Journal of Computer Science

Original Research Paper

Developing the Concept of Methodological Support for Designing and Assessing the Efficiency of Information Protection Systems of Standard Information Systems Considering Their Vulnerabilities

[1]Islam Alexandrovich Alexandrov, [2]Andrey Victorovich Kirichek, [1]Vladimir Zhanovich Kuklin, [1]Alexander Nikolaevich Muranov and [1]Leonid Mikhajlovich Chervyakov

[1]World-Class Scientific Center "Digital Biodesign and Personalized Healthcare", Institute of Design and Technology Informatics, Russian Academy of Sciences, Russia
[2]Rector's Office, Bryansk State Technical University, Russia

Article history
Received: 03-05-2023
Revised: 03-07-2023
Accepted: 22-08-2023

Corresponding Author:
Vladimir Zhanovich Kuklin
World-Class Scientific Center "Digital Biodesign and Personalized Healthcare", Institute of Design and Technology Informatics, Russian Academy of Sciences, Russia
Email: kuklin_vladimir_ran@mail.ru

Abstract: The Information Protection System (IPS) is an integral part of any Information System (IS). To develop an optimal IPS model at the earliest stages of the IS lifecycle, it is necessary to develop IS resource and threat models. This study is devoted to developing a specific model of IS resources, allowing a detailed description of the relationship between resources and business processes and developing an IS threat model to describe in detail the relationships between threat implementations, various IS vulnerabilities, and the relationships between them. To solve these problems, this study used the methods of set theory, graph theory, probability theory, game theory, random processes theory, mathematical logic, and object-oriented approach. This study simulated different variants of the IPS and found that only a balanced IPS project met the Pareto demands. The projects where the emphasis is on countering only external or internal threats do not meet these demands.

Keywords: Information Protection System, Information Security, Information System, Threat Implementation Model, Vulnerability

Introduction

Any modern company cannot function without using large amounts of information, which needs constant processing and analysis to optimize its activities (Raguseo, 2018; El Alaoui and Gahi, 2020). Only specific IS, a streamlined set of documents and IT that collect, process, and communicate information (Stratton and Carter, 2023; Kuklin *et al*., 2022) can perform such activities. Public and commercial companies must protect data, which is, along with material resources, one of their most valuable resources (Párizs *et al*., 2022). To protect data, companies use special IPS, a combination of various software, technical, and hardware tools and approaches to ensure the safety of information processed within the IS (Kuklin *et al*., 2023; Alexandrov *et al*., 2022). The main problem in IPS development is that all existing IPS have vulnerabilities that make it possible to bypass protections and gain unauthorized access to data. The vulnerabilities are usually the result of mistakes made in the IPS design or the direct implementation of software and hardware security tools (Friha *et al*., 2023; Louk and Tama, 2023).

To minimize the number of vulnerabilities in IPS, constant refinement and improvement are necessary (Jbair *et al*., 2022). Discovering vulnerabilities is complicated because they can exist in any structural element of IS; moreover, problems can relate to both software and hardware. Information security requires investigation of IS structure features with a particular focus on interacting its various components with each other (Khalil *et al*., 2023). Therefore, creating an IPS model at the earliest stages of IS lifecycle is an urgent scientific challenge.

From the literature and practice, many approaches to modeling IPS are known, such as generalized models, models involving the use of probability theory principles, models based on the theory of random processes, models based on Petri nets, and many others. However, none of the approaches can fully satisfy all the security criteria. In addition, as far as we know, no detailed analytical review has yet been published to understand the current state of

the art in IPS model development, to classify and compare IPS models while identifying their advantages and disadvantages. Therefore, it is relevant first to conduct an analytical review of current IPS models to determine their theoretical significance and practical applicability. Furthermore, it is necessary to create methodological support for synthesizing the optimal IPS model, including creating a model of IS resources and IS threat modeling. The solution to these scientific problems is the purpose of this study. The results of this study can be helpful to practitioners-developers of IPS of modern IS and enrich the theoretical area of IPS research by analyzing and comparing existing IPS models and identifying their strengths and weaknesses.

Analytical Review of Current IPS Models

Many IPS models now exist, allowing the study of IS information security (Akkad *et al*., 2023; Ahmad *et al*., 2022). Along with this, note that in practice, different approaches to modeling such information security systems exist, allowing a wide variety of aspects of security systems (Logrippo, 2021; Yamin *et al*., 2021). Classification of such models is performed depending on the specific tools used in the study. Thus, generalized models, models implying the use of probability theory principles, models based on the theory of random processes, and models based on Petri nets exist. Moreover, note that these are far from the only tools to solve such problems because they are based on automata theory, graph theory, and fuzzy sets.

Many studies by Ghiasi *et al*. (2023); Zhang *et al*. (2020) have investigated generalized IPS models. Their main feature is the simultaneous consideration of numerous factors that determine the functioning of the protection system. To date, the most widely used in practice is the approach to model building based on probability theory (Mazzoccoli and Naldi, 2022). Along with this, zone, probabilistic, and destructive impact models exist (Egoshin *et al*., 2020; Gontarczyk *et al*., 2015; Oleinik *et al*., 2020). The main advantage of probabilistic models is that they allow for the most accurate determination of the probability of a particular threat occurring. However, it is necessary to understand that these models have a significant disadvantage they do not make it possible to determine the specific temporal characteristics of the threat implementation process.

Table 1: Result of comparative analysis of IPS modeling approaches on calculated parameters

	Ability to calculate			
IPS model type	Probability of overcoming	Time to overcome	Detection time	Risks
Generalized models	-	-	-	-
Probability theory	-	-	-	-
Random process theory	+	+ (For a semi-Markov process)	-	-
Petri nets	+	-	-	-
Automata theory	-	-	-	-
Graph theory	+	+	-	-
Fuzzy sets theory	+	-	-	+
Game theory	-	-	-	-
Entropy approach	-	-	-	-

Table 2: Results of comparative analysis of IPS modeling approaches on practical applicability and ease of defining input parameters

