https://orcid.org/0000-0002-9374-2833
https://orcid.org/0000-0002-8047-7647

UDC 004.772

H.T. SAMOILENKO[*], Yu.Yu. YURCHENKO[*]

CONCEPTUAL MODEL OF ENTERPRISE SECURITY IN THE INFORMATION ENVIRONMENT

[*]State University of Trade and Economics, Kyiv, Ukraine

Анотація. *Визначено характерні риси та ознаки інформаційного суспільства. Інформаційне середовище, яке розглядається для формування моделі безпеки підприємства, є складовою інформаційного суспільства. Виділено класи інтелектуальних інформаційних технологій (ІІТ), необхідних для взаємодії суб'єктів в інформаційному суспільстві. Зазначені класи ІІТ, взаємно доповнюючи один одного, створюють умови сталого доступу до інформації і знань, що оновлюються. Визначено та охарактеризовано складові інформаційного середовища, а саме: організація; технології; цифровий репозиторій інформаційних та методичних ресурсів; сервіси; математичні методи моделювання; система моделювання безпеки підприємства відповідно до типів, цілей і принципів та інформаційно-телекомунікаційна інфраструктура. Визначено внутрішні і зовнішні ресурси організації, наявність яких впливає на формування моделі безпеки підприємства. В рамках інформаційного суспільства запропонована концептуальна модель дозволяє визначити необхідний набір сервісів і інформаційних ресурсів, потрібних для формування моделі безпеки підприємства. Виділено основні компоненти моделі безпеки підприємства: задачі безпеки; комп'ютерні комунікації; засоби безпеки; гнучкість; організаційне середовище. Запропонована практична реалізація дає можливість доступу до інформаційних ресурсів, обміну повідомленнями з використанням існуючих комунікацій, участі в загальних дискусіях, пошуку інформації відповідно до запиту, організації колективної (спільної) діяльності. Грунтуючись на структурі організації, запропонована практична реалізація моделі забезпечує розмежування рівнів доступу, реалізує індивідуальні профілі захисту та забезпечує безпеку персональних даних користувачів.*
Ключові слова: *інформаційне середовище, концептуальна модель, модель безпеки.*

Abstract. *Characteristic features and signs of the information society are defined in the paper. The information environment, which is considered for the formation of the enterprise security model, is an information society component. The classes of intelligent information technologies (IIT) that are necessary for the interaction of subjects in the information society are highlighted. Complementing each other, the specified IIT classes create conditions for stable access to information and knowledge that are updated. According to their types, goals, and principles, the article defines and characterizes such information environment components as organization, technologies, a digital repository of informational and methodical resources, services, mathematical modeling methods, enterprise security modeling system, and information and telecommunication infrastructure. The internal and external resources of the organization, whose presence affects the formation of the enterprise security model, are determined. Within the framework of the information society, the proposed conceptual model makes it possible to determine the necessary set of services and information resources needed for the formation of the enterprise security model. The paper highlights the following main components of the enterprise security model: security tasks, computer communications, safety equipment, flexibility, and organizational environment. The proposed practical implementation allows accessing information resources, exchanging messages using existing communications, participating in general discussions, searching for information, according to the request, and organizing collective (joint) activities. Based on the organization structure, the offered practical implementation of the model ensures the delimitation of access levels, implements individual protection profiles, and ensures the security of users' data.*
Keywords: *information environment, conceptual model, security model.*

DOI: 10.34121/1028-9763-2023-1-112-117

1. Introduction

The use of models as simplified descriptions of important system components makes it possible to simplify the solution to the task of creating a security system adequate to real threats [1]. The use of various methods to evaluate information protection at enterprises was considered by many scientists, namely: V.V. But, V.V. Mykytenko, O.V. Grebenyuk, M.O. Zhivko, O.A. Sorokivska, V.S. Tsymbalyuk, A.M. Chorna. But the justification of the need to use research models and methods remains an unsolved issue in the field of information protection. Modern methods are not always available and convenient to use, they require significant financial costs. Security models are one of the main elements of protection. They are integral parts of the overall modeling process that can be divided into two components: construction and implementation of the model [2].

The aim of the article is to present a conceptual model of enterprise security in the information environment.

2. Results of the research

In a multiple notation theory, information environment can be represented as follows:
IE = {organization, intelligent information technologies, resources, services, enterprise, security modeling system, and information and telecommunication infrastructure}.

