Developing the Comprehensive Technology for Alternative Management of Complex Organizational and Technological Objects in the Conditions of Cyber Threats

Tatiana Prokopenko[1], Yaroslav Tarasenko[1], Olha Lavdanska[1], Serhii Rudnytskyi[1], and Yuliia Rudnytska[1]

[1] *Cherkasy State Technological University, Shevchenko ave., 460, Cherkassy, 18006, Ukraine*

Abstract

It was suggested the comprehensive technology for alternative management of complex organizational and technological objects basing on combined application of grapho-analytical methods and the steganographic protection method of the classified proprietary data from the threats of insider attacks This will provide increasing the efficiency of management through avoiding the risk of leaking classified proprietary information. Within this technology it was developed a simulation model of the system for alternative management of complex organizational and technological objects based on the mathematical apparatus of Petri nets. This allows to determine the development scenario for the object of management and to predict the dynamics of achieving strategic goals, the dynamics of processes' carrying out, the dynamics of the risky events impact. The steganographic method of classified proprietary data protection from threats of insider attacks in the system was also proposed. The developed comprehensive technology for management of complex organizational and technological objects in the conditions of cyber threats provides opportunities to present the strategy of the future and its consequences with full data protection from leakage. The technology also provides information protection from unauthorized access, detecting the fact of aggressive interference in the data and counteracting the information leakage possibility. In addition, along with improving the efficiency of identifying the insider, it is given a possibility to assess the impact of the actions and to use different options for achieving different system's goals. This technology can be used for software development in intelligent control systems of technological complexes of continuous type, including enterprises and corporations of food, chemical industry, as well as in projects.

Keywords

Comprehensive technology, alternative management, organizational and technological objects, steganographic method of data protection.

1. Introduction

New technologies are required in a fierce competitive difficult environment of such organizational and technological facilities management as enterprises and technological complexes, corporations in various industries, as well as projects. Such technologies should provide the opportunity of maximizing the objective information about the current situation, with the possibility of taking into account possible threats, and with prompt assessment and predicting the future efficiency. Therefore, the use of a comprehensive information technology which combines models, methods and ways of making decisions that take into account the operation peculiarities of the management facility will be actual. In addition, it will ensure the processing and obtaining of qualitative and quantitative information with maximum data protection.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: t.prokopenko@chdtu.edu.ua (T. Prokopenko); yaroslav.tarasenko93@gmail.com (Y. Tarasenko); yegorovaov@gmail.com (O. Lavdanska); s.v.runitskiy@gmail.com (S. Rudnytskyi); y.v.rudnitskaya@gmail.com (Y. Rudnytska)
ORCID: 0000-0002-6204-0708 (T. Prokopenko); 0000-0002-5902-8628 (Y. Tarasenko); 0000-0001-5571-2281 (O. Lavdanska); 0000-0003-4389-1088 (S. Rudnytskyi); 0000-0001-6384-0523 (Y. Rudnytska)

The use of information technology in the strategic management of complex organizational and technological objects, in particular automated strategy building, is accompanied by cyber threats. Any intentional change in the input data can cause the threat of obtaining an incorrect prediction and, consequently, to significant losses. In addition, obtaining the final strategy by third parties, including competitors, may lead to the risk of significant financial and reputational damage. Such kind of risks can be caused by insiders. There are other technical risks, such as the possibility of the system failure or the possibility of the errors occurrence in data analysis, etc. Such risks are relatively easy to track and, accordingly, reduce the negative effect of their occurrence. However, insider attacks such as industrial espionage, stealing important commercial information as well as sabotage, committed by making changes to the input data are much more difficult to detect and localize. At the same time, the report for 2019 by Fortinet Corporation on the threat of insiders was considered [1]. It was found that the most serious information security threats are not related to malefactors' aggressive actions or the use of malicious software, but are directly caused by the insiders' actions. This makes sense, since the measures implemented by the company security department (CSD) can effectively prevent most of these threats except the insider attacks.

This substantiates the relevance of the research.

2. Review of the Literature and Problem Statement

In [2] it was studied such features of modern organizational and technological objects (OTO), as multidimensionality, complexity of the structure, the presence and change of many goals, activity, the need to ensure minimal losses of the target product with severe restrictions of energy carriers, non-stationary processes, indeterminacy, close relationship of organizational and technological processes. Therefore, taking into account the management comprehensiveness of such facilities, it is important to select and make adequate management decisions, both operational and strategic, which will provide a long-term development strategy with the ability of information protection. At the same time, it is obligatory to take into account the risks directly related to industrial espionage, theft of important commercial information, as well as potential crisis conditions.

