UDC 004.43(031):681.3.01(02)
DOI: 10.15587/1729-4061.2023.291616

DETERMINING QUALITY INDICATORS FOR PROJECTS OF INFORMATION PROTECTION OF INFORMATION ACTIVITY OBJECTS

Vladymyr Lutsenko
PhD, Associate Professor*
Dmytro Progonov
Corresponding author
PhD, Associate Professor*
E-mail: progonov@gmail.com
*Department of Information Security
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Beresteiskyi ave., 37, Kyiv, Ukraine, 03056

The design and analysis of the effectiveness of modern integrated information protection systems (IIPS) is complicated by the influence of the designer's subjective decisions regarding methods and means of protection, the need to determine the quality criteria for the functioning of the designed objects. The work is aimed at improving the technology of automated design of IIPS by determining the quality of projects. When creating a database (DB) of objects with such "qualitative" performance indicators of information protection systems, it is possible to compare existing and new protection objects and to adjust the protection projects of existing objects. Moreover, the ontological properties of active and threat-resistant objects are taken into account.

To illustrate the use of the methodology for determining and comparing the quality of projects, an example of comparing the quality of projects obtained in different ways is given. One way currently operating involves the use of expert evaluation of the quality of protection projects for existing facilities. The second way is intended for objects defined as objects of protection of the general structure (OPGS) and involves a principally objective assessment of design quality using known quality diagrams and control of Ishikawa and Pareto design consequences. As a result of the given example, it was determined that the quality of projects according to quality diagrams and control of design consequences should increase by more than two times.

The proposed method of comparing the quality of information protection projects for different objects or different protection projects of one object allows to improve the process of creating information protection projects. At the same time, it is possible to exclude the human controller from the process of determining the reliability of object protection. It also allows you to automate the design process, reduce the time and cost of design costs

Keywords: information security, quality of projects, security of protection objects, comparison of the quality of information protection projects

Received date 27.09.2023
Accepted date 13.12.2023
Published date 28.12.2023

***How to Cite**: Lutsenko, V., Progonov, D. (2023). Determining quality indicators for projects of information protection of information activity objects. Eastern-European Journal of Enterprise Technologies, 6 (2 (126)), 41–48. doi: https://doi.org/10.15587/1729-4061.2023.291616*

1. Introduction

Any project related to information protection systems (IPS) [1] or integrated information protection systems (IIPS) [2] must determine the real safety of protection objects, and this, in turn, predetermines the quality of the protection project [3, 4]. It is worth noting that there are currently no specific issues in the field of legal norms, regulatory framework, and methodical support. However, in the area of technical information protection (TIP), including the creation of a high-quality threat model and the design of protection systems, there is a significant imperfection. In general, this is related to the objective development lag in time of this field. The currently present technological crisis includes an imperfect methodology for designing IPS. This imperfection is related to the lack of an objective comparison of the quality of projects. Currently, the quality of protection projects is determined by an expert method, which has many shortcomings and does not differ in proven objectivity. It is time to get rid of the designer's dependence on the person [5] by devising a procedure for the objective comparison of the quality of the designed protection system for various protection objects. It is necessary to compare different protection projects for the determined project that is the most resistant to threats. In addition, it is important to identify weak points in the security of objects when using various protection projects.

Solving these tasks is currently the most relevant when creating projects for the protection of objects of information activity, especially when ensuring the possibility of comparing the quality indicators of these projects. The use of the specified comparison will allow creating projects of protection objects with a predetermined level of protection.

2. Literature review and problem statement

Improvement of projects of technical information protection systems is possible under the condition of consideration of the process of creating protection systems in a complex. For this, it is necessary to combine into a single process such design components as survey and description of the object, solving the problem of designing a financially minimized protection system, audit of the object's resistance to threats, and post-project [6] and pre-project [7] audit of the object's security. The listed fragments of the integrated approach will be effective under the condition of an objective compar-

ison of the quality of the created projects and the quality of the design methodology itself.

At the same time, it is absolutely necessary to adapt the methodology of designing information activity objects to international standards [8]. New design solutions are considered by various authors. But this process is slow due to the complexity of the task. For example, the so-called evolutionary architecture of a complex information and communication system (ICS) is proposed in [9]. The approach involves creating a model of the object's behavior in accordance with its current state. The behavior of the object and its current state are determined by the method of forming the description of the object and the model of events (current behavior in the sequence of events) in the form of some image, which the author of work [9] calls *Statechart* [10]. The set of possible behaviors (library of possible images for a specific object) is represented by the *Viewchart* behavior image. *Viewchart* images develop *Statechart* images. Creation of object images is based on the *Statemate* toolset. The specified approach at the expense of *Statechart* determines what the object was and what it will be. In essence, *Viewchart* is a set of options for data representations (images). Moreover, the trends regarding the sequence of states of the object are taken into account. Images are represented either by histograms of states over time, or by a sequence of possible states. At the same time, the design methodology is reduced to formalized, i. e., mathematical tools (*Statemate*), which are used as communication functions between possible *Statecharts* and existing *Statecharts*. In general, this approach is promising. The disadvantage is that the quality indicators of the protection project are uncertain. Thus, the protection project is not a final technological product. It can be one of the possible options for a technological product. That is, on such grounds, there is no question of the objectivity of design decisions, and the optimization of projects with respect to any design parameter is impossible.