IPS model type	Practical applicability	Ease of determining input parameters
Generalized models	Use in practice is difficult because of the weak elaboration of the formal side of the model	The model uses abstract quantities to work, so the work is possible only with experts
Probability theory	does not allow for considering the potential ability of an attacker to overcome defenses through special training or equipment	From a practical viewpoint, it is too difficult to get parameters required for the model operation because statistical sampling will be insufficient
Random process theory	It has a poor correlation of model data with practice since the model uses abstract states of processes	Abstract parameters and does not make it possible to to determine the flux density and residence time in a particular state, which significantly reduces the system efficiency
Petri nets	This model is unable to characterize various ways to Overcome the protection systems	All necessary parameters are easy to determine
Automata theory	Using this model makes it possible to accurately Describe the features of the threat implementation process	determine the needed parameters is extremely simple and often involves the use of neural networks
Graph theory	It allows the most accurate description of all potential threat options	The required parameters are easy enough to obtain in practice
Fuzzy sets theory	It is relatively easy to use in practice	This implies the use of expert review results, but The disadvantage is that the results largely depend on the qualifications of specialists
Game theory	It is unable to consider the potential ability of an attacker to overcome defenses through special training or equipment	It is extremely difficult to obtain the needed input data
Entropy approach	This model implies using an approach by which it is impossible to describe the IPS features	It is extremely difficult to obtain the needed input data

As for models based on the theory of random processes, it is worth noting that their use in practice makes it possible to determine the probability of a specific threat occurrence. Moreover, this model allows the use of a semi-Markov process, with which it will be possible to estimate the temporal parameters of the particular threat implementation (D'Amico and Petroni, 2023; Dhulipala and Flint, 2020). However, it is necessary to understand that this approach has a significant disadvantage it is heavy to use in practice because of the need to define multiple states. In particular, it is difficult in practice to estimate the exact values of the flux density parameter since this criterion depends on numerous factors that are impossible to consider in this model (Marinin *et al*. 2023; Kharchenko *et al*., 2022; Gupta and Dharmaraja, 2011).

Thus, based on the statements above, it was possible to determine that none of the listed models fully satisfies the criteria identified. Tables 1-2 show more detailed results of the analysis.

Thus, based on the considered models, it is possible to conclude that all modern models can be used mainly for IS operation and support. The main disadvantage of these models is the impossibility of analyzing the compliance of a particular IS with all security parameters. Moreover, it is practically impossible to determine the most optimal IPS projects. In this regard, an urgent task today is to develop an IS resource model that can most accurately reflect the relationships between various resources and ongoing business processes. In such conditions, it is evident that it will be much easier to determine the potential threats encountered during IS operations.

Materials and Methods

To develop IPS design solutions, it is first necessary to determine:

- Methods and means of protecting information efficient in the operational aspects of the existing IS;
- The constraints are specific to IS. These are solutions already embedded in the latter and not amenable to change and adjustment;
- Security policy concepts. They may be specified and supplemented concerning individual design decisions to create an IPS

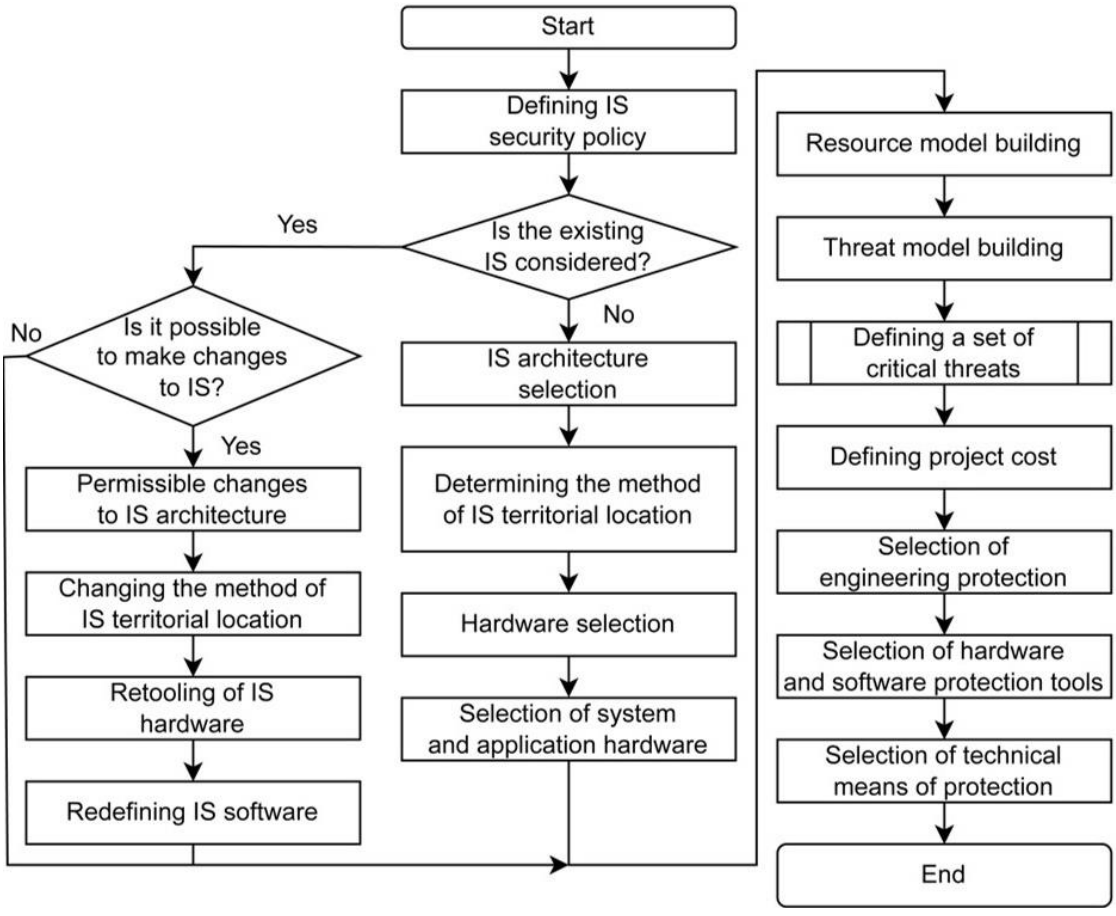

Fig. 1. Flowchart of the algorithm for creating a specific project for the IPS implementation

The algorithm for developing an IPS project consists of the following steps (Fig. 1):
Start as the first step:

1. Defining a security policy for a particular design solution that can either be uniform for all projects or include, in each case, some specific guidelines and criteria
2. Analyzing an existing IS or designing a new one parallel to developing a system to protect the information; however, if the IS does not exist yet, it is necessary to consider key security requirements
3. Determining the IS architecture if it develops parallel to the IPS preparation
4. Choosing how to locate IS (or to "relocate" the new system)
5. Selecting hardware and solutions, considering the provisions included in the security policy;
6. Selecting software tools, considering, as before, security policy
7. Evaluating the possibility of adjustments when working with an existing system
8. Determining the adjustments required for IS;
9. Building resource and threat models
10. Determining the most dangerous potential incidents when implementing a specific design solution;
11. Selecting the required information protection tools;
12. Estimating the cost of the design solution

Steps 4-7 and 9-12 must consider the list of constraints caused by changes to the IS. Using this algorithm, the specialists of the working group prepare individual design solutions, which are subsequently reviewed by the expert committee members.