1. Based on the analysis of the existing IE, it becomes obvious that the functioning of IE is always supported by the basic organization (enterprise) whose aspects are logistical support for the implementation of the IE functions, and, accordingly, the implementation of processes (a set of sequential actions to achieve the result) representing these functions [3]. The performance of these functions depends on the characteristics of the organization – its type, goals, and principles (Fig. 1).

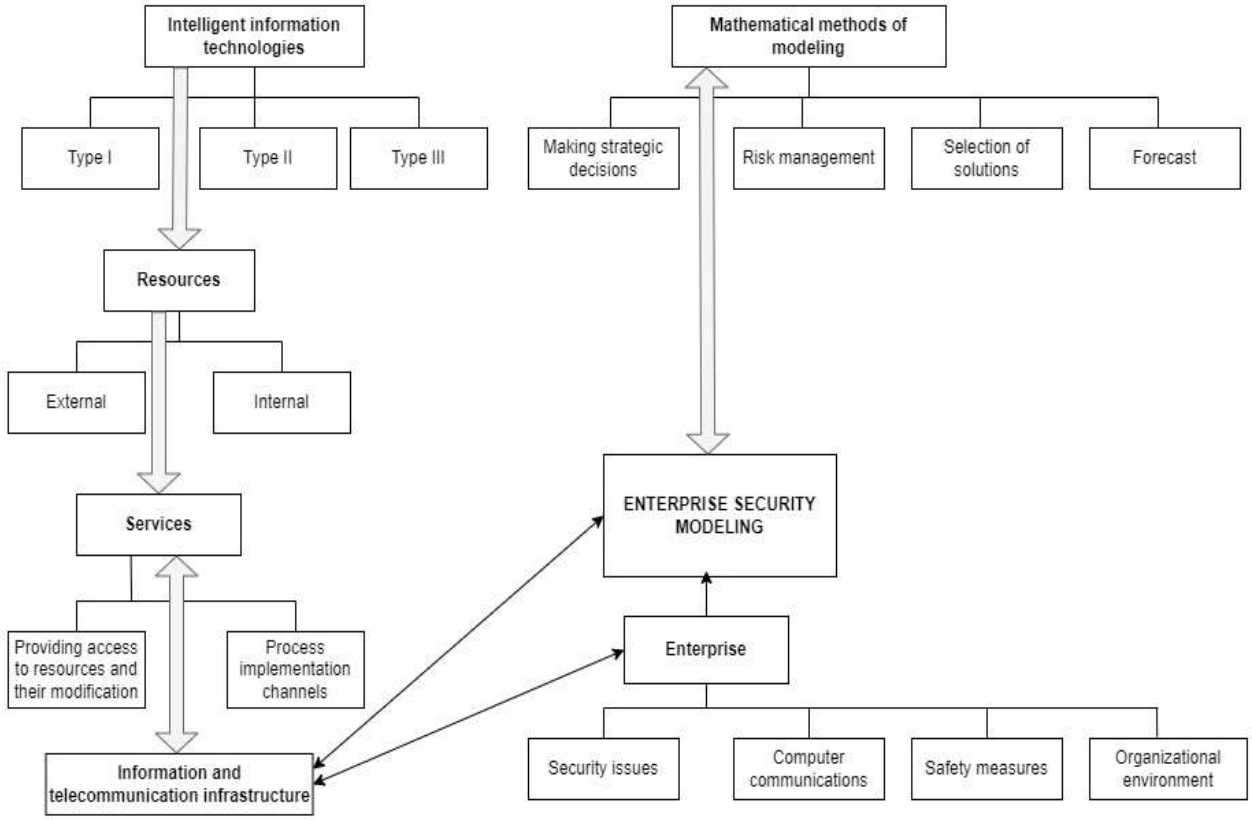

Figure1 – Conceptual model of enterprise security [adapted by the authors]

As an organization, there can be a network structure as a subsystem within an existing institution, enterprise, other organization, or an independent network organization that implements the goals of IP, being its leading component [4].