Methods of risk analysis and management are close. These include the CRAMM method (the UK Government Risk Analysis and Management Method, Great Britain, 1985). It is a universal tool designed to conduct an inspection of the object of protection, risk analysis, audit for compliance with the requirements of the British Government and the standard [11] that ensures business continuity.

The disadvantage is that the CRAMM method is focused on object security audit and is intended for objects operating within the framework of a separate standard.

The Cobra method [12] provides a quantitative analysis of risks and provides an assessment of the compliance of the information system with individual standards. It implements tools for security consulting and review. It has a large base of threats and vulnerabilities. But at the same time, a large number of questionnaires is needed. The disadvantage is that it leads to providing purely subjective solutions. especially if survey statistics are insufficient. The question of determining the degree of the specified "sufficiency" also remains open.

The Risk Watch method (USA) is a software product and is a means of risk analysis and management [12]. It provides various types of security audits. The choice of audit type is determined by the user. The disadvantage is that it is not about the design procedure.

The Buddy System method [12] by the company "Consultation Objective and Bi-Functional Risk Analysis" is also a software product. It implements both quantitative and qualitative risk analysis. It has means of creating reports. The main attention is paid to the risks associated with the violation of physical security. The disadvantage is that the focus is on project management rather than the design process.

In addition to the above approaches, the EBIOS, MEHARI, OCTAVE, CORAS, Grif methods are also used to analyze the security of protection objects. The disadvantage of these methods is that when using them, it is necessary to take into account the peculiarities of the legislation and standards of Ukraine. There are also peculiarities of relations between user organizations within the existing infrastructure. Creation of the structure of information systems has local and regional features and traditions.

The results of our review indicate that neither the audit standards and programs, nor the auxiliary software tools for designing or other tools related to designing, do not allow a comparison between already created and new protection projects. This shows that the method of comparing the quality of object of information activity (OIA) protection and the objectivity of such a comparison are urgent.

3. The aim and objectives of the study

The purpose of our research is to devise a procedure for the objective and effective comparison of projects or information protection systems of OIA and ICS based on them. The model of such a means of comparison will provide an opportunity for the development of a new methodology for the design of IPS or IIPS.

To achieve the goal, the following tasks were solved:

– to show the existence of uniformity of quality indicators of information protection systems projects;

– to propose an approach for obtaining quality indicators of information protection projects, which will allow obtaining objective conclusions when comparing the quality of projects at the expense of data obtained subjectively;

– to give an example of obtaining quality indicators that illustrates the possibility of creating projects with predetermined quality indicators while reducing the influence of the subjective component of the designer on the design process.

4. The study materials and methods

The object of this study is the process of determining the quality of physical access restriction and control systems, as well as access to information at the objects of information activity and in the information and telecommunication systems of the State.

The subject of our research is the methods, means, and methodology of designing information protection systems of information activity objects and information and telecommunication systems, the procedure for comparing the quality of protection systems as an operating environment of self-discipline and work with information, procedures, and algorithms.

The research was conducted using theoretical methods, namely modeling the process of developing an information protection system and synthesis of the design algorithm, which allows determining the quality indicators of the work of IIPS. At the same time, expert assessments of specialists in the field of information security were involved. When conducting the study, assumptions were adopted that the development of IPS takes place in accordance with the current normative acts of Ukraine, namely DSTU 3396.0-97

"Protection of information. Technical protection of information. Basic Provisions" and DSTU ND TZI 3.7-003-05" Procedure for building an integrated information protection system in the information and telecommunications system".

The materials of the study are the projects of currently active protection objects and reports on the effectiveness of countermeasures against threats in recent years.

Microsoft Office was used as the research software.

5. Results of research into the possibility of obtaining quality indicators of information protection projects

5. 1. Unity of quality indicators of information protecp tion systems projects

To compare the quality indicators of the projects, the language of the description of the objects is necessary. One of the possible procedures for representing the description of objects in the form of a semantic description of images of objects is given in work [5].

The sequence of design stages is considered according to two logical levels of decision-making. At the same time, at the first level, the possible actions of the intruder are determined in the definitions of threats to the object, which, in turn, determine the possible directions of protection. At the second level, possible countermeasures on the part of the object are determined.

At the same time, a separate automated system (AS) as the body of ICS, and a separate OIA that does not include ICS in its composition, are represented in their entirety in the form of some complex object called the object of protection of the general structure (OPGS) [5].

In general, the structure of the protection system should correspond to the structure of a hierarchical distributed AS of class 3, according to ND TZI 2.5-005 -99 "Classification of automated systems and standard functional profiles of protection of processed information against unauthorized access".