Researching the basic measures to fight against insider attacks with the help of computer systems becomes of great importance. Thus, the most common 4 categories of information systems for data proceeding are described in [3]. Approaches are based on the use of statistical analysis for anomaly detection, contextual information derivation for network intelligence, specific threat detection use cases and the use of meta learning. At the same time, according to the [4], the most common system of counteracting insider attacks is the data loss prevention (DLP) system, based on the approaches of meta learning use. However, such information systems for counteracting the risks of insider attacks use have a number of disadvantages. It was found that DLP systems and similar to them, which belong to the aforementioned categories, counteract only active users' actions that are made to cause harm. In addition, they can help in detection of only the information leakage channels through the enterprise networks. At the same time, some threats remain unaccounted. Firstly, it is entering the knowingly false information that in a particular case in using the information system of managing the complex organizational and technological objects may lead to the risk of forming an incorrect prediction. Secondly, it is an intentional change of the already entered data or forming strategies and transferring it to the third parties without use of the enterprise's equipment and networks. It is offered to solve such defects by the help of the integrated in system module for information steganographic protection taking into account the system's specificity of managing the complex organizational and technological objects. This will allow, in contrast to similar systems to counter insider attacks. There will be an opportunity not only to detect the fact of aggressive intervention and to fight the attack's consequences after its performance, but, above all, to counter the possibility of information theft itself. In addition, it will be received an opportunity to increase the effectiveness of identifying the person who directly carried out the insider attack, which is quite difficult to make using existing tools.

Thus, today the Balanced Scorecard Concept (BSC) is often used to develop a long-term strategy [5]. According to the strategy, one can juxtapose the company's corresponding task and the employee who performs it. It can be assumed the presence of an inverse relationship between the employee and his task. Thus, with the help of specially designed steganographic protocol it is possible to identify a particular employee who performed this or that task of interaction with the system at a certain stage of the information system life cycle, which will ultimately help to identify an insider himself.

In [6] the authors proposed a method of strategic decision-making in management of technological complexes of continuous type in various industries (food, chemical, oil refining). However, the possibilities of data protection from insider attacks are not considered [7].

Therefore, at the present stage of information technology development in the management of complex organizational and technological objects, it is raised a critical problem of developing the comprehensive technology that would provide comprehensive information capabilities. Namely, to perform the functions of current information collection, processing and analysis, to present a wide range of opportunities for protecting the operational and strategic data, as well as for defining rational trajectories in crisis conditions under rapidly changing circumstances.

3. The Aim and the Objectives of the Research

The aim of the work is developing a comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats on the basis of combined application of grapho-analytical methods and the steganographic protection method of the proprietary data from insider attacks.

For achieving the aim, the following main tasks have been set:

- to build a simulation model of the system for alternative management of complex organizational and technological objects based on the mathematical apparatus of Petri nets;
- to substantiate and to investigate the steganographic method of classified proprietary data protection from threats of insider attacks in the system for alternative management of complex organizational and technological objects.

4. Methods for Researching the Alternative Management of Complex Organizational and Technological Objects in Cyber Threat Conditions

Alternative management of complex organizational and technological objects is based on integrating the tasks of strategic and operational management [6], which are considered in two aspects: using methods of building static models and dynamic models based on them. At the same time, alternative management involves implementing a set of targeted actions in a certain sequence, which are characterized by the efficiency indicators, with the availability of alternative options for the situation's development. Static models are being built through a scenario-target approach [7], based on the mathematical apparatus of Petri nets, and cognitive maps [8], which makes it possible to investigate the influence of one factors on another. Dynamic models allow analyzing scenarios of situations' development in time. The combination of static and dynamic models provides opportunities to fully develop and analyze alternatives of management decisions, which is important for the decision-making person (DMP). And this contributes to the development of appropriate databases and knowledge bases.

The system for alternative management of organizational and technological objects is a complex polysystem that includes a subsystem of strategic management as part of the organizational component, which is influenced by the technological processes operational activities subsystem performance. This system should provide the effectiveness assessment for implementation of this or that alternative strategy on the basis of balanced performance indicators. Indicators should reflect the strategic and operational activities in a comprehensive interaction, identifying and analyzing approaches to strategies' transformation and the movement of material, information, energy flows. The strategy's implementation is carried out under the influence of probable negative events and changes in the environment and circumstances. That is why it is necessary to investigate the impact on each alternative of probable risk events and predict the expected strategy's effectiveness. In addition, it is necessary to compare it with the planned one, taking into account the changes arising from the occurrence of probable risk due to competition factors, political, social, economic, market factors and emerging innovations.

Usually, formalized methods are based on the principles of systems analysis, computational intelligence, and the theory of object-oriented programming. It is quite difficult to implement the problem's solution of building a system's simulation model for the alternative management of complex organizational and technological objects in the conditions of cyber threats by applying these methods. Therefore, to improve the confidence in modelling and to ensure the model's flexibility, it is advisable to use different methods. The comprehensive combination of traditional formalized methods with such methods as methods of hierarchies' analysis, methods of actions' sequence logical control, cognitive analysis, contributes to meeting these objectives.

