,N,K)=Z(P)\wedge\left[Z_2(A_i)\vee Z(K)\right]\leftrightarrow \\ \leftrightarrow \min\left[Z(P),Z_2(A_i)\vee Z(K)\right]. \tag{8}$$

The possibility of reducing (1) to (7) to a concise form (8) has a logical justification. Indeed, since active methods have restrictions under paragraph 1 of Table 3, then the means specified by formulas (2), (4), and (5) may not be used. The absence of (7) is logically explained by the fact that only the cryptographic method of protecting the IAO within the framework of the development of IISS does not make sense due to the lack of logic for the case when the information flow is protected, and the information carrier is absent. Theoretically, there are two cases when it is possible to use an exclusively cryptographic method of protection. One case involves the use of a separate device (or subscriber kit) to protect speech information, such as a masker, scrambler, vocoder, or lip reader. Subscriber kits are used both in conductor telephone communication channels and in walkie-talkies. Another case is the use of special communication devices when performing tactical operations by special purpose units. In both cases, there is no talk of IISS due to the actual absence of the object of protection, or ITCS.

### 5. 4. Proving the uniformity of the decision on the choice of methods and means of protection in the construction of IISS for certain structures of OPGS

The right side of expression (2) essentially means that if 3 conditions are met, namely:

– when the objects of protection should be represented in accordance with the structures of OPGS;

– the structures of OPGS should be classified by type according to Table 2;

– use protective equipment on the basis of restrictions and prohibitions in accordance with Table 3, and at the design stages to use AM as a database describing the state of the object, the database of threats, and the database of methods and means of protection, then according to the design result, a decision should be made on the use of methods and means of protection in their minimum volume. This automatically minimizes the financial burden on the protection system as a whole, if minimizing the number of methods and means of protection is considered a condition for minimizing the financial burden.

The presence of a single solution by expression (2) also indicates that when designing according to this logic, it can be considered proven that the situation when the same, or almost identical objects, receive completely different decisions regarding their ISS and IISS.

Thus, predicate (2) [15] is a sufficient single expression that describes the logic of choice when completing the protection system of any OPGS. That is, taking into account expression (2), it can be assumed that the algorithm for training the network model is one that should and can lead to the adoption of a single decision for each individual OPGS. Moreover, expression (2) itself is not a description of the sequence of actions by which the modeling process is determined. Predicate (2), by definition of a mathematical reference book [14], is an optimization predicate. And the proof of its unity means that for any real object there is only one solution in the choice of methods and means of protection. This has the property of sufficiency of the selected methods and means of protection, that is, it does not include in its composition unnecessary, repeatable elements of protection. That is, for such objects there is an objective solution. This is the point of optimizing the solution in the design.

## 6. Discussion of the possibility of creating an automatic design system for protecting objects of arbitrary complexity

The practical application of the technology without the subjective influence of the designer will ensure financial minimization of the designed protection system. At the same time, the effectiveness of information protection of objects increases due to the fact that such projects are created as part of the unified formalized structures of objects within the State. That is, prerequisites are created for the unification of all existing protection projects, regardless of the qualifications and preferences of the designers. When achieving design automation, the absence of a human designer ensures the objective effectiveness of projects, which determines the relevance of the proposed approach.

Currently, the link between threats and counteractions according to Fig. 1 is a task not solved by the regulatory and methodological framework of TPI, even for threats at the level of individual IAO. Therefore, to determine such relationships for arbitrary objects, it is proposed to formalize the general structure of such objects. This requires the introduction of concepts of structures of objects of protection according to Fig. 3 and Table 2 and the introduction into the regulatory framework of TPI of the concept of restrictions on the use of passive, active, and cryptographic methods of protection, as indicated in Fig. 4. In this case, it becomes possible to create a procedure of computer-aided design of protection systems by determining the evolutionary architecture of a complex information system, as is also proposed in [7]. For a given case, it is proposed to introduce the structures of OPGS with their basis according to Fig. 2 and Table 1.

The justification for this introduction is based on the fact that in DSTU on TPI and methodological documentation for ISS, projects are created for various objects of protection. Such objects can be, for example, information telecommunication or automated systems. These include fiber-optic communication systems, wired telephony systems, satellite communication or production management systems, etc. Also, separately, projects are created for such IAOs that are not related to telecommunication or automated systems.

It should be noted that projects exist but there is no documentation or design regulations. Thus, according to ND TPI 1.1-005-07, ND TPI 3396.2 and the current order of the Cabinet of Ministers of Ukraine No. 906 of 27.07.15, the IAO is defined as "an engineering and technical structure (premises), a vehicle where activities related to state information resources and information are carried out, the requirement for the protection of which is established by law." Also valid is the Law of Ukraine of 23.02.2006 No. 3475-IV where the IAO is defined as "engineering and technical structure (premises), a vehicle where the sounding and/or processing by technical means of IzOD is carried out".