2. The modern stage of the formation of the information society is characterized by the development of intelligent information technologies (IIT). Due to the spread of IIT in the information society, the technological component of IE is radically changing. The use of these technologies greatly facilitates access to information, means of its processing and, accordingly, expands the range of consumers of information, which is one of the main conditions for building an information society. The specifics of the developing information society impose very high demands on the pace of dissemination of new knowledge. This requires highly effective technologies for extracting expert knowledge and presenting them in a widely available digital form – this is the first class of IIT that is desirable to use in IE. The second class of IIT is a technology that allows you to overcome spatial and temporary restrictions and provides access to information and knowledge, and the possibility of interpersonal communications regardless of the subject location and at any given time. The third class of IIT is technologies ensuring the interaction of the distributed structure of IE with distant participants in the process, the possibility of implementing active methods of modeling, and intensive interaction of subjects.

IE is a phenomenon where all three of these IIT classes are combined, mutually complement each other, and create conditions for constant access to information and knowledge that are intensively updated, as well as the implementation of the paradigm of modeling the choice of the investment portfolio of the enterprise.

3. Resources. In the framework of IE, information resources and knowledge of community members are produced. Information resources intended for wide access are also produced and subjected to examination, and quality processing of information is carried out (its relevance and value are determined). The information component expands due to the inclusion of digital resources with unlimited access, because there are no spatial and temporal restrictions, and the borders between states are being erased. Internal and external resources of the organization are allocated, whose presence affects the formation of the security model of the enterprise.

4. Services. They are represented by many functions, each of which corresponds to a certain service that provides access to resources and their modification and many channels for the implementation of processes that operate information flows and provide interpersonal communications of IE for the implementation of information interaction of its participants (in fact, this is application software of IE).

The list of services provided by IE gives an opportunity to access information resources, exchange messages using existing communications, participate in general discussions, search for information, according to the request, and organize collective (joint) activities. The technical service platform should be based on system software that includes various Internet services.

5. Mathematical methods of modeling. By systematizing mathematical modeling methods according to the application criterion, the following four independent directions can be distinguished:

- analytical methods;
- statistical methods;
- mathematical programming;
- game-theoretic methods.

Thus, analytical methods are used in conditions of complete certainty of information and are characterized by the establishment of functional dependencies between the conditions for solving the problem and its results (the adopted decision). These include finite and infinite numerical methods. One of the key tasks of finite numerical methods is making strategic decisions. Infinite numerical methods are highly effective in constructing the break-even equation. Unlike analytical methods, statistical methods are used in conditions of probable certainty of information

about the decision-making situation and are based on the collection and processing of statistical materials. A characteristic feature of these methods is the consideration of deviations and probabilistic processes. In modeling, the methods of statistical tests have become widely used, and it makes it possible to analyze and evaluate different ways of project implementation. Currently, these methods are considered to be one of the most effective methods of researching complex systems and managing risks. Mathematical programming methods (linear and nonlinear) are used to ensure the maximum (or minimum) of the objective function under certain constraints. The majority of mathematical programming problems in research projects and design are nonlinear programming problems. One-stage and two-stage tasks can be distinguished from them. In the tasks of building individual security profiles, two-stage tasks show high efficiency. Linear programming methods have become widely used in the field of resource allocation. Game-theoretic methods are devoted to the study of models and methods of making optimal decisions in conflict conditions. In order to study the conflict situation, a formalized simplified model of it is being built. Game theory methods are used in cases where the uncertainty of the situation is caused by the conscious actions of the opponent, including predicting his actions. The methods of the theory of statistical decisions are used under conditions of uncertainty of the situation caused by circumstances of a random nature. These methods are most widely used to choose solutions taking into account the actions of competitors.

Among the wide range of components of the information environment, we will single out the enterprise security modeling system as the basis for the formation of the enterprise security policy.

6. The enterprise security modeling system is a system of information and technological resources, means, methods, and forms of project selection, as well as relevant computer communications, both between participants in the process (which are elements of the system) and between participants and resources provided by the system, which ensures the selection of technical tasks in accordance with the chosen task (for example, optimizing access to information resources). The introduced concept includes elements of informational, technological, organizational, and mathematical components of IE. The composition of these elements determines the system-forming factor – the goal of modeling. The goal of enterprise security modeling is the main statement this system can offer – knowledge, skills, and abilities to be acquired by the organization in the process of interaction with this system.