The effectiveness of simulating the process of building scenarios' alternative versions to achieve the set goals in cyber threats conditions depends on a clearly defined goals' hierarchy, where the list of goals should be quite complete. Goals usually consist of goal components (sub-goals) and are represented by the graphs' type such as tree [9]. The goal scenario will be defined as a set of processes being run in a given order. The execution order allows for a variety of inter-process communication: parallel processes' execution along with sequential execution as well as synchronization, alternatives, etc. Transitions between processes are initiated by events, the occurrence of which is characterized by the transmission of information messages about possible threats.

A balanced system of indicators [5] is used to determine the process's inverse dependence of the alternative management of organizational and technological objects and the corresponding executor of this process. The protection system is based on the steganographic protocol of embedding digital watermarks (DW), which implementation is carried out through the main approaches of the method for embedding two-level digital watermarks [10]. Watermark concealment is based on the semantic methods of computer linguistic steganography. At the same time, through the role-based model of operators' distributed access to the system, the risk of entering knowingly false information is reduced and the probability of malefactor's detection is increased. The effectiveness prediction of risk consideration measures implementation was carried out on the basis of a two-component calculation by using a process-statistical approach [11].

5. The Research Results of Comprehensive Technology for Management of Complex Organizational and Technological Objects in the Conditions of Cyber Threats

The basis of the simulation model of the system for alternative management of complex organizational and technological objects is the goal scenario, which is being built on the basis of Petri nets. The goal scenario is presented in the form of a processes' graph [6], which reflects the relationship between goals, processes, transitions, taking into account the risk of insider attacks.

The goal scenario for functioning of the system for alternative management of organizational and technological objects will be presented as follows:

$$Q = \langle F, C, O, T, R, S \rangle, \tag{1}$$

where $F=\{f_i\}$, $i=1,\dots n$ - a set of management processes of organizational and technological objects, $C=\{c_i\}$, $i=1,\dots,m$ - a set of goals (main and additional), $O=\{o_i\}$, $i=1,\dots,e$ - a set of objects, $T=\{t_i\}$, $i=1,\dots,k$ – a set of transitions, $\Theta = \{0,1,\dots, h\}$ - a set of ordered time moments (time scale), $R=\{r_i\}$, $i=1,\dots,l$ - a set of resources, $S=\{s_i\}$, $i=1,\dots,h$ - a set of events.

To form the goal scenario of the system for alternative management of the organizational and technological object, the goals are presented in the table 1, the processes in the table 2.

Table 1
Table of goals

Designation	The essence of the goal
c_0	To increase the profits
c_1	To increase the revenue
c_2	To increase the production volume
c_3	To increase the order volume
c_4	To supply the market demand maximally

c_5	To choose the best strategy of production technology
c_6	To achieve the maximum volume of final products
c_7	To reduce the losses in production
c_8	To increase the enterprise profitability
c_9	To increase the technical level of production
c_{10}	To predict the production process at interval τ under different strategies
c_{11}	To form a matrix of parameters' mutual influence for each production strategy
c_{12}	To set the initial values for the criteria at the time interval τ of the production process

Table 2
Table of processes

Designation	The essence of the operation
f_1	Evaluating the effectiveness of the organizational and technological objects functioning in the conditions of cyber threats
f_2	Defining different production strategies on a time interval τ
f_3	The strategy of productivity maximizing while maintaining allowable losses and expenditures of resources (at interval τ)
f_4	The strategy of losses minimizing in production by introduction of new technologies during maintaining productivity (at interval τ)
f_5	The strategy of expenditures minimizing by increasing production capacity (at interval τ)
f_6	Formation of orders for products (at interval τ)
f_7	Production
f_8	Sale (marketing) of products

The goal scenario is presented in Fig. 1 as a processes' graph, where the processes are represented by rectangles, transitions by bold vertical lines, the processes' goals are shown by vertical arrows connected with the upper side of the rectangle. Resources that are consumed are presented in table 3, objects that are transferred are presented in table 4, and the list of events in table 5.

Table 3
Table of resources

Designation	The name of costs
r_1	Costs of production
r_2	Costs of predicting and strategy selection
r_3	Costs of improving production technology
r_4	Costs of forming orders

Table 4
Table of objects

Designation	The essence of objects
o_1	Data for predicting the production strategy
o_2	Description of the productivity maximizing strategy while maintaining allowable losses and expenditures of resources
o_3	Description of the losses minimizing strategy in production by introduction of new technologies during maintaining productivity
o_4	Description of the expenditures minimizing strategy by increasing production capacity
o_5	Documentation for products which in needed by the market
o_6	The orders' "portfolio"
o_7	Production report
o_8	Product sales report

Table 5
Table of events

Designation	The essence of the event
s_1	To transfer o_1 from f_1 to f_2 at the time τ_1
s_2	To transfer o_2 from f_2 to f_6 at the time τ_2
s_3	To transfer o_3 from f_2 to f_3 at the time τ_3
s_4	To transfer o_4 from f_2 to f_4 at the time τ_4
s_5	To transfer o_4 from f_2 to f_5 at the time τ_4
s_6	To transfer o_5 from f_3 to f_6 at the time τ_5
s_7	To transfer o_6 from f_4 to f_6 at the time τ_6
s_8	To transfer o_5 from f_5 to f_6 at the time τ_6
s_9	To transfer o_7 from f_6 to f_7 at the time τ_7
s_{10}	To transfer o_8 from f_7 to f_8 at the time τ_8