Results

Developing the IPS Model

IPS Design Principle

This study considers the IPS model of the resource type. Its characteristic feature is that all existing relationships between resources appear using the following expression:

$$M_R = \{\{\mathrm{Or}\},\mathrm{HK},\mathrm{PT},\mathrm{S},\mathrm{R}f^R\} \quad (1)$$

where $\{o_R\}$ makes it possible to characterize specific information about the investigated potential resources of the system. The remaining parameters allow for describing the particular types of organization of the relationship between resources and their types. Rf^R is a relationship matrix whose main task is determining the potential presence of a relationship or its type between the information units that form the network.

Here it is essential to go into detail about *a* set of information data. It is an aggregate of the following forms:

$$\{O_R\} = \{\{\mathrm{BP}\},\{\mathrm{Sn}\},\mathrm{Rm}\},\{\mathrm{DC}_0\},\{\mathrm{DC}_a\},\{\mathrm{DC}_h\},\{\mathrm{NE}\},\{C\},\ \{\mathrm{SS}\},\{\mathrm{AS}\},\{D\},\} \quad (2)$$

where, $\{BP\}$ characterizes the specific business processes whose support provides the same for all system resources. $\{Sn\}$ describes the IS particular components designed to solve certain tasks. $\{DC_0\}$, $\{DC_a\}$, and $\{DC_h\}$ characterize the various data carriers used during the system operation. $\{NE\}$ is a set of devices to ensure the full functioning of the computer network. $\{C\}$ is a set of jobs to perform service software maintenance.

The outgoing source of the indicated relationship deserves special attention. This specific kind of source provides communication. It is necessary to understand that the functioning of any company involves using a set of dependent communication resources. Figure 2 presents in more detail a unified semantic network of IS sources developed during this research.

Figure 2 considers the aggregate of class resources or ongoing business processes in more detail. After analyzing this network, it may be concluded that only specific options exist for connecting networking elements. Figure 3 describes in more detail a particular network exit scheme.

Creating a Threat Scheme for a Company IS

The primary purpose of the threat scheme is that it can most accurately assess the specific damage formed with the launch of the threat. Simultaneously, it considers the particular negative consequences that occur using this source. It is essential to understand that the main feature of this threat scheme is that it is essentially a semantic grid whose formation occurs because of the significant increase in the sources with updated data. In this case, this threat scheme is considered to be a security threat. Thus, it may be concluded that the threat scheme has the following form:

$$\mathrm{M}_T = \{\{\mathrm{O}_T\},\mathrm{HK},\mathrm{PT},\mathrm{S},\mathrm{T},\mathrm{R}f^T\} \quad (3)$$

Next, let us propose to elaborate on considering the set of informational elements, a specific set described by the following expression:

$$\{\mathrm{O}_T\} = \{\{\mathrm{BP}\},\{\mathrm{Sn}\},\{\mathrm{Rm}\},\{\mathrm{DC}_0\},\{\mathrm{DC}_a\},\{\mathrm{DC}_h\},\{\mathrm{NE}\},\{C\},\ \{\mathrm{SS}\},\{\mathrm{AS}\},\{D\},\{\mathrm{Th}\}\} \quad (4)$$

where,

$\{\mathrm{BP}\},\{\mathrm{Sn}\},\{\mathrm{Rm}\},\{\mathrm{DC}_0\},\{\mathrm{DC}_a\},\{\mathrm{DC}_h\},\{\mathrm{NE}\},\{C\},\{\mathrm{SS}\},\ \{\mathrm{AS}\},\{D\}$ act as a general aggregate of resources used within a given system.