Then the general structure of ZI system is a set of complexes of means of protection (CMP) of certain levels. And the quality of information protection projects and the quality of protection of projected OIA also have a hierarchical nature. That is, the quality of the higher-level protection project has the worst indicators of the quality of the lower-level protection projects.

The rules for the formation of IPS and IIPS, formulated for various cases of distributed OPGS, are given in work [5]. According to these rules, the image of threats (Y) determines the directions of protection, while the definition of means of protection (Z) is carried out using the corresponding database. The set of protection means consists of active ($Z(A_i)$) and passive ($Z(P_i)$) protection means, prohibitions (restrictions) in the use of certain means ($Z(N_i)$), as well as cryptographic means ($Z(K_i)$).

In work [5] it is shown that the general expression of logical connections for the set of considered OIA structures takes the form:

$$Z(A,P,N,K) = Z(P) \wedge \left[Z(K) \vee Z_2(A_i) \right] \Leftrightarrow$$
$$\Leftrightarrow \min\left[Z(P), Z(K) \vee Z_2(A_i) \right]. \quad (1)$$

The right-hand side $\min[Z(P), Z(K) \vee Z_2(A_i)]$ of expression (1) meaningfully means that if three conditions are fulfilled, namely:

1) when the objects of protection will be represented according to the structures of OPGS;

2) classify the structures of OPGS by types according to Table 1;

3) at the design stages, use protective measures based on restrictions and prohibitions $Z(N_i)$ and associative memory (AM) as a database describing the state of the object, a database of threats, and a database of methods and means of protection. Accordingly, based on the design result, a decision should be made regarding 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 according to expression (1) proves that it is impossible to create a situation where the same or almost identical objects receive different solutions regarding their IPS and IIPS.

Thus, predicate (1) is a sufficient single expression that describes the logic of selection [5, 13–18] when equipping the protection system of any OPGS. As a result, the learning algorithm of the network model during the formation of the database of the description of the object's state, the database of destabilizing factors (DF) or threats, the database of protection means and the connections between them will make it possible to obtain a single solution for each individual OPGS. Moreover, the expression (1) itself is not a description of the sequence of actions by which the design process is determined. The proof of the validity of predicate (1) in work [5] means that for any real object (that is, one for which the restrictions according to $Z(N_i)$) are fulfilled) there is only one decision in the choice of methods and means of protection. At the same time, this decision objectively makes logical sense and has the property of the sufficiency of the selected methods and means of protection to solve the protection problem without the need to include redundant (repeated) protection elements. That is, for such objects, there is an objective solution, and it is the only possible one. This is where the meaning of decision optimization lies in designing, and therefore in determining the quality indicators of information protection projects and the quality of OIA protection.

This means that the quality indicators of protection designs are also the same, regardless of the preferences and qualifications of the human designer.

5. 2. Obtaining quality indicators of information protection projects

In general, the design structure of IPS (or IIPS) consists of stages, some of which do not lend themselves to strict algorithmizing. Such stages are determined by the list according to Table 1.

The design algorithm of IPS according to DSTU 3396, and IIPS according to ND TZI 3.7-003-05, is currently determined for ICS by eight stages of creating IIPS and is shown in Fig. 1.

The design algorithm of IIPS for IIPS should additionally take into account:

– the main principles that determine the sequence of actions during design according to Fig. 1, given in [5];

– the procedure for developing an information protection system;

– directions for protection of OPGS for technical channels and protection against physical unauthorized access (UAA).

Table 1

List of design stages with the use of AM

No.	Stage name
1	Formation of the list of threats of the i-th object Y_i from the database of threats $Y(S, \mathrm{DF})$ according to the state of the object $S(I)$ with elements I, defined in the form of specification DF_i from the database of DF
2	Determining the relationships between violations Y_i and counter-actions as components of IIPS Z_i
3	Formation of a list of means of protection by directions of protection $\{Z(A,P,K), N=\mathrm{const}\}$

The main difference of the design algorithm of IIPS for OPGS is the need at the initial stage to determine the structure of OPGS, taking into account the functional purpose of the design object and the connection of its functional purpose with the object of protection. The object of protection can be a room or territory where restricted access information (RAI) circulates with a defined restricted area (RA), a physical line of communication as the body of ICS, information circulating within the ICS. At the same time, ICS has a single-level or hierarchical (multi-level) structure and may include open communication channels (for example, mobile or satellite communication networks).

The sequence of stages, which determines the general algorithm for creating IIPS for OPGS with either an existing AS concept or a defined functional purpose of OIA, is shown in Fig. 2.