These documents for IAO are not related to information and communication systems. There are objects themselves that do not contain telecommunication or automated systems, for example, dedicated premises for confidential negotiations. According to the order of the Department of Special Telecommunication Systems and Information Protection (SSISS) of the Security Service of Ukraine No. 61 of 22.12.99, this is an engineering and technical structure (premises), a vehicle where activities related to state information resources and information are carried out, the requirement for the protection of which is established by law. Telecommunication systems are prohibited here, and it is desirable that there are no technical means at all. These can be the premises of military headquarters, points of customs service, police, court, secret departments of enterprises, etc. with their information carriers. The carriers include written documents, logs of events, safes for them, security rooms, people, etc. Also, carriers are uncontrolled physical fields, such as speech acoustic signals, radiation of kinescopes or loudspeakers, etc.

At the same time, UAA is distinguished to the information, whether the UAA to their carriers separately, or the UAA to the territory (up to the perimeter), that is, to the controlled zone (the territory or space in which unauthorized and uncontrolled stay of unauthorized persons, the placement of technical and vehicles is impossible). There may be no controlled zones in telecommunication or automated systems. For example, a satellite communication channel, or remote communications of wired or optical or radio communication, etc.

If there is a telecommunication system in the controlled area, for example, a PC of any of the three known classes or a specialized computer, protection projects are created for the controlled area separately, for a PC, an automated control tool, and similar devices separately. At the same time, the regulations for the operation of protective equipment in their life cycle or the regulation of possible actions in the controlled zone have the right not to be part of a single project for their protection. The structure of such systems should be hierarchical, determined by their vital or secondary purpose.

Other terms are used in the meaning given in the Laws of Ukraine «On the Fundamentals of National Security», «On Defense of Ukraine», «On Information», «On Telecommunications», «On Protection of Information in Information and Telecommunication Systems». The concept of hierarchy is not mandatory for such systems.

In determining the structures of objects of arbitrary complexity, taking into account their functional hierarchy, a formalized description of the links between threats and counteractions becomes possible. The architecture of the protection system and the evolution of the list of links between threats and counteractions can be ensured by the creation of appropriate images of threats to objects according to predicates (1) to (7), and databases.

A feature of the proposed approach to design is the absence of an existing similar method of designing systems for protecting objects of any level, from a separate IAO at the infrastructure level of a separate organization, to a national one. And this, as can be seen, requires a description of any objects of protection according to their infrastructural features and an evidence-based determining of the effectiveness of future projects. One of the evidence-based arguments is the evolution of the architectures of complex TPI objects and, as a result, the evolution of projects for their protection, where each new project is created using data on the life of existing projects.

According to the results of the analysis of the proposed approach to design, it was established that its implementation can be limited only by factors of either economic or legislative and regulatory and methodological nature.

Since the introduction of such an approach makes sense when it is distributed throughout the State, or at least on a regional scale, this leads to the need for significant financial costs. Moreover, these costs should be carried out in a short time. The reason is that the formation and commissioning of the necessary databases should be carried out subject to the currently operating objects of protection. And to stop the action of objects even for a short time is impossible.

Another restriction is based on the fact that the use of evolutionary projects requires the introduction of new documents into legislation and additions to the regulatory framework of TPI, which are indicated in Fig. 4 as a «restriction» and which still hasn't existed.

In general, the practical application of the technology without the subjective influence of the designer will ensure financial minimization of the designed protection system. At the same time, the effectiveness of information protection of objects increases due to the fact that such projects are created as part of the unified formalized structures of objects within the State. That is, prerequisites are created for the unification of all existing protection projects, regardless of the qualifications and preferences of the designers. When achieving design automation, the absence of a human designer ensures the objective effectiveness of projects, which determines the relevance of the proposed approach.

Further research areas can be focused on solving the problem of creating semantic databases of library type, which are able to provide a link between threats and counteractions of objects of arbitrary complexity.

## 7. Conclusions

1. The proposed approach to structuring information security systems by defining the IAO and ITCS of arbitrary complexity in the form of objects of the general structure – OPGS, and the properties of such objects have been determined. A formalized description of their functional hierarchical structures is given, that is, the functional basis of the structures of protection objects is given. Within the framework of this basis of the structures of all possible objects, it is possible to strictly coordinate the projects for the protection of OPGS. It also makes it possible to create the databases necessary for computer-aided design of ISS using memory usage technology with a sample of the content of the request (AM). The specification of links between the DF database and the database of information threats at the protection object in the form of "images" of DF and "images" of threats of threats in the form of "images" of DF and "images" of threats is described in the design of IISS.

2. The presence of a specification of the links between the DF database and the threat database makes it possible to ensure the choice of a single set of means of protection from their entire set for each individual object of protection of a given structure. It is shown that the possibility of such an unambiguous choice of a set of protective equipment is provided by changes in the list of clusters of protective equipment. This gives grounds for the further creation of tools of the automatic design system, which includes in its composition the only possible and sufficient elements of protection.