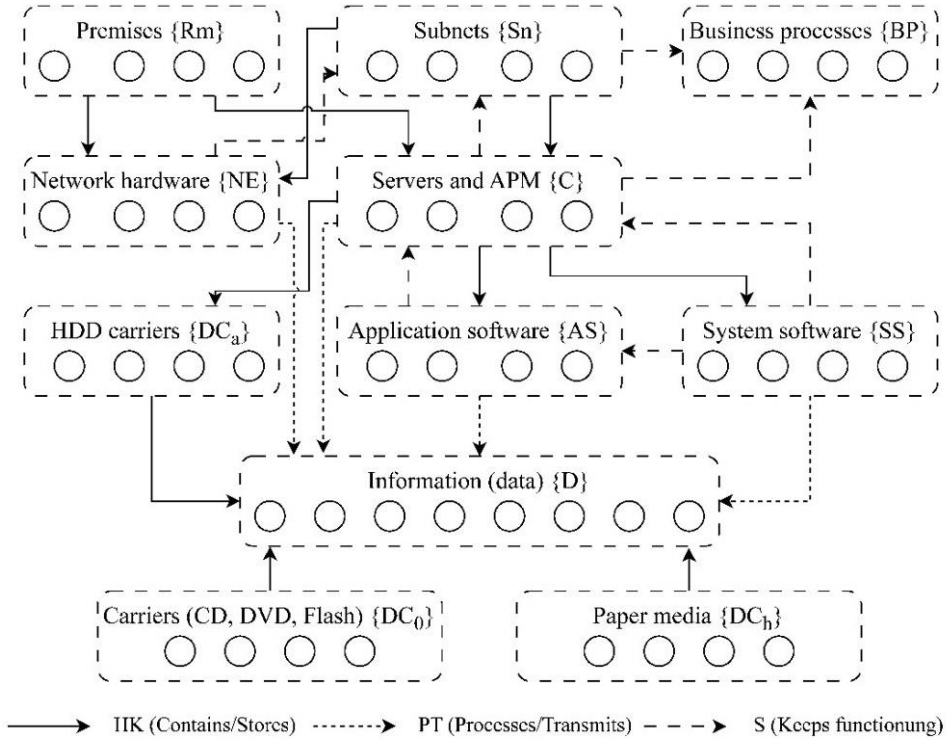

Fig. 2: Scheme of IS information resources

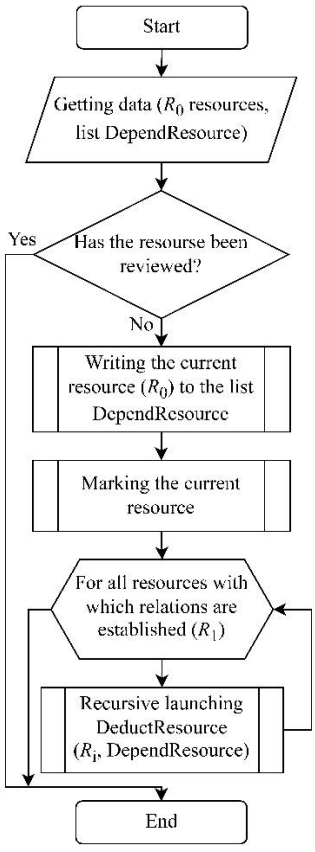

Fig. 3: Flowchart of the algorithm for exiting

Using such an approach makes it possible to define more precisely the set of threats, which looks as follows:

$$\{Th\} = \{CV,IV,AV,Ds,Mf,Tf,A\} \quad (5)$$

where, CV describes data leakage directly, AV-unavailability, Ds-elimination, Mf-malfunctions, Tf-theft, and A-adding adjustments.

Figure 4 shows in more detail the threat model developed as part of this research.

It is worth understanding that there is a very specific relationship between all threats and resources described by the following relation:

$$x_i \mathrm{Ty}_j \quad (6)$$

where x_i characterizes a particular kind of resource or defines a type of business activity and y_i describes the type of threat itself. Here the matrix of the form $M = |t_{ij}|(i \in \{O_R\}, j \in \{Th\})$ plays an important role, allowing a more detailed threat description. The matrix element t_{ij} is 0 if the relationship is absent and 1 if it occurs. Table 3 presents this matrix M in a general form.

A characteristic feature of this matrix is that it does not consider a specific type of resource or a business process. Instead, the key focus is on examining this potential diversity which makes this methodology more versatile, but one must understand that it is crucial to define all the possible elements of the matrix as accurately as possible.

Table 3: Connection matrix of data system resources and threats

	CV	IV	AV	Ds	Mf	Tf	A
BP	0	0	0	0	1	0	0
SN	0	0	0	1	1	0	0
RM	0	0	0	1	0	0	0
DC_0	0	0	0	1	0	1	0
DC_a	0	0	0	1	0	1	0
DC_h	0	0	0	1	0	1	0
NE	0	0	0	1	1	1	1
C	0	0	0	1	1	1	1
SS	0	0	0	1	1	0	1
AS	0	0	0	1	1	0	1
D	1	1	1	1	0	0	0