It is necessary to take into account the mutual influence of the components of the security modeling system of the enterprise, which allows you to make reasonable design decisions at each step of the design. Within the framework of IS, the descriptive model of the system will allow you to determine the necessary set of services and information resources necessary for the formation of the security model of the enterprise. The proposed enterprise security model, which is a structural element of IE, consists of the following components:

• security tasks (purpose, characteristics of the organization, security policy, enterprise capabilities, mathematical approach (meaning the last level in the scheme of methods), methodological materials, and adaptation);

• computer communications (online platforms, means of interpersonal communications (for discussions, exchange of views, and debates), resource allocation systems, and collective support systems);

• security means (technical implementation of access to information and resources, individual security profiles, and organization of authorized access to resources and information);

• flexibility (the ability of the system to tune in to any challenges of the time);

• organizational environment.

The organizational environment is an important element of the enterprise. Security modeling system, as a rule, includes the following components (some of them are provided by IE):

• administrative region, which is used for registration, making announcements, announcement of plans, etc.;

• information area, which contains the study of offers for possible technical tasks;

• computer conference (for discussion);

• navigation system;

• tools (for example, tools for working inside small groups, shared workspaces, and windows);

• resources (archives, e-mail addresses, scientific articles, links, etc.).

7. As an internal system-forming factor of IE, it is possible to consider its information and telecommunication infrastructure ensuring the complementarization of elements, exchange of information and functional connections, including between IE participants in the joint solution of tasks. An external system-forming factor is a need for society, that is, the above-mentioned goal of society (social order). It should be noted that under the influence of socio-economic conditions, namely, the active process of building an information society, and with the advent of IIT, IE in this time significantly expands its functionality and, accordingly, the number of processes implemented. First of all, this is due to the widespread distribution of virtual enterprises and the need to jointly solve professional problems outside of spatial and time restrictions. In turn, the above classes of IIT, which have found their intensive application in IE, provide effective means for creating a unified representation of information and, consequently, solving a variety of professional tasks, overcoming spatial, temporal and linguistic restrictions.

3. Materials and methods

The implementation of the conceptual model on the example of the data protection system in the medical center is offered. The proposed system does not belong to typical technical solutions. It required the development of individual protection profiles, data virtualization, copy schedules for different servers, and user instructions [5]. Information for the construction of a comprehensive data protection system was taken on the basis of a comprehensive survey of the organization for which the development was carried out (Fig. 2).

Among the requirements for the data protection system, the following should be highlighted:

• ensuring the integrity, relevance, and consistency of the processed information;

• ensuring the confidentiality of the information stored in the information system of the company;

• ensuring the demarcation of user access to system objects and functions;

• storing information about the author and the time of creation, modification, and deletion of any object or data in the system;

• supporting the possibility of interaction and exchange of information with other interested users.

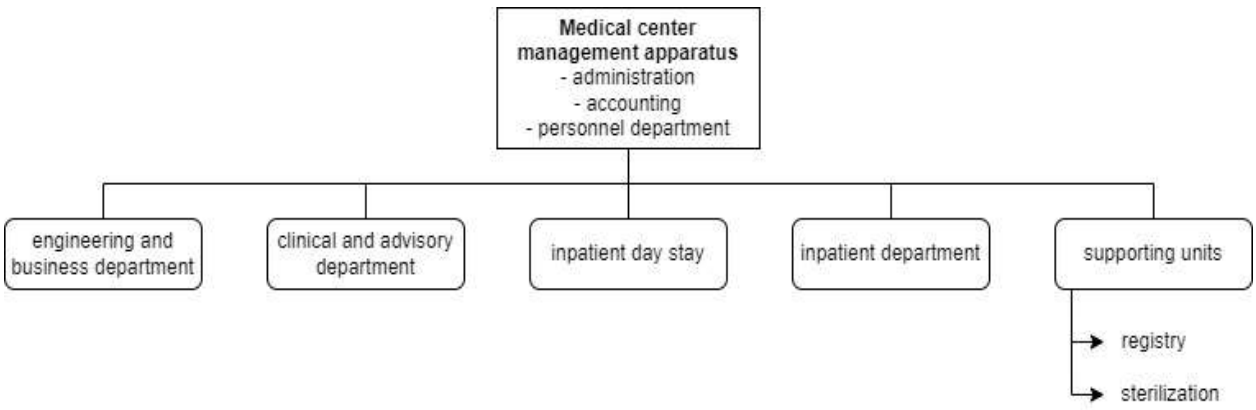

Figure 2 – Organizational structure of the enterprise

As a result of the implementation of the data protection system of the company, it was possible to significantly increase the level of protection, namely, monitor and control the network traffic of the corporate network of the company, monitor any actions to the end computer and user, and monitor changes to the data of the company. Taking into account the specifics of the enterprise, namely the medical center, the proposed data protection system ensures the delimitation of access levels, implements individual protection profiles, and secures patients' data.