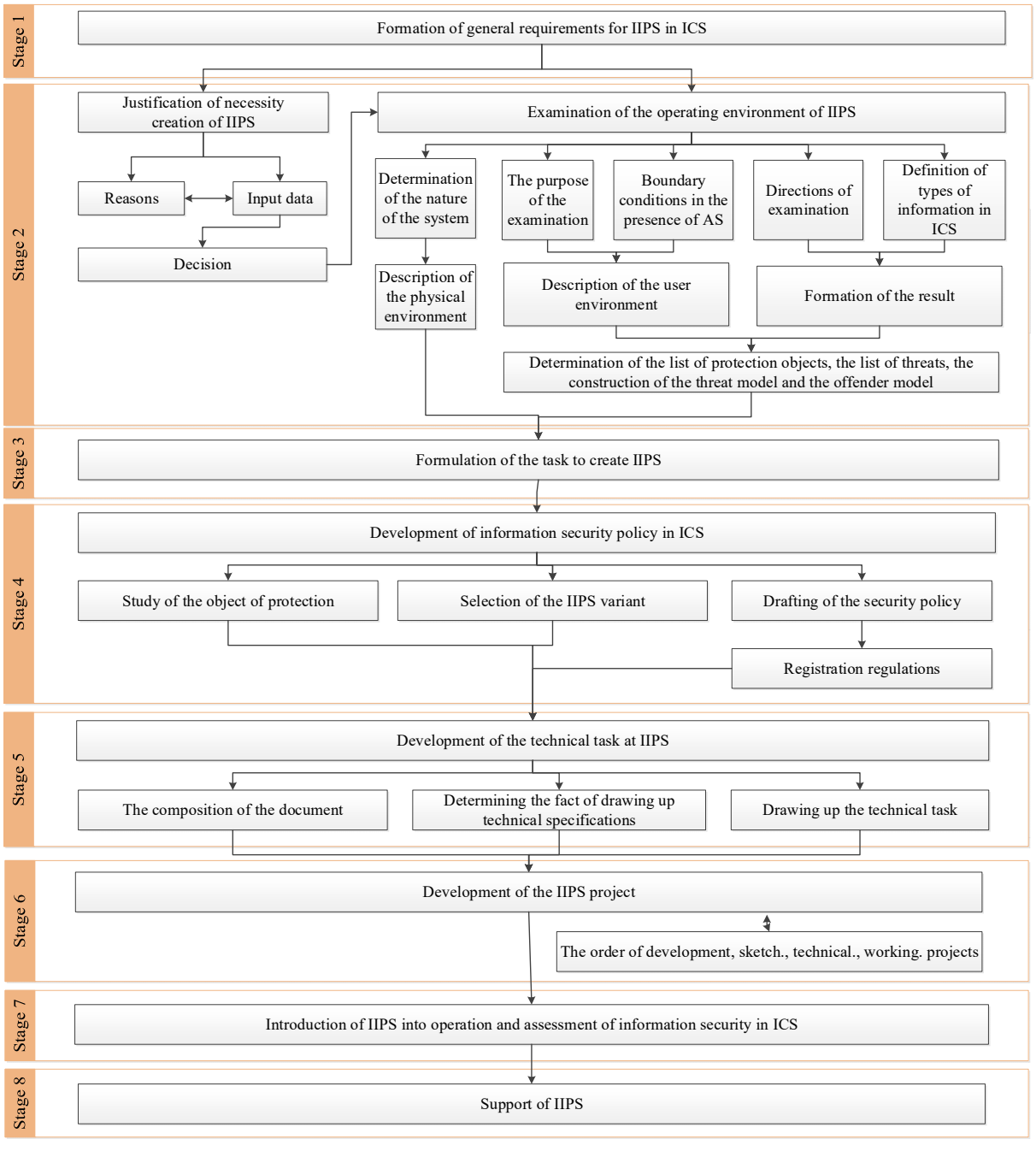

Fig. 1. Stages of creating an integrated information protection system in the information and communication system according to [2]