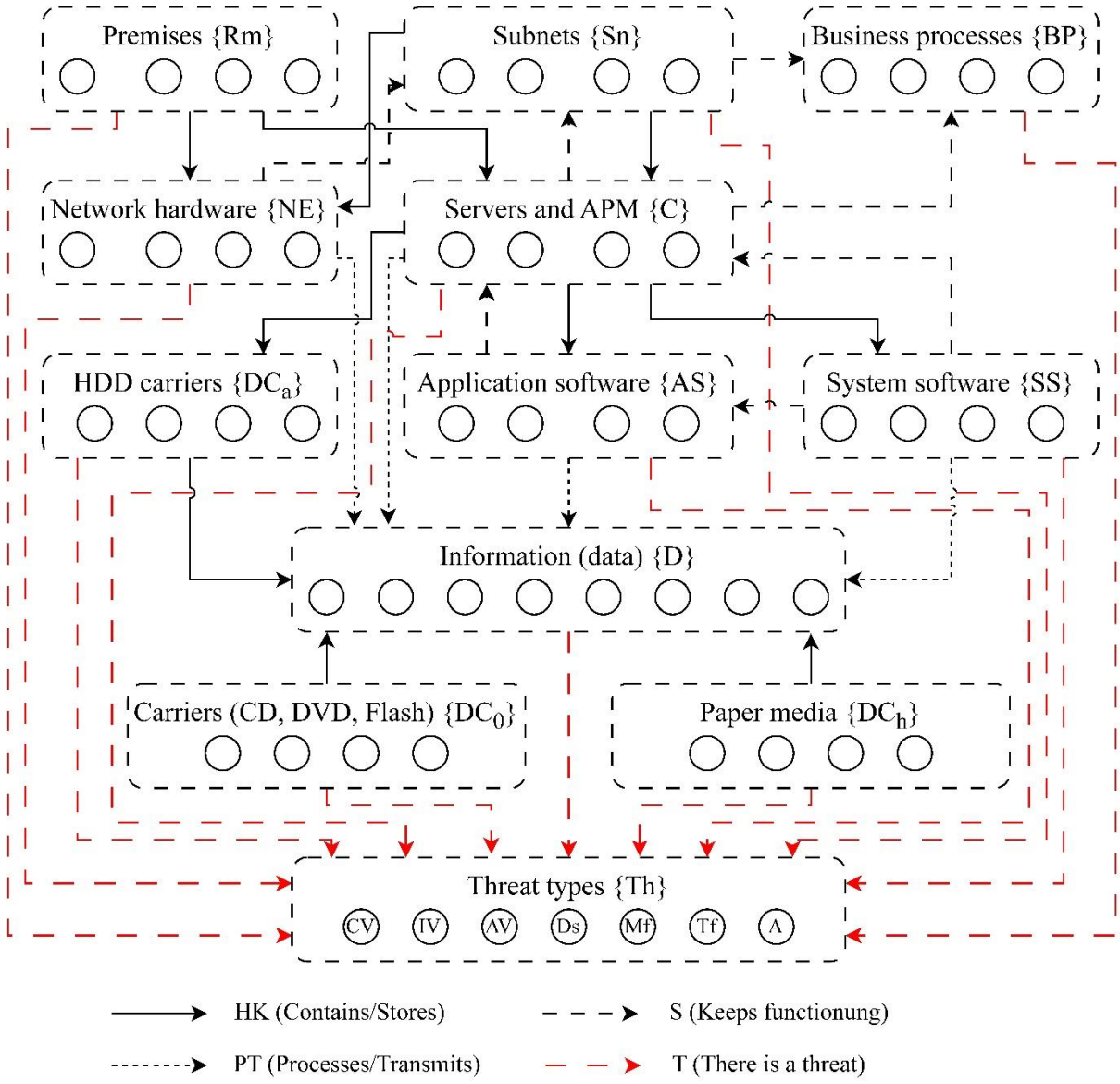

Fig. 4: Description of the resource and threat schemes

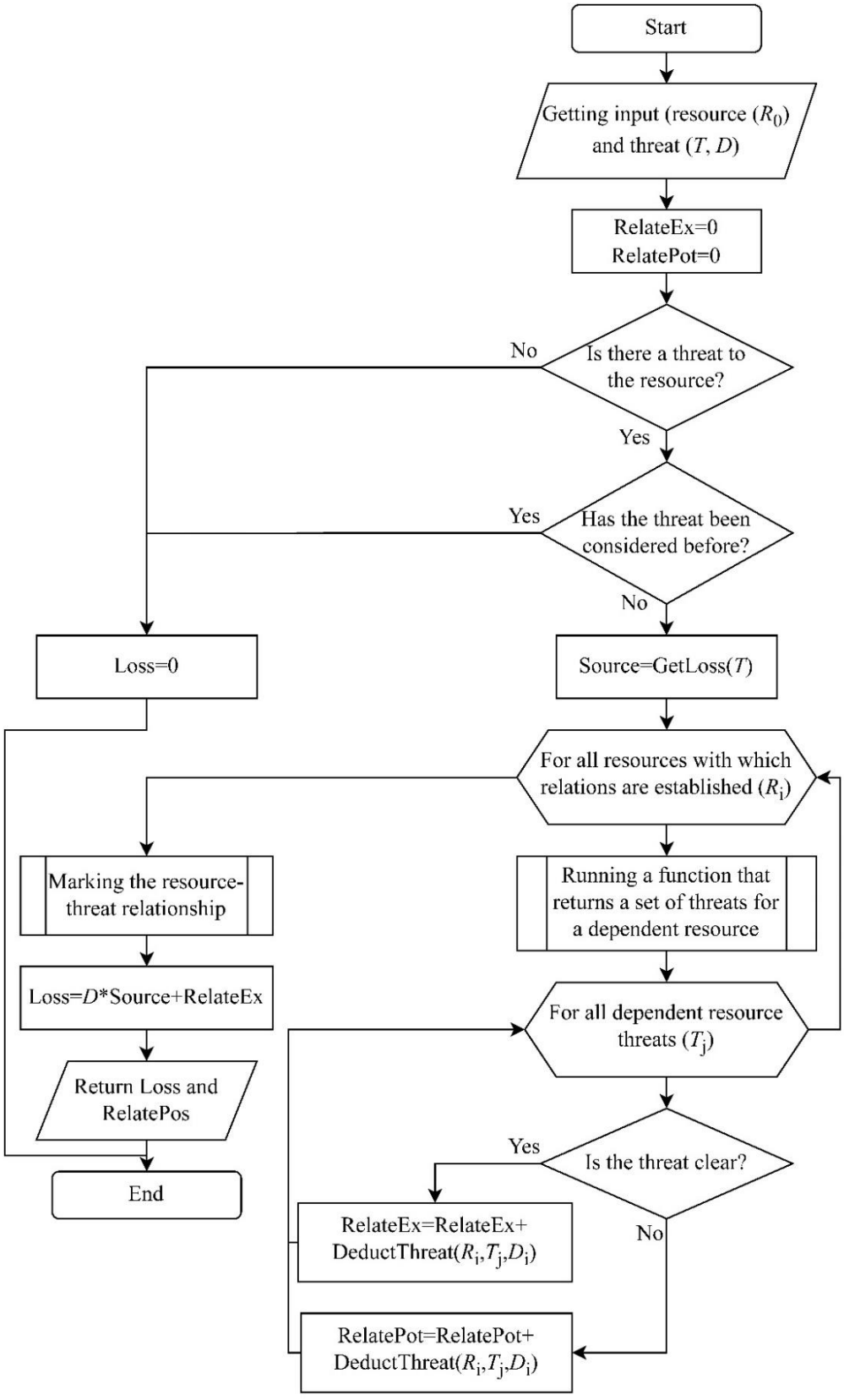

Fig. 5: Flowchart of the inference algorithm from the resource model

The process of threat implementation implies that some initial source facilitates the threat launch transmitted through appropriate relationships.

However, other linked sources and resources will not necessarily become carriers of this risk. For example, information carrier elimination will lead to damage or complete loss of information, but these data will not lose their secrecy. Thus, it is crucial to consider the specific type of the formed threat additionally classified into obvious and potential within this approach. Obvious threats are the category that requires compulsory execution in terms of the initial type of sources. The second category includes threats that function only when their source has a certain permissibility. A striking example is an attempt to steal a data carrier, where a thief will find competent encryption of all data, preventing him from gaining access to it. Figure 5 shows in more detail the specific algorithm for resource withdrawal from the scheme.

Principle of Forming a Complex IPS

If we consider a variety of resource and threat schemes, it is worth noting that in practice, the method of creating a separate program with a graphical user interface is widespread. This interface makes it possible to build and efficiently configure semantic grids and as a result, obtain all necessary research results. In this approach, it is essential to identify and highlight the most critical threats. Initially, a general list of hazards from sources is generated and then classified according to the level of damage and risk. A specific threat is critical if one of the following conditions applies:

$$Loss_{ThR_1} \geq Loss_{крит}$$

$$Loss_{ThR_1} + RelatePot_{ThR_1} \geq Loss_{крит}$$

It is worth understanding that the user will determine critical conditions. The category of critical threats may include all potential threats to existing resources. The effective execution and solution of all tasks assigned to an organization's protective system require implementing this system in complex modeling. Figure 6 describes this approach in more detail.

Determining the specific value of the risk of the model disposed at the lowest level requires special semi-Markov schemes for the threat implementation. However, determining the probability of a hacker's desire to implement a particular threat requires other approaches.

Developing an Optimal Data Protection Project Scheme

As a part of this paragraph of the research, let us consider in a little more detail the search scheme of the efficient project. Its basis is the organization of the efficient interactions between statistical data and the environment. Such a search scheme will have the following form:

$$\gamma = (X, D, H)$$

$$\gamma = \max_i \min_j h(x_i, \omega_{jk})$$

$$S = \max_i \min_j R(x_i, \omega_{jk})$$

where, $R(x_i, \omega_{jk}) = \max_i (H(x_i, \omega_{jk})) - H(x_i, \omega_{jk})$-auxiliary losses (risks).