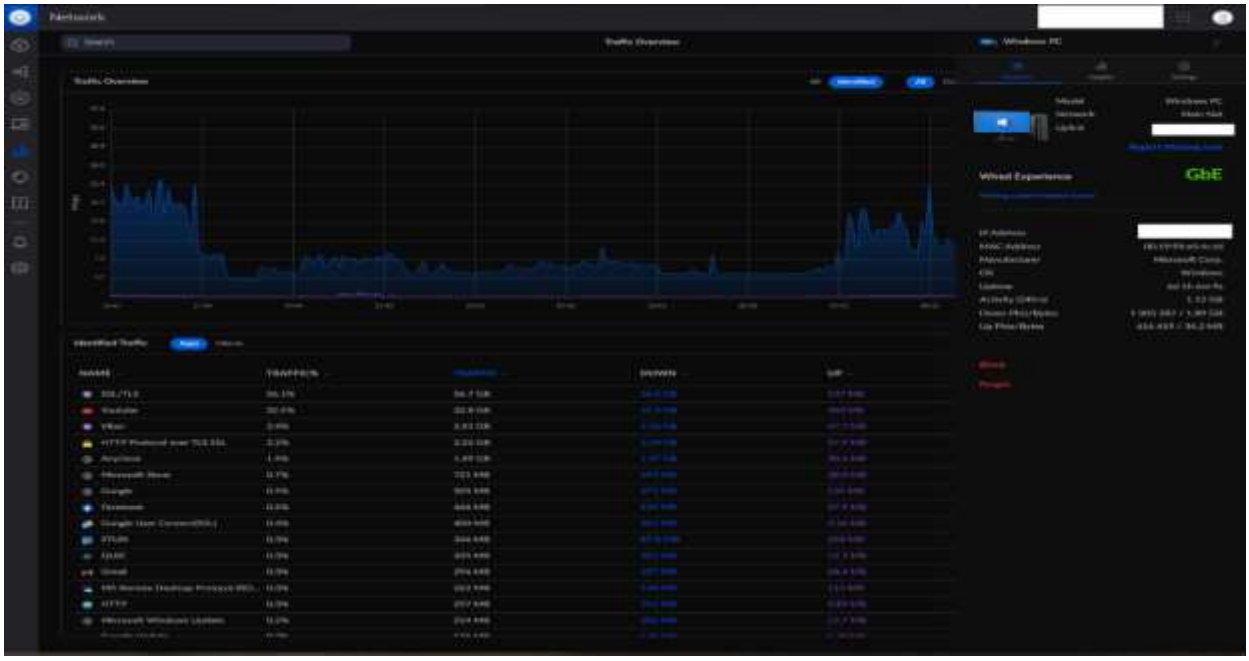

Figure 3 – Analysis of the network traffic of a corporate computer network

4. Conclusions

IE accumulates symbiosis by mutually complementing each other and interacting classes of the latest information technologies, mathematical methods of modeling, and means of global computer communications. A conceptual model of enterprise security as a component of the information society is proposed. The requirements for the components of the information environment are defined. The use of conceptual models as simplified descriptions of important system components makes it possible to simplify the solution to the task of creating a security system adequate to real threats. The offered model can be used as a basis for enterprise security mechanisms, for the analysis of the security system and discretionary separation systems, for access control, for ensuring data integrity, etc.

REFERENCES

1. Common Criteria Services – ISO 15408.
2. Диогенес Ю., Озкайя Е. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.
3. Gritsenko V.I., Bazhan L.I. Desirable. Digital transformation of economics. *Control systems and machines*. 2017. N 6. P. 3–16.
4. Verenych O.V. Formalized model of mental space of project manager, project team. *Management of complex systems development*. 2015. N 24. P. 23–29.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020. 1008 с.

Стаття надійшла до редакції 10.01.2023