3. When creating protection projects for objects with features of OPGS, an unambiguous definition of the links of the structures of OPGS with a set of means of protection is provided. It is also shown that the specified stability of the ISS to countering threats is ensured if the library type database is used with training and subsequent selection of solutions according to the content of the request. The stability of the projected objects is explained by the fact that the methods and means of protection $Z_i$ and the decision on their use $Y_i$ are made by sampling $Z_i$ from memory with a sample according to the content of the request. The AM contains data in which the destabilizing factors $F_i$ and the methods and means of protection against them $Z_i$ are interrelated. These projection connections are entered in the AM according to ontological information from projects of existing objects, or the closest existing projects of stable objects. The robustness of objects is determined by the longest time of existence of objects without violations. Such an AM algorithm resembles a well-known perceptron algorithm, when the decision to select $Z_i$ is made by sampling such $Z_i$, which has the maximum number of stability indicators. The library of such indicators should be created as the final and sufficient to describe any structures of objects with states $S_i$. Creating such a library requires additional time. In addition to robustness indicators, preference is also given to such existing projects where restrictions and prohibitions on $Z_i$ are minimal, if any. The new project being created is entered into the DF database and the database of protective equipment with its own indicators. This determines the ontological nature of the database of projects.

At the national level, such formation of a database means the uniformity of all existing and created projects for the protection of objects.

4. The uniformity of the decision on the choice of methods and means of protection in the construction of IISS for certain structures of OPGS has been determined. The sufficiency of the use of the selected methods and means of protection in the development of IISS for objects of arbitrary complexity has been established. Accordingly, the construction of IISS is carried out by minimizing the number of methods and means of protection used, provided that a given level of protection of the object and a fixed financial load are ensured. This makes it possible to represent the problem of designing an information security system as a solution to the corresponding multi-criteria optimization problem with limitations.

## Conflicts of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

## Financing

The study was conducted without financial support.

## Data availability

All data are available in the main text of the manuscript.

## References

1. Wu, T., Zhang, R., Dai, P., Liu, S. (2018). Research on information system architecture of standardized organization based on data repository. 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). doi: https://doi.org/10.1109/itoec.2018.8740482
2. Grishina, N. V. (2007). Organizaciya kompleksnoy sistemy zashchity informacii. Moscow: Gelios ARV, 256.
3. Zakaria, K. N., Othman, S. H., Zainal, A. (2019). Review of Cybersecurity Audit Management and Execution Approaches. 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS). doi: https://doi.org/10.1109/icriis48246.2019.9073641
4. Karagiannis, S., Manso, M., Magkos, E., Ribeiro, L. L., Campos, L. (2021). Automated and On-Demand Cybersecurity Certification. 2021 IEEE International Conference on Cyber Security and Resilience (CSR). doi: https://doi.org/10.1109/csr51186.2021.9527958
5. Turner, R. C. (2022). Process Mining for Asymmetric Cybersecurity Audit. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). doi: https://doi.org/10.1109/csr54599.2022.9850298
6. Progonov, D., Yarysh, M. (2022). Analyzing the accuracy of detecting steganograms formed by adaptive steganographic methods when using artificial neural networks. Eastern-European Journal of Enterprise Technologies, 1 (9 (115)), 45–55. doi: https://doi.org/10.15587/1729-4061.2022.251350
7. Isazadeh, A., Karimpour, H. (2011). Formal Specification of Control Software Systems Using Behavioral Views. International Journal of Advanced Research in Computer Science, 2 (1), 62–67. Available at: http://www.ijarcs.info/index.php/Ijarcs/article/view/246/236
8. Mierlo, S. V., Vangheluwe, H. (2018). Introduction to statecharts modeling, simulation, testing, and deployment. 2018 Winter Simulation Conference (WSC). doi: https://doi.org/10.1109/wsc.2018.8632384
9. Hoffmann, J. L. C., Horstmann, L. P., Wagner, M., Vieira, F., de Lucena, M. M., Frohlich, A. A. (2022). Using Formal Methods to Specify Data-Driven Cyber-Physical Systems. 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE). doi: https://doi.org/10.1109/isie51582.2022.9831686
10. Eckhart, M., Ekelhart, A., Weippl, E. (2022). Automated Security Risk Identification Using AutomationML-Based Engineering Data. IEEE Transactions on Dependable and Secure Computing, 19 (3), 1655–1672. doi: https://doi.org/10.1109/tdsc.2020.3033150
11. Cha, S.-C., Yeh, K.-H. (2018). An ISO/IEC 15408-2 Compliant Security Auditing System with Blockchain Technology. 2018 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2018.8433185
12. Buddy System. Available at: https://www.securitylab.ru/software/234275.php
13. Budko, M., Vasylenko, V., Korolenko, M., Butochnov, O. (2002). Systema zakhystu informatsiyi vid NSD „RUBIZh”. Praktychni aspekty realizatsiyi kontseptsii tsentralizovanoho upravlinnia bezpekoiu korporatyvnoi systemy. Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsiyi v Ukraini, 4, 154–161.
14. Hodel, R. (2013). An Introduction to Mathematical Logic. Dover Publications, 512.
15. Shoenfield, J. (2018). Mathematical Logic. A K Peters/CRC Press, 356. doi: https://doi.org/10.1201/9780203749456