Laplace:

$$L = \max_i H(x_i | P(\omega_k)) = \max_i \sum_{j=1}^{n} h(x_i, \omega_{jk}) p(\omega_{jk}) \quad (7)$$

at:

$$p(\omega_{jk}) = 1/n$$

Hurwitz:

$$G = \max_i [\lambda \min_j h(x_i, \omega_{jk}) + (1 - \lambda) \max_j h(x_i, \omega_{jk})] \quad (8)$$

at:

$$0 \leq \lambda \leq 1$$

It is essential to understand that the semi-Markov model of overcoming the defense system will be applied to determine the specific size of the threat. Such an approach implies that the threat implementation, in any case, implies an attempt by the hacker to overcome the existing means of protection. A requirement for such an attempt is that any protection system has particular weaknesses acting as a threat. These include software vulnerabilities, misconfigured security systems, physical media problems, and other factors.

Creating a Semi-Markov Threat Implementation Model

One of the characteristic features of any IS vulnerability is that not all of them are easy to use by attackers. For example, a sufficiently large category of threats can occur only if the attacker has specific knowledge and special equipment. Moreover, it is worth understanding that in practice an attacker can find only those vulnerabilities that he can use with his capabilities. Thus, when designing IS, it is necessary to adequately assess the existing weaknesses. If using them requires an unreasonably large number of resources or highly specialized knowledge, then with a high probability, most attackers will not be able to use them. The specific sequence of vulnerability applications can be represented as a tree (Fig. 7).

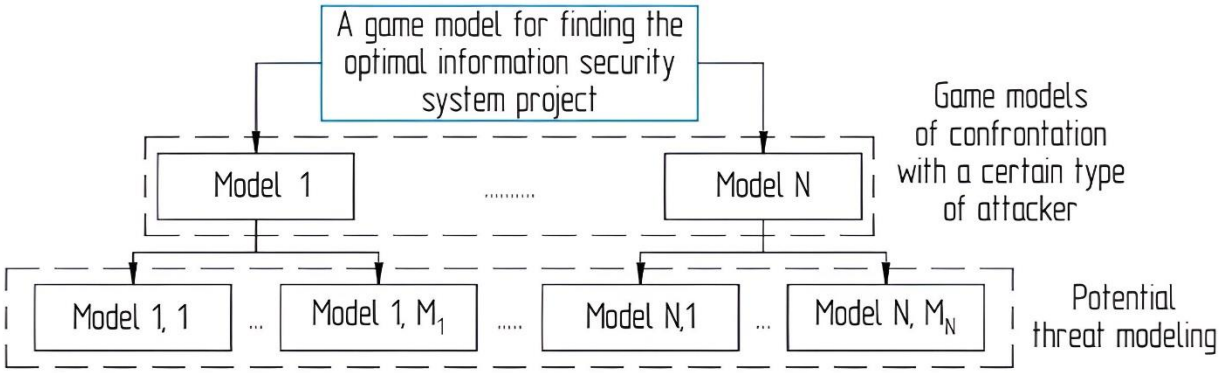

Fig. 6: Hierarchical scheme of the organization of model relationships

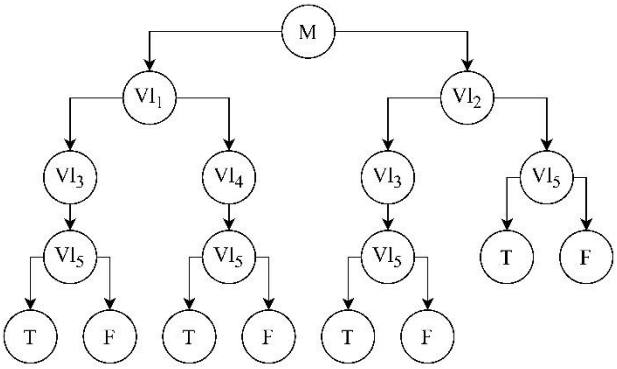

Fig. 7: Threat implementation in a tree form

The tree presented in Fig. 7 depicts the G-threat implementation process overcoming a data protection system containing five vulnerabilities ($Vl_1 \ldots Vl_5$). The G-threat implementation tree shows only the paths that could lead to threat creation. It does not estimate IPS optimality indicators such as the average time to implement a threat or the probability of a threat being implemented within a given time.

Developing an Integrated Software Architecture

The above models can be applied in practice, but this will require developing software with the following functionalities:

1) Organization of effective interaction with the user through a dedicated graphical interface
2) Processing and storage of design decisions related to the development of data protection systems
3) Ability to simulate and assess the results of the system operation
4) The selection of the most efficient and rational design solution

The reflection of the architecture of a complex software tool is the game model, the type of attacker, and the specific design solution. It is worth understanding that forming the graph of potential risks is because the ordinary user cannot encounter problems during the operation of the software tool.

When working with the graph, the number of objects requiring control decreases significantly. Interestingly, it is possible to automatically build an implementation tree of a potentially adverse scenario for a particular type of attacker. The class in any case in this context can be represented as follows:

$$Class = \{name, properties, methods\}$$

where "*name*" is a "pointer" to a particular class; "*properties*" is a set of characteristics of class objects; and "*methods*" are functions specific to all class elements.

IPS Design Solution

If we consider the IPS design solution in more detail, we need to understand that it inherently involves the parameters of a particular solution. Moreover, it covers an enormous number of various factors, not only cost, risks, and requirements. The design solution acts as an aggregate, which has the following form:

$$\{Project, \{M\}, \{F\}\}$$

To describe a set of attacker types, it is necessary to use the following expression:

$$Cr = \{Cr_1 Cr_2, \ldots Cr_n\}$$

$$\{F\} = \{F_{risk}, \{F_1\}\}$$

where, F_{risk} characterizes the aggregate calculated risk and F_1 is the interaction tool between the class and interface.

Discussion

This study examined three IPS models, demonstrating variants of events under the condition that the IPS and the intruder come into contact. A game model that considers attackers of all types analyzed these three models.