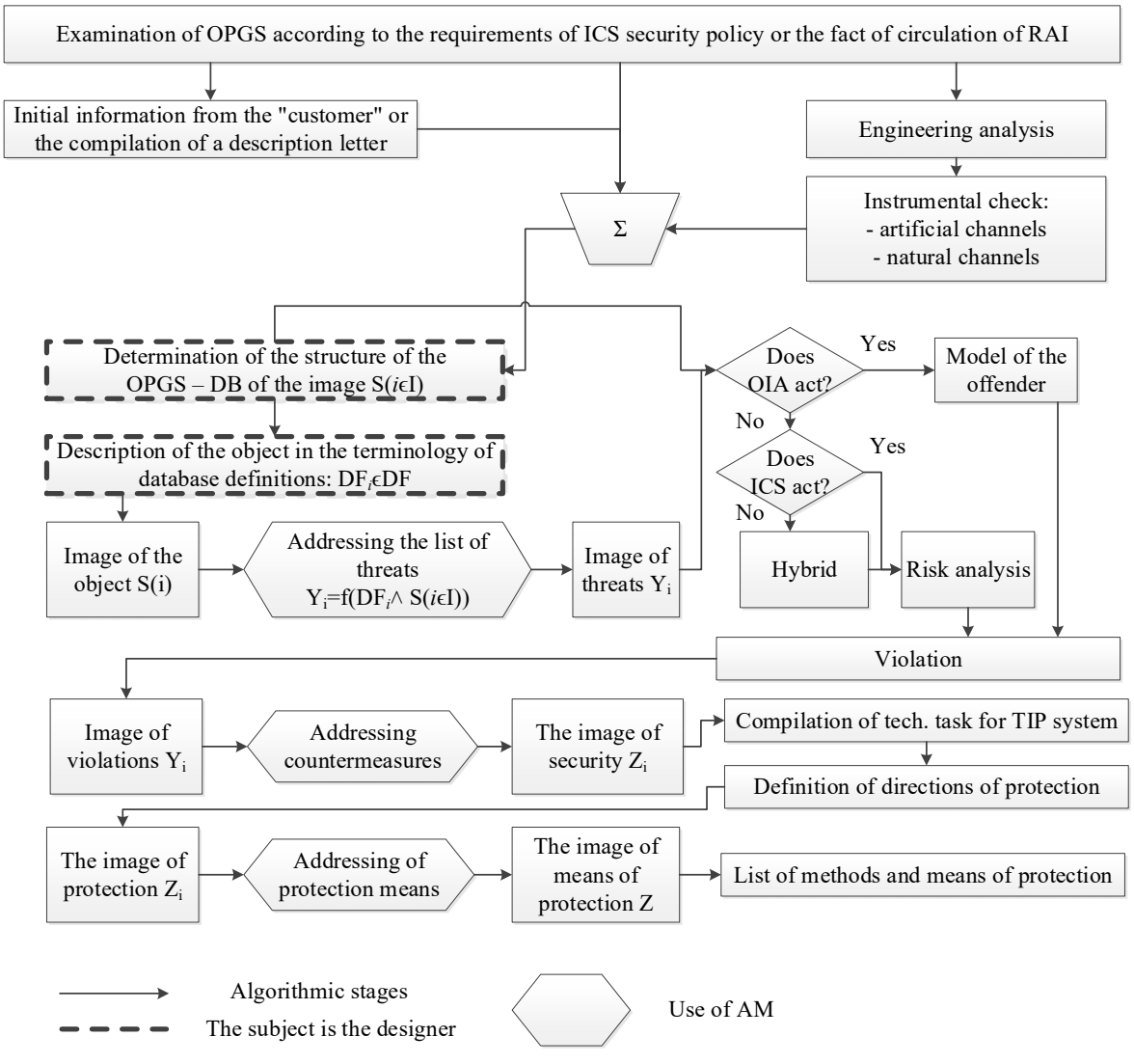

Fig. 2. The general algorithm for designing an integrated protection system for the protection object of the general structure

The results of the comparison of the main stages of the creation of IIPS in ICS according to the current regulatory documents (Fig. 1), as well as the proposed method (Fig. 2), are given in Table 2. The main differences are formulated at the end of Table 2 in the Notes section.

Table 2

Comparison of OPGS design algorithm and the current IPS design sequence

Eight stages of creation of IIPS in ICS (according to Fig. 1)	The general algorithm for the design of IIPS for OPGS (according to Fig. 2)
1	2
Formation of general requirements for IIPS in ICS	Examination of OPGS according to the requirements of ICS security policy or the fact of circulation of RAI
This stage according to ND TZI 3.7-003-05 arises as a result of the already adopted decision at the stages «Formulation of requirements for AS» and «Development of the concept of AS». Therefore, at the second stage of creation of IIPS, the point «Justification of the need to create IIPS» according to Fig. 2 does not make sense because such justification has already been implemented. Therefore, the item «Survey of the operating environment of IIPS» actually makes sense as an initial stage	Together with the items "Engineering analysis" and "Information from the customer" (if necessary, similarly to receiving the "survey letter" "Development procedures" of the ZI system), the difference between this stage and the current one is the difference in the purpose of the survey. Here, the goal is to determine the place of IPS or OIA as a structural unit that is examined in the general hierarchy of the structure of the protection object. That is, the type of OPGS structure is determined. The completion of this stage is "Determining the structure of OPGS – DB image $S(i\epsilon I)$"
2. «Description of User Environment», «Description of Physical Environment» and definition of «Threat List» and «Threat Model»	Description of the object of OPGS structure using the terminology of the definitions of the DB $DF_i\epsilon DF$
3. Formation of the task of creating IIPS	Obtaining an image of threats from the AM list of threats: $Y_i=f(DF_i\wedge S(i\epsilon I))$

Continuation of Table 2

1	2
4. Development of information security policy in ICS. Studying the object	Obtaining an image of Z_i security against AM countermeasures
5. Development of the technical task for IIPS	Obtaining a list of methods and means of protection $Z(A,P,K,N$=const) against AM of means of protection
6. Development of the IIPS project. Development procedure, sketch, technical, working projects	Documentation of the project result in the form of «Implementation of OPGS IIPS into operation».
7. Implementation of IIPS and assessment of information security in ICS 8. Accompanying IIPS ICS	Support of OPGS IPPS