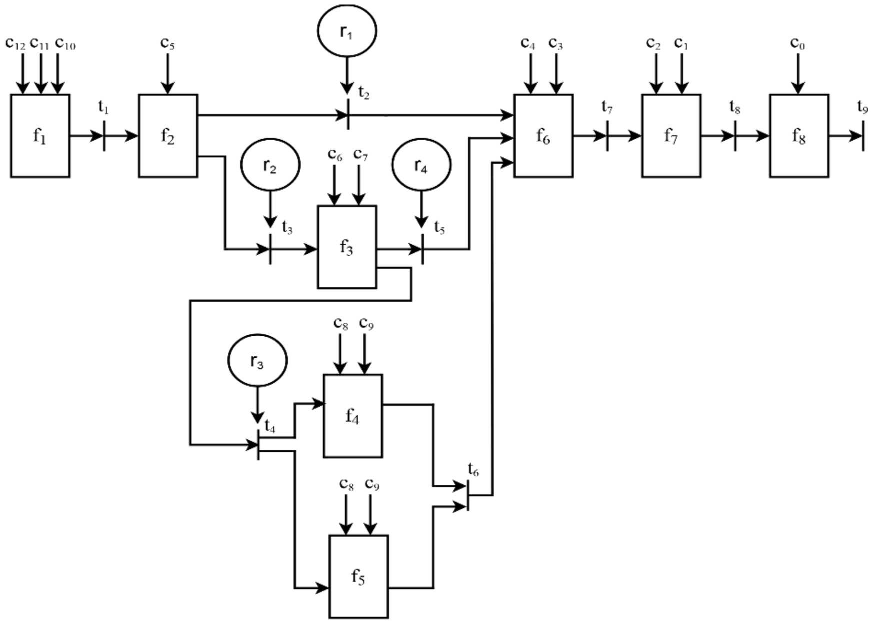

Figure 1: The processes' graph of the goal scenario in the conditions of cyber threats

The simulation model of the system for alternative management of complex OTO works as follows. The basis of the processes' graph is a Petri net [7]. The actions' execution is modeled by finding the mark in the appropriate position. The transition is activated if a mark is at all of its input positions. When transitioning, marks are removed from the input positions, and are added to the output positions. The event s_i is defined as the fact of transferring the object o_i from the input process f_{in} to the output f_{out} at the time τ of triggering transition *t*. When implementing processes, resources r_i are consumed. It is assumed that any event s_i occurs only at the clock moments that correspond to the transitions in the processes' graph. The discrete simulation model is quite simple and is comfortable to perceive. However, in real conditions of alternative management of complex OTO, events can occur within the intervals between the specified clock moments. There is a possibility of events' displacement in time and transition to the next clock moment in a discrete model, which is a limitation of this model.

The steganographic method of classified proprietary data protection from threats of insider attacks in the system for alternative management of complex organizational and technological objects is used at the time of transition activating. To increase the security level of the system for alternative management of complex OTO in general and to reduce the risk of the entire data set modification at the stage of entering data to the system, the distribution of operators' roles is performed (Fig. 2).

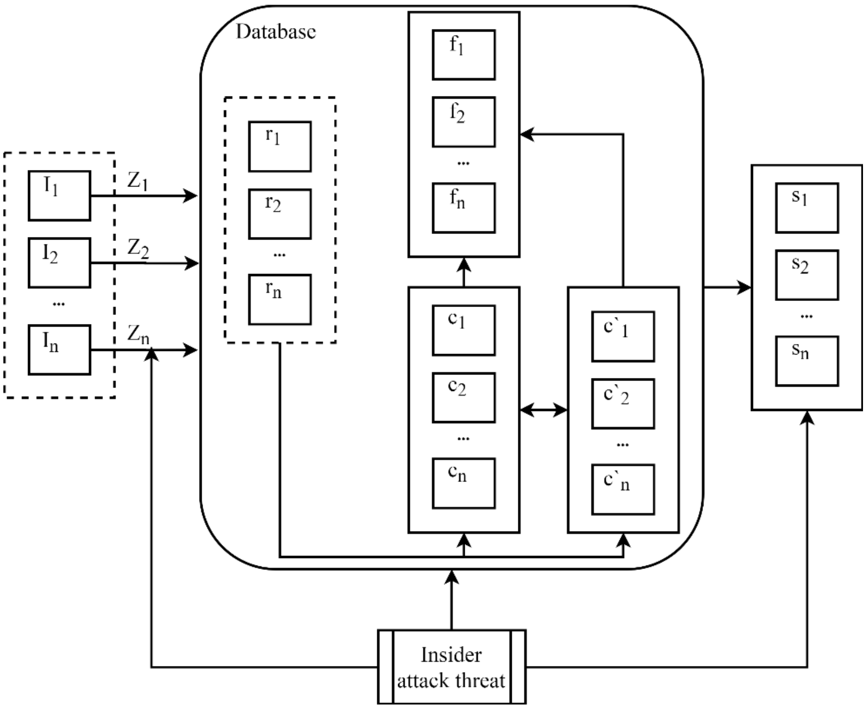

Figure 2: The general operation principle of the system for the enterprise strategy automated construction with distributed operators' roles and indicated threats of insider attacks