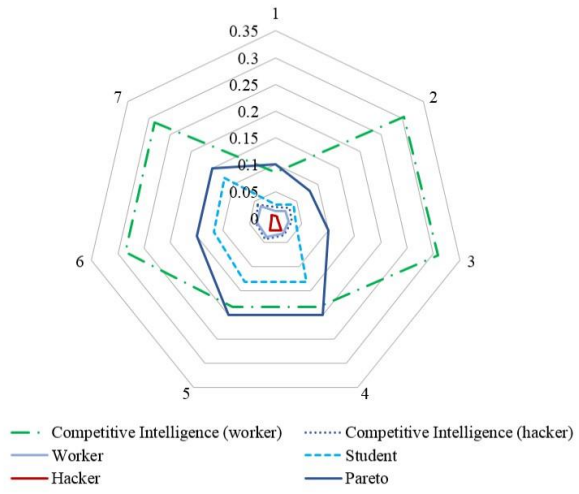

Fig. 8: Diagram of compliance with pareto demands of IPS project oriented against outsider attackers

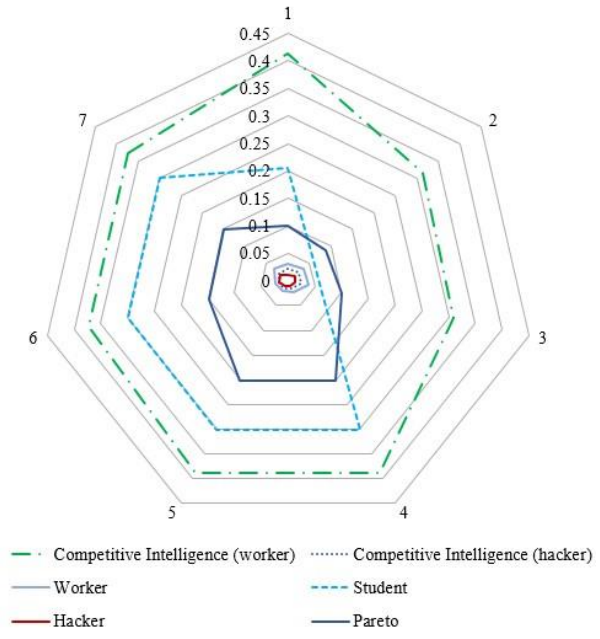

Fig. 9: Diagram of compliance with Pareto demands of IPS project oriented against insider attackers

The first of the considered IPS projects assumed that the primary efforts focus on leveling outsider threats. The diagram in Fig. 8 shows that the modeling results of this project with its focus do not meet the Pareto demands. In particular, this applies to the situation where the attacker is a hacker hired by competitors.

The second IPS project countered insider attackers. The diagram in Fig. 9 shows that in this case, the resulting data also do not meet the Pareto demands, including when the hacker represents the interests of competitors.

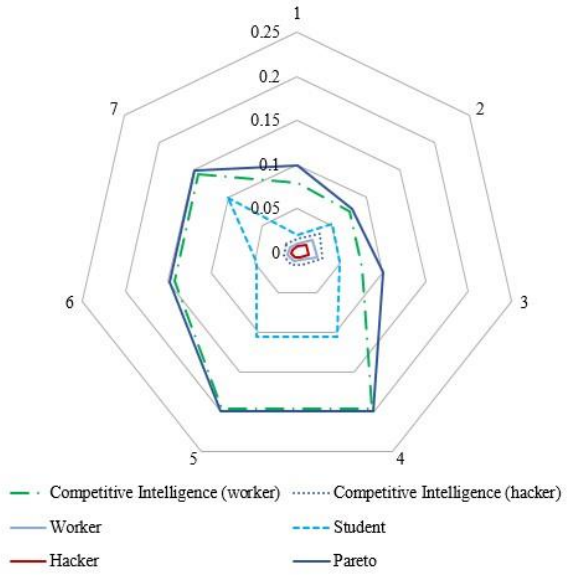

Fig. 10: Diagram of compliance with Pareto demands of the balanced IPS project

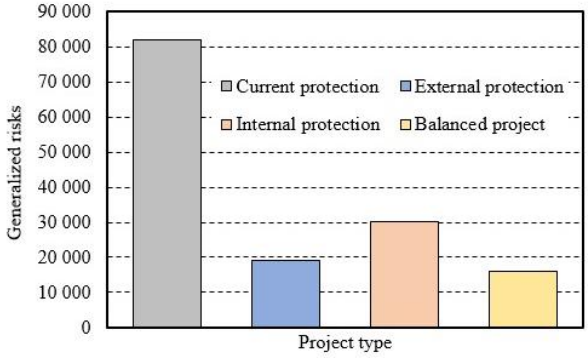

Fig. 11: Comparison diagram of generalized risks

The third IPS project was the balanced IPS project. Figure 10 shows a diagram that makes it possible to trace how the obtained results for this project meet the Pareto demands.

Figure 11 shows a comparison diagram of generalized risks for all projects.

Based on the simulation results, given these diagrams, we can conclude that only a balanced IPS project meets the Pareto demands. The projects focused on countering only external or internal threats do not meet these demands. The balanced IPS project has minimal generalized risk and compared to the existing protection system, there is a 5-fold reduction.

Conclusion

The main conclusions of this study. The main result of the work carried out is the developed set of models for

determining the optimal design of the information security system, in particular, the following tasks were solved:

1. A model for the implementation of a threat in an information system in the form of a semi-Markov process has been developed, taking into account the presence of vulnerabilities in information security systems and the relationships between them. The semi-Markov model allows you to calculate the time and the probability of a threat being realized by an attacker
2. A game model has been developed for choosing the optimal design of an information security system in terms of the time and the probability of a threat, the cost of the project, and the magnitude of the generalized risk associated with threats
3. Algorithms for modeling the processes of threat implementation and searching for the optimal design of an information security system have been developed
4. The architecture of the software package that implements the described models and algorithms has been developed
5. A modeling technique has been developed, focused on the use of the proposed models

Strengths and limitations of results. Several studies (Ghiasi *et al*., 2023; Zhang *et al*., 2020) have studied generalized IPS models, but the main drawback of generalized models is the very poor elaboration of their formal aspects. A characteristic feature is that this problem is very complex and nontrivial and its solution requires a lot of time and resources, which significantly complicates the practical use of such models. To overcome these shortcomings, this study proposes a resource model described as a heterogeneous semantic network. Mathematical formalization begins with Eq. (1) and diagrams and then a matrix of relationships between information system resources and threats is presented. The strength of the semantic web approach is the ability to take into account the increase in source schema with updated data.

Recommendation for use and future direction of work. The use of the developed models makes it possible to increase the efficiency of the created information protection systems at the stage of their design. The results of using the information security threat implementation model can be used to assess existing information security, including the information security audit of information systems to obtain probabilistic values of threats and information risks.