*Notes: the stage "Description of the object of the structure of the OPGS using the terminology of the definitions of the DB DF_i**O**DF" allows one to bypass the definition of the connections between the description of the object and the definition of threats (or DF of threats), which is currently a problem (chapter 2.1.2, Fig. 6). The stage "Obtaining an image of the protection Z_i against AM of countermeasures" during the design of IIPS for OPGS made it possible to exclude from the procedure "Creation of IIPS for ITKS" the fourth stage of design – "Study of the object", which fundamentally transfers the design process from a scientific and technical task to a formal one implementation of the proposed procedures*

5. 3. An example of obtaining quality indicators that illustrates the possibility of creating projects with predetermined quality indicators

The specified comparison of design algorithms requires an assessment of the quality of existing IPS or IIPS projects and such projects, which are proposed in this work and involve the introduction of the concept of OPGS. At the same time, we note that when creating a design methodology, it is advisable to evaluate the quality and design procedures and the quality of the design consequences.

Under such conditions, the quality of any IIPS project should be determined by the level of decisions made in relation to the fulfillment of the assigned task. The main quality indicators can be maximum manufacturability, minimum project implementation costs, maximum used parameters of the technical characteristics of the design object, level of detail, minimum or maximum project costs, project completion period. Two types of quality indicators should be taken into account in the case of design of IIPS. One type of indicator is the quality of functioning of the designed protection object. The second is the quality of the design process. Having the design algorithms of ICS and OPGS, it is possible to compare these algorithms according to both types of quality indicators.

There are several procedures of structural analysis of cause-and-effect relationships, which can be used both individually and in various combinations to find the root causes of incidents in statistical quality control. One of them is the method of compiling Ishikawa diagrams [19] and Pareto charts [20]. In the scientific literature, Kaoru Ishikawa's cause-effect diagram is also known as the fishbone diagram, the control diagram of the effects of design due to the cause-and-effect diagrams of quality loss. Accordingly, a comparison of the reasons for the decline of those factors that reflect the sustainability of the object can be represented using this type of diagram.

For any information protection projects, the stability of the object of protection is determined by the preservation of five properties of information, which are: confidentiality, integrity, availability, observability, and controllability (controllability is defined as a guarantee of the correctness of services).

If we take into account this list of information properties, then the 5-factor Ishikawa diagram can look like Fig. 3. Reasons that reduce the quality of the design consequences are included in the consideration of the Ishikawa diagram, if you use the current design algorithm of IIPS according to Fig. 3 in comparison with the design algorithm of the IIPS OPGS proposed in this work in Fig. 2, on the condition that the quality of the project of IIPS OPGS is 100 %.

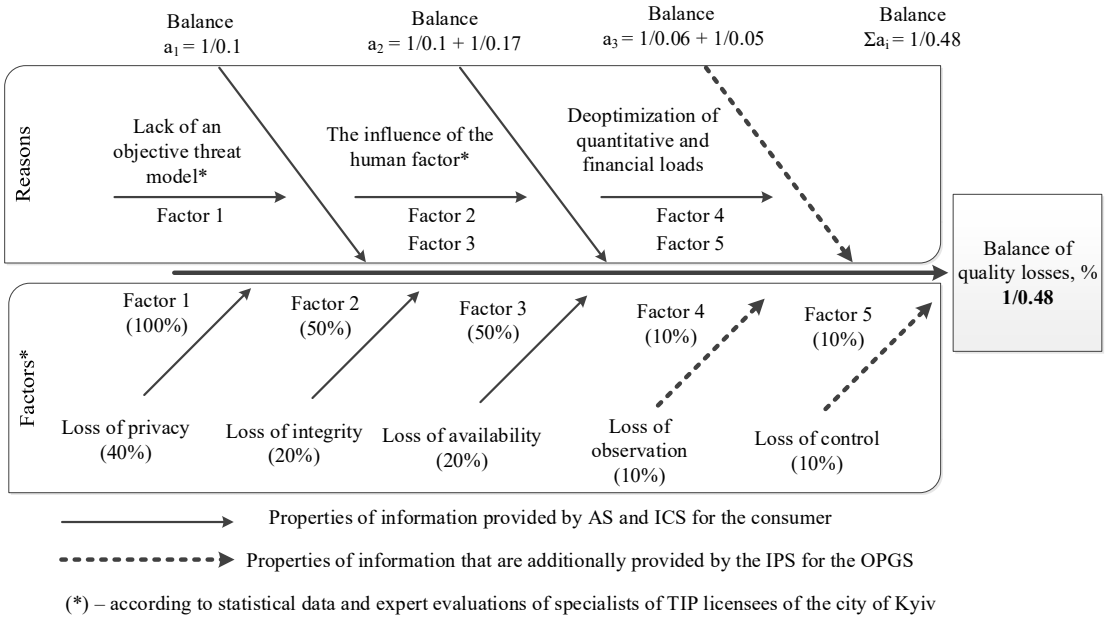

Fig. 3. Ishikawa diagrams of quality control of design results

As follows from the diagram, the overall quality balance is 1/0.48. This means that the quality indicator of the design consequences, that is, the quality of the designed object protection system according to the proposed algorithm (Fig. 2), is 2.08 times higher than the current design technique.