In this case, I is the set of input data that are required for the system's work and are entered by the operator Z, the number of which corresponds to the number of roles. The dotted line shows the blocks in which the information is variable. The input information is entered into the database, where it affects the set of resources r, which, in turn, affects the choice of this or that main goal c, or an additional goal c`. The goal determines the required process f. Processes, main and additional goals relate to the system's built-in data, and only the process of choosing them affects the definition of the event s, which is the result of the system's work.

Based on insider attack threat statistics [1], precisely databases as well as file servers are the most vulnerable to attack (56% and 54% respectively). Endpoints are number three in vulnerability rate (51That is why it was decided to protect, first of all, the information in the database and the end result, as shown in Fig. 2. In addition, there is a probability of not only theft, but also of data modification at the stage of entering information by the operator, and therefore there are risks not only for the database or for the final result, but also for data transferring.

Steganographic information protection methods are applied to reduce the risk of insider attacks by using a computer program and to increase the efficiency of DLP systems. The general operation principle of the system for the enterprise strategy automated construction at comprehensive use of the protection module will look different (Fig. 3).

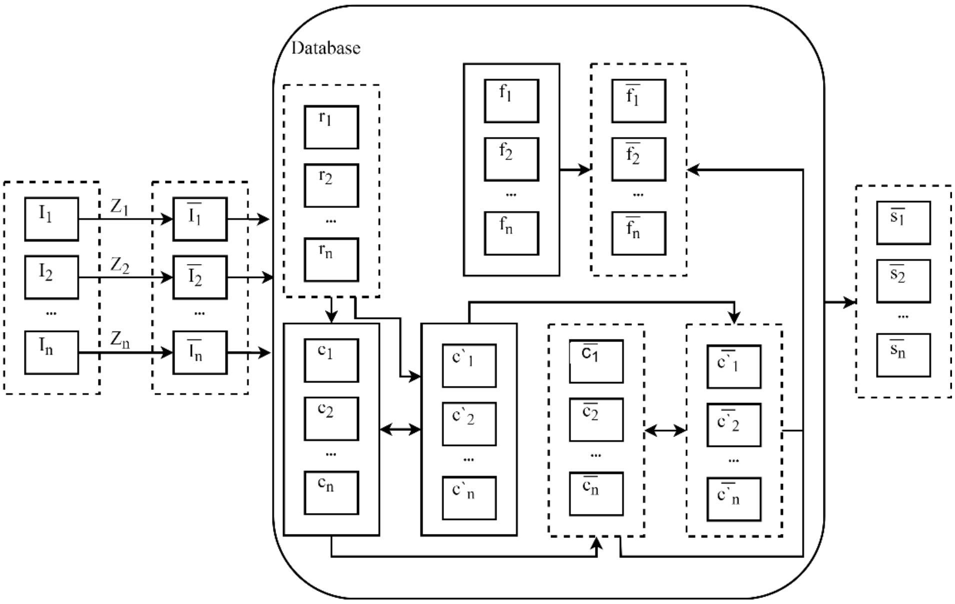

Figure 3: The general operation principle of the system for considering insider attacks

Thus, the information I after entering by the operator Z is modified using a steganographic key by the formula:

$$\bar{I} = \sum_{i=1}^{n} \log_{(N_Z+1)\cdot K_{mod}}(p_i) + p_i, \qquad (2)$$

where N_z – the number of system's operator who enters the data, K_{mod} – public steganographic key, p_i – the parameter of input data in numerical form. Under conditions that $p_i \neq N_{z+1}$, $I \neq 0$, $I \neq 1$, $I \neq 2$. Thus, the database receives modified information with marking of particular operator, which can be restored, if necessary, by the head of the enterprise, or by any authorized person who has a valid key. As a result of this, it is simultaneously provided a process for misinforming an insider who will try to possess information from the database, as well as increased the accuracy of identifying a user who might be an insider and has entered knowingly false data. Of course, it is difficult to counter the risks of insider attacks due to the possibility of obtaining other people's account by the malefactor. However, the identification of a person who has gained access to this or that account belongs to the area of CSD responsibility, in turn, the system's task is to identify the particular user who entered the wrong data into the system. In addition, the system records users' actions, but the described risks do not exclude the possibility of gaining access to the user's actions log and the deletion of traces by an insider. However, it is impossible to counteract modifying of the entered data by the probable insider taking into account the information on the user, because all subsequent system's actions will be carried out with these data.