The effectiveness of the proposed approaches is proved by the fact that according to the simulation results, it was found that only a balanced design of the information security system satisfies the Pareto requirements. Projects focused on countering only external or internal threats do not meet these requirements. A balanced information security design has minimal overall risk. Thus, the main results and provisions of the study can be applied in the development of projects for improving secure information systems to select the most optimal design for an information security system.

Acknowledgment

The authors declare no conflicts of interest. The results presented in this study were obtained under the grant agreement dated April 20, 2022, No. 075-15-2022-307.

Funding Information

The results of this study were obtained under the grant agreement in the form of subsidies from the Federal Budget of the Russian Federation for state support for the establishment and development of world-class scientific centers performing R and D on scientific and technological development priorities dated April 20, 2022, No. 075-15-2022-307.

Author's Contributions

Islam Alexandrovich Alexandrov: Carried out validation and visualization, prepared the manuscript drafted and contributed to formal analysis.

Andrey Victorovich Kirichek: Conducted formal analysis and investigation and prepared the manuscript drafted.

Vladimir Zhanovich Kuklin: Responsible for conceptualization, reviewed and edited of the manuscript drafted, supervised and administering the project.

Alexander Nikolaevich Muranov: Prepared the manuscript drafted and contributed to conceptualization and methodology.

Leonid Mikhajlovich Chervyakov: Is in charge of the methodology, software, visualization and resources.

Ethics

This article is an original research work. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved.

Conflicts of Interest

The authors declare no conflicts of interest as there are no financial, personal, or other ties that may influence or may be perceived as affecting their work.

References

Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assessment of potential security threats and introducing novel data security model in cloud environment. *Materials Today: Proceedings*, *62*, 4909-4915. https://doi.org/10.1016/j.matpr.2022.03.536

Akkad, A., Wills, G., & Rezazadeh, A. (2023). An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. *Computers and Electrical Engineering*, *105*, 108491. https://doi.org/10.1016/j.compeleceng.2022.108491

Alexandrov, I., Tatarkanov, A., Kuklin, V., & Mikhailov, M. (2022). Development of algorithm for calculating data packet transmission delay in software-defined networks. *Emerging Science Journal*, *6*(5), 1062-1074. https://doi.org/10.28991/ESJ-2022-06-05-010

D'Amico, G., & Petroni, F. (2023). ROCOF of higher order for semi-Markov processes. *Applied Mathematics and Computation*, *441*, 127719. https://doi.org/10.1016/j.amc.2022.127719

El Alaoui, I., & Gahi, Y. (2020). Network security strategies in big data context. *Procedia Computer Science*, *175*, 730-736. https://doi.org/10.1016/j.procs.2020.07.108

Dhulipala, S. L., & Flint, M. M. (2020). Series of semi-Markov processes to model infrastructure resilience under multihazards. *Reliability Engineering & System Safety*, *193*, 106659. https://doi.org/10.1016/j.ress.2019.106659

Egoshin, N. S., Konev, A. A., & Shelupanov, A. A. (2020). A model of threats to the confidentiality of information processed in cyberspace based on the information flows model. *Symmetry*, *12*(11), 1840. https://doi.org/10.3390/sym12111840

Friha, O., Ferrag, M. A., Benbouzid, M., Berghout, T., Kantarci, B., & Choo, K. K. R. (2023). 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. *Computers & Security*, *127*, 103097. https://doi.org/10.1016/j.cose.2023.103097

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975. https://doi.org/10.1016/j.epsr.2022.108975

Gontarczyk, A., McMillan, P., & Pavlovski, C. (2015). Blueprint for Cyber Security Zone Modeling. *Information Technology in Industry*, *3*(2). https://doi.org/10.17762/itii.v3i2.28

Gupta, V., & Dharmaraja, S. (2011). Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks. *Reliability Engineering & System Safety*, *96*(12), 1627-1636. https://doi.org/10.1016/j.ress.2011.08.003

Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, *137*, 103611. https://doi.org/10.1016/j.compind.2022.103611

Khalil, S. M., Bahsi, H., Ochieng'Dola, H., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems-A Case Study of a Microgrid System. *Computers & Security*, *124*, 102950. https://doi.org/10.1016/j.cose.2022.102950

Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. (2022). Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *Cryptography*, *6*(3), 44. https://doi.org/10.3390/cryptography6030044

Kuklin, V., Alexandrov, I., Polezhaev, D., & Tatarkanov, A. (2022). Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *6*(3), 44; https://doi.org/10.11591/eei.v12i3.4840

Kuklin, V., Alexandrov, I., Polezhaev, D., & Tatarkanov, A. (2023). Prospects for developing digital telecommunication complexes for storing and analyzing media data. *Bulletin of Electrical Engineering and Informatics*, *12*(3), 1536-1549. https://doi.org/10.11591/eei.v12i3.4840

Logrippo, L. (2021). Multi-level models for data security in networks and in the Internet of things. *Journal of Information Security and Applications*, *58*, 102778. https://doi.org/10.1016/j.jisa.2021.102778

Louk, M. H. L., & Tama, B. A. (2023). Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system. *Expert Systems with Applications*, *213*, 119030. https://doi.org/10.1016/j.eswa.2022.119030

Mazzoccoli, A., & Naldi, M. (2022). An Overview of Security Breach Probability Models. *Risks*, *10*(11), 220. https://doi.org/10.3390/risks10110220

Oleinik, A., Kapitanov, A., Alexandrov, I., & Tatarkanov, A. (2020). Calculation methodology for geometrical characteristics of the forming tool for rib cold rolling. *Journal of Applied Engineering Science*, *18*(2), 292-300. https://doi.org/10.5937/jaes18-25211

Párizs, R. D., Török, D., Ageyeva, T., & Kovács, J. G. (2022). Machine learning in injection molding: An industry 4.0 method of quality prediction. *Sensors*, *22*(7), 2704. https://doi.org/10.3390/s22072704

Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management*, *38*(1), 187-195. https://doi.org/10.1016/j.ijinfomgt.2017.07.008

Stratton, C., & Carter, D. (2023). Locating information systems in the freedom of information process. *Government Information Quarterly*, *40*(2), 101807. https://doi.org/10.1016/j.giq.2023.101807

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security*, *110*, 102450. https://doi.org/10.1016/j.cose.2021.102450

Zhang, B., Chang, X., & Li, J. (2020). A generalized information security model SOCMD for CMD systems. *Chinese Journal of Electronics*, *29*(3), 417-426. https://doi.org/10.1049/cje.2020.02.017