The quality of the design procedure itself can be illustrated by the well-known Pareto chart of the distribution of quality by defects in Fig. 4, where defects are quality indicators a_i.

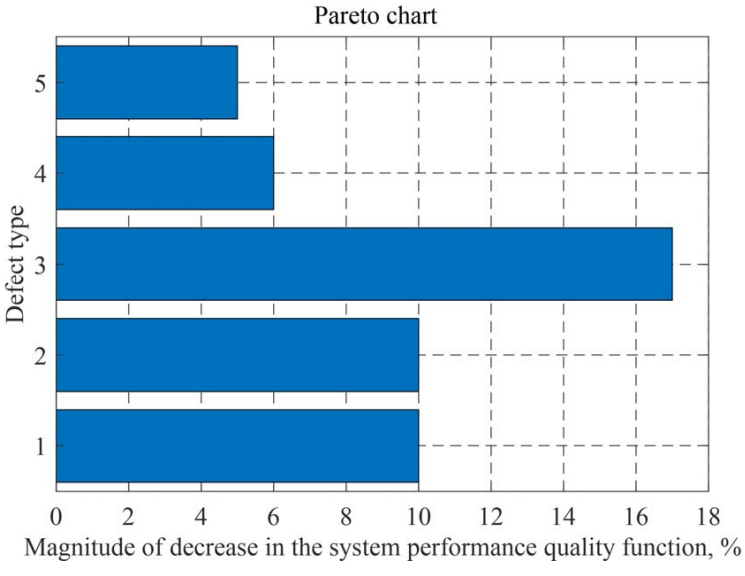

Fig. 4. Quality of the design procedure

It follows from the Pareto chart that the quality of the design procedure according to the current algorithm (Fig. 1) does not exceed 20 % in comparison with the design proposed according to the design algorithm of OPGS.

Ishikawa diagram and Pareto chart are drawn up under the conditions of the theoretical worst case for the design methodology of IIPS for OPGS. Thus, when comparing indicators according to the Pareto chart, only defect No. 3 is taken into account, because it is the most disadvantageous for the projects of IIPS OPGS. That is, practically, the comparative values of the quality indicators are significantly higher in favor of the projects of IIPS OPGS.

6. Discussion of results of investigating the possibility of creating and comparing the quality of information protection projects of objects

We have obtained results regarding the possibility of creating and comparing the quality of information protection projects. This became possible due to the introduction into the design process of the technique for analyzing the quality of future projects, which had not been used until now.

The features of the proposed method of comparing the quality of projects are based on the consideration of the structures of any objects of information activity, as such, which have the properties proposed in [5]. At the same time, they are called objects of protection of the general structure. The design stages for such objects involve the use of AM according to the generalized algorithm according to Table 1.

The main feature of the projects of OPGS is the unity of protection projects, which is proved by predicate (1). Therefore, the comparison of projects for OPGS is an objective and obvious procedure. In order to compare the quality of projects for the protection of existing facilities with OPGS, examples of the list of design stages of existing projects and projects for future OPGS are considered. Such lists are presented in Table 2. The sequences of creating projects according to the design stages are described in detail by block diagrams in Fig. 1, 2. Our paper examines the procedure for comparing the quality of projects of OPGS and existing objects, which is based on the use of Ishikawa quality diagram and Pareto chart. They have not yet been used in the field of information protection. An example of such use is given, respectively, to determine the quality of the design result in Fig. 3, and to determine the quality of the design procedure in Fig. 4. Moreover, according to Fig. 4, it is convenient to determine the weakest points in protection projects. For example, for this case, quality indicator number 3 has the biggest quality defect. It is a generalized indicator of loss of integrity and availability.

The limitation in the use of the technology for comparing the quality of protection projects is limited access to the documentation of existing objects. In addition, the limitations are the shortcomings of the currently valid normative-methodical and legislative documentation in the field of technical information protection. These limitations require adjustment.

To obtain qualitative and quantitative indicators of research results, statistical data on the operation of protection objects is necessary. Such statistics require the collection of data on the quality indicators of future projects for at least 4 or 5 years.

The development of this study consists in the adjustment of the regulatory and methodological base of technical information protection, adjustment of some current standards according to [3].

7. Conclusions

1. The presence of a single solution indicates that during design, it can be considered proven to prevent the situation when the same or almost identical objects receive completely different design decisions regarding their IIPS, and the quality of IPS also has the unity of indicators of this quality.