Modified initial data lead to the emergence of alternative main $\bar{c}$ and additional $\bar{c}'$ goals. At the same time, it is carried out steganographic encryption of the processes *f*, which lead to the emergence of alternative processes $\bar{f}$, the choice of which is influenced by alternative main and additional goals. Based on semantic substitution, modification of processes is carried out through the alternative action, which is determined according to the changed data.

As a result of such modifications, alternative events $\bar{s}$ will be formulated. The main task of these events is misinforming the malefactors, who is trying to get the strategy's final result through insiders. But in case of gaining the access to a stolen strategy, it is possible to identify the particular employee who entered the information or formulated the strategy.

Under these conditions, the development of a steganographic protocol is carried out in order to solve the problem of taking into account the risks of insider attacks. Due to the presence of two encryption stages (input data and available data) the best choice is to use the method of embedding of two-level digital watermarks [10]. However, the proposed key distribution protocol differs from that described in [10] and is as follows:

$$\begin{aligned} &z \rightarrow B: \{I\}K_{mod} \\ &B \rightarrow z: K_t \qquad , \\ &z \rightarrow B: \{\bar{I}\}K_t \end{aligned} \tag{3}$$

where K_{mod} is the public key for encrypting the input information I, B is the risk accounting module, z is the operator who entered the data or formed the final prediction, $\bar{I}$ – is modified input data containing the information on the operator and necessary for embedding his digital watermark into the stego-container of the processes f using a secret key K_t.

In this case, the general scheme of embedding a digital watermark and key distribution is shown in Fig. 4.

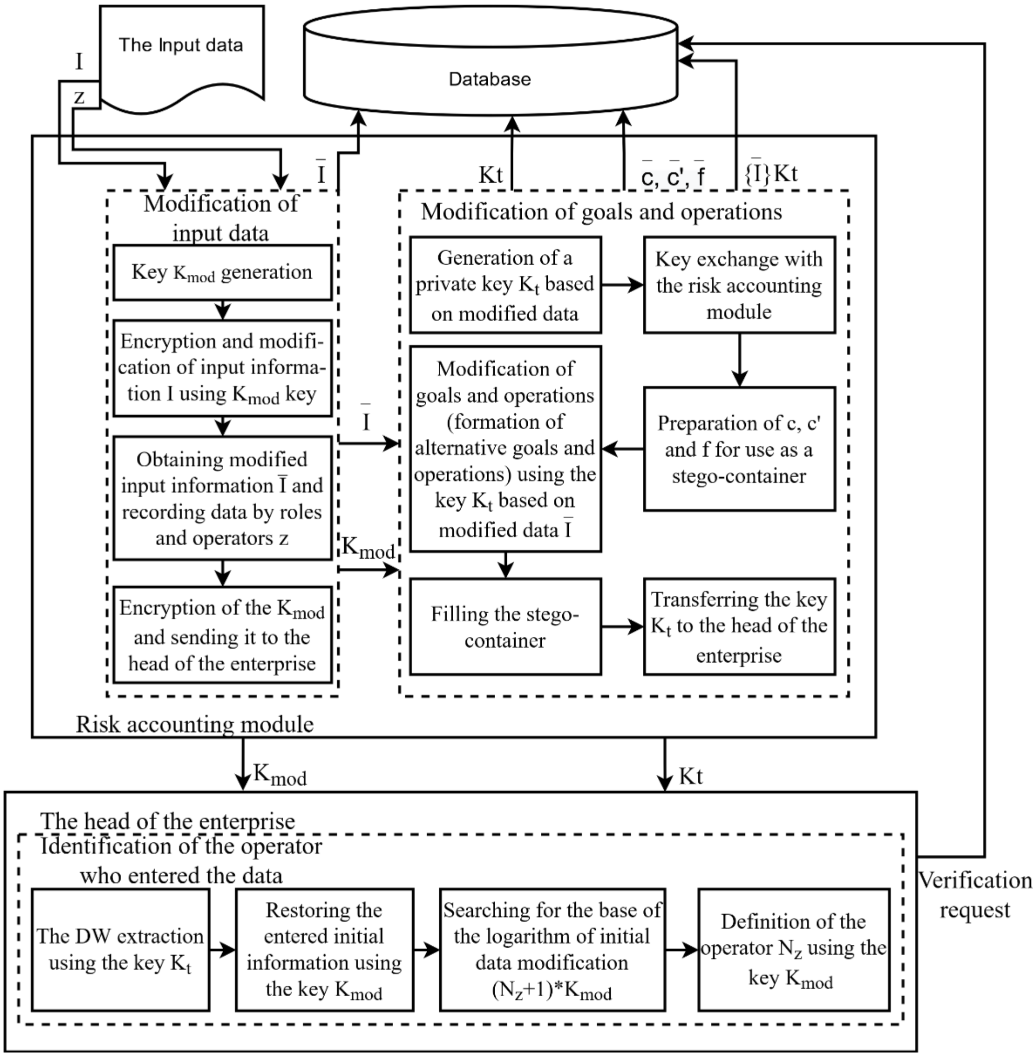
The Input data
Database
I
z
$\bar{I}$
Kt
$\bar{c}$, $\bar{c}'$, $\bar{f}$
$\{\bar{I}\}$Kt
Modification of input data
Key K_{mod} generation
Encryption and modification of input information I using K_{mod} key
Obtaining modified input information $\bar{I}$ and recording data by roles and operators z
Encryption of the K_{mod} and sending it to the head of the enterprise
$\bar{I}$
K_{mod}
Modification of goals and operations
Generation of a private key K_t based on modified data
Key exchange with the risk accounting module
Modification of goals and operations (formation of alternative goals and operations) using the key K_t based on modified data $\bar{I}$
Preparation of c, c' and f for use as a stego-container
Filling the stego-container
Transferring the key K_t to the head of the enterprise
Risk accounting module
K_{mod}
Kt
The head of the enterprise
Identification of the operator who entered the data
The DW extraction using the key K_t
Restoring the entered initial information using the key K_{mod}
Searching for the base of the logarithm of initial data modification $(N_z+1)*K_{mod}$
Definition of the operator N_z using the key K_{mod}
Verification request