2. We have proposed an approach to obtain project quality indicators through the use of the well-known Ishikawa quality control diagram and Pareto chart. Moreover, these diagrams were not previously used for quality control of projects in the field of information security, and there are no references to them from the regulatory and methodological documentation.

3. An example of the use of 5-factor Ishikawa diagram and Pareto chart is given. Weight percentages of factors affecting the quality of current projects and projects created according to the proposed methodology were obtained in relation to hypothetical objects. At the same time, the statistics of percentage ratios of influencing factors are set hypothetically.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

The data will be provided upon reasonable request.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. DSTU 3396.0-96. Information protection. Technical protection of information. Basic principles. Available at: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
2. ND TZI 3.7-003-2005. Poriadok provedennia robit iz stvorennia kompleksnoi systemy zakhystu informatsiyi v informatsiyno-telekomunikatsiyniy systemi. Available at: https://tzi.com.ua/downloads/3.7-003-2005.pdf
3. Jiang, Y., Ye, J., Zhang, Z. (2023). Protection and Utilization of Personal Information in the Context of Big Data. 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). doi: https://doi.org/10.1109/icdcece57866.2023.10151146
4. Blix, F., Elshekeil, S. A., Laoyookhong, S. (2017). Data protection by design in systems development: From legal requirements to technical solutions. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). doi: https://doi.org/10.23919/icitst.2017.8356355
5. 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
6. Yaremchuk, Yu. Ye., Pavlovskyi, P. V., Kataiev, V. S., Siniuhin, V. V. Kompleksni systemy zakhystu informatsiyi. Available at: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/
7. Yudin, O. K., Korchenko, O. H., Konakhovych, H. F. (2009). Zakhyst informatsiyi v merezhakh peredachi danykh. Kyiv: Vyd-vo TOV «NVP» INTERSERVIS», 716. Available at: http://bit.nau.edu.ua/vydannya/pidruchnyky/743
8. Informatsionnye tehnologii. Metody zashchity. Sistemy menedzhmenta zashchity informatsii. Trebovaniya. ISO/IEC 27001:2005(E):ISO/MEK.
9. Isazadeh, A., Lamb, D. A., MacEwen, G. H. (1996). Behavioral views for software requirements engineering. Proceedings IEEE Symposium and Workshop on Engineering of Computer-Based Systems. doi: https://doi.org/10.1109/ecbs.1996.494542
10. Harel, D. (1987). Statecharts: a visual formalism for complex systems. Science of Computer Programming, 8 (3), 231–274. doi: https://doi.org/10.1016/0167-6423(87)90035-9
11. von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security, 6 (5), 224–225. doi: https://doi.org/10.1108/09685229810240158
12. Buchyk, S. S., Shalaev, V. A. (2017). The analysis instrumental methods of identification of risks of information security information and telecommunication systems. Science-Based Technologies, 35 (3). doi: https://doi.org/10.18372/2310-5461.35.11841
13. Dombrovskyi, V. A., Kryzhanivskyi, I. M., Matskiv, R. S., Myhovych, F. M., Nemish, V. M., Okrepkyi, B. S. et al. (2003). Vyshcha matematyka. Ternopil: Vydavnytstvo Karpiuka, 480. Available at: http://dspace.wunu.edu.ua/bitstream/316497/612/1/vm_pidr.pdf
14. Zubenko, V. V., Shkilniak, S. S. (2020). Osnovy matematychnoi lohiky. Kyiv: NUBiP Ukrainy, 102. Available at: http://csc.knu.ua/media/filer_public/3b/80/3b805f5a-fb43-4249-b587-f13852e8ba37/osnovy_mat_logyky_posibn_020620.pdf
15. Bokan, B., Santos, J. (2022). Threat Modeling for Enterprise Cybersecurity Architecture. 2022 Systems and Information Engineering Design Symposium (SIEDS). doi: https://doi.org/10.1109/sieds55548.2022.9799322
16. Kiran, A., Dharanikota, S., Basava, A. (2019). Blockchain based Data Access Control using Smart Contracts. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). doi: https://doi.org/10.1109/tencon.2019.8929451
17. Peiris, C., Pillai, B., Kudrati, A. (2021). AWS Cloud Threat Prevention Framework. Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks. Wiley, 243–319.
18. Tekinerdogan, B., Ozcan, K., Yagiz, S., Yakin, I. (2021). Model-Based Development of Design Basis Threat for Physical Protection Systems. 2021 IEEE International Symposium on Systems Engineering (ISSE). doi: https://doi.org/10.1109/isse51541.2021.9582528
19. Pidvyshenna, N. V., Kubyshyna, N. S. (2015). The quality management of productsin industrial enterprises. Efektyvna ekonomika, 11. Available at: https://ela.kpi.ua/bitstream/123456789/12600/1/2013_5_Pidvyshenna.pdf
20. Kalashnikova, Kh. I. (2023). Upravlinnia yakistiu. Kharkiv: KhNUMH im. Beketova, 138. Available at: https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0052415.pdf