Figure 4: The general scheme of embedding a digital watermark and key distribution

For embedding a two-level DW, it is necessary to follow the steps:

1. The system of input data modification receives input data I and information on the operator z.
2. The system generates a public encryption key K_{mod}.
3. It is performed a comparison between the modified data and the operator as well as his role and it is performed input data modification using the key K_{mod}. As a result, the received modified input information is written to the database and transmitted to the system of goals' and operations' modification in conjunction with the key K_{mod}.

4. The system of goals and operations modification generates a private key K_t. As a result of exchanging keys inside the risk accounting module, the system receives the key K_{mod}. This is followed by the preparation of the next 3 sets: the set of main goals c, the set of additional goals c` and the set of processes f for use as a stego-container.
5. Alternative sets of goals and processes are formed by steganographic semantic modification of existing information using the key K_t.
6. The stego-container is being filled up.
7. The key K_t is passed to the database in conjunction with alternative main goals $\bar{c}$, additional goals $\bar{c}'$ processes $\bar{f}$ and with a version of the key, encrypted through the modified information $\{\bar{I}\}K_t$ and also the key is passed to the head of the enterprise.

If it is necessary to form a real prediction or identify a possible insider, the head of the enterprise, having both keys, can extract the DW using the key K_t. He can also recover the initial data using the key K_{mod} and generate a real prediction, or find the operator N_z by finding the base of the logarithm of the initial data modification $(N_z+1)\cdot K_{mod}$.

Forecasting the effect of measures implementation in order to take into account the risk of insider attacks has a high degree of uncertainty. However, based on a two-component calculation using the process-statistical approach described in [11] and statistics of financial losses from insider attacks [12], it is possible to predict the effect of the risk accounting system at highest accuracy. Thus, the overall efficiency will consist of two components: the total value of preventable losses and the cost of providing the necessary measures. It follows that the efficiency can be determined by the following formula:

$$E = \sum_{i=1}^{n}(P_i + R_i) - \sum_{j=1}^{m} K_j, \tag{4}$$

where P_i – prevented losses, R_i – funds that can be returned as a result of the system functioning, K_j – the cost of providing the necessary measures.

Based on statistics [12], insider attacks require some defined costs to eliminate a single incident. This is the cost of: monitoring and surveillance – $10,902, investigation – $88,982, escalation – $18,734, incident response – $109,300, containment – $196,891, ex-post analysis – $11,443, remediation – $171,494, which is total $607,745. On average, it is possible to lose about $ 2,992,054 per year, which corresponds to 5 incidents. Thus, in this case, the prevented losses include: monitoring and surveillance, escalation, containment and remediation. Containment can be attributed to reimbursable funds due to the ability to prove the guilt of the party who caused the incident. At the same time, there is no need to purchase specialized and other means of counteracting insider attacks, such as DLP systems. Thus, taking into account the cost of such systems, which consists of the system's license cost and the cost of its implementation and is about $600 for one personal computer, and considering the availability of about 500 PCs in medium-sized organizations, the cost of such system will be $300,000 per year. Thus, the efficiency will be calculated by the formula E=5*(10902+18734+196891+171494)=1990105, which means cost reduction of $2 million per year. In this case, if compared with the use of DLP systems, the efficiency will be calculated as follows E_{DLP}=5*(196891+171494)-300000=1541925. According to the analysis, the efficiency of DLP systems [1] is equal to 54% and coincides with the calculation in the work with an error of 2.5% (51.5%). Based on this, it can be argued that the efficiency error of the developed system will be within 2.5% as well. Thus, it can be assumed that the effectiveness of the developed system will be 66.5%, and it means increasing the effectiveness of the insider attacks risks prevention by 15%.

6. Discussion of the Results of Researching the Comprehensive Technology for Alternative Management of Complex Organizational and Technological Objects in the Conditions of Cyber Threats

The comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats is developed basing on combined application of grapho-analytical methods and the steganographic protection method of the proprietary data from insider attacks. This technology provides opportunities to present the strategy of the future and its consequences with full data protection from leakage. The use of grapho-analytical methods increases the confidence in modelling and ensures the model's flexibility. The proposed system for alternative management of complex organizational and technological objects allows to determine the development scenario of the management object and to predict the dynamics of achieving strategic goals, the dynamics of processes' carrying out, the dynamics of the risky events impact. In addition, it is provided an opportunity to determine the best option to build a strategy for the development of organizational and technological object for the long term. The steganographic protection method of the proprietary data from insider attacks is not limited to providing the ability of detecting the fact of aggressive interference in the data. The method also allows to counteract the possibility of information leakage and to increase the efficiency of identifying the person who directly carried out the insider attack. The disadvantage is the reduced efficiency of identifying the malefactor's identity if gaining the access and using operator's profile by a third party. The further development of the protection method involves leveling this limitation by focusing on the psycholinguistic portrait of the person who enters the data, which will eliminate the possibility of substituting the operator's profile by an insider. At the stage of implementing such improvement, there may be difficulties associated with the computerized definition of the insider's psycholinguistic portrait, which can be formed basing on one malefactor or a group of insiders and that requires the development of additional analysis methods. Thus, the scheme of for two-level DW embedding should be modified by developing the third level, which will be responsible for computerized psycholinguistic analysis.

7. Conclusions

It was developed the comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats:

1. It was carried out a simulation modelling of the system for alternative management of complex organizational and technological objects based on the goal scenario, presented by the processes' graph. This model reflects the relationship between goals, processes, transitions, and presents different implementation options of a management strategy for organizational and technological objects.
2. It was suggested the steganographic method of classified proprietary data protection from threats of insider attacks which provides prevention of insider attacks risk by 15% in comparison with separate use of specialized systems. Applying of this method in the system for alternative management of complex organizational and technological objects provides information protection from unauthorized access, detecting the fact of aggressive interference in the data and counteracting the information leakage possibility, along with increasing the efficiency of identifying the insider.

8. Acknowledgements

We express our gratitude and deep appreciation to our colleagues at the Department of Information Technology Design for their support during the work on the article as well as to the Department of Information Security and Computer Engineering of the Cherkasy State Technological University and especially to the Head of the Department—Volodymyr Rudnytskyi, Sc.D., Professor for the relevant notes and advice on the article.

9. References

[1] Insider Threat Report, 2019. URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf.

[2] T. O. Prokopenko, A. P. Ladanyuk, Information technology management organizational and technological systems, Vertical, publisher Kandych S. G., Cherkasy, 2015.

[3] D. Lin, Insider threat detection: Where and how data science applies, Cyber Security: A Peer-Reviewed Journal. 2(3) (2018) 211–218. URL: https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000003/art00003.

[4] K. W. Kongsgård, N. A. Nordbotten, F. Mancini, P. E. Engelstad, An Internal/Insider Threat Score for Data Loss Prevention and Detection, in: Proceedings of the 3rd ACM on International Workshop on Security and Privacy Analytics, Scottsdale, USA, 2017, pp. 11-16. doi: https://doi.org/10.1145/3041008.3041011.

[5] E. Benková, P. Gallo, B. Balogová, J. Nemec, Factors Affecting the Use of Balanced Scorecard in Measuring Company Performance, Sustainability, 12(3) (2020) 1178. doi: https://doi.org/10.3390/su12031178

[6] T. A. Prokopenko, Ya. L. Zyelyk, Complex method of strategic decision-making in management of technological complexes of continuous type, Journal of Automation and Information Sciences, 49 (2017) 71-79. doi: https://doi.org/10.1615/JAutomatInfScien.v49.i11.70

[7] S. A. Yuditsky, Operational-target modeling of the development dynamics of organizational systems by means of Petri nets, Automation and Remote Control, 1 (2008) 114 -123.

[8] B. Kosko, Fuzzy Cognitive Maps, International Journal Man-Machine Studies, 11 (1986) 65-67.

[9] S. A. Yuditsky, Modeling of cycles in developments of organizational systems. Instruments and Systems: Monitoring, Control, and Diagnostics, 2 (2011) 17-20.

[10] E. V. Meleshko, Method of embedding of two-level digital watermarks into media files for copyright protection, Scientific Works of Kharkiv National Air Force University 37(4) (2013) 127-131.

[11] E. N. Efimov, G. M. Lapitskaya, Evaluation of the effectiveness of information security in conditions of uncertainty, Business Informatics 31(1) (2015) 51–57.

[12] 2018 Cost of Insider Threats: Global Report, 2018. URL: https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf.