THE MATHEMATICAL MODELS AND METHODS OF COMMERCIAL INFORMATION PROTECTION USAGE IN THE BUSINESS ENVIRONMENT

ВИКОРИСТАННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ТА МЕТОДІВ ЗАХИСТУ КОМЕРЦІЙНОЇ ІНФОРМАЦІЇ У БІЗНЕС-СЕРЕДОВИЩІ

UDC 004:338

Kolenko V.V.
Specialist of the Second Category,
Instructor of Computer Science
and Information Technologies Department,
Head of the training laboratory
Kherson Polytechnic College
of Odessa National Polytechnic University
Nakonechna V.I.
Specialist of the Second Category,
Instructor of Management, Economics
and Administration Department,
Kherson Polytechnic College
of Odessa National Polytechnic University
Anosova Yu.P.
Specialist of the Highest Category,
Instructor of the Foreign Language Cycle
Committee, Methodologist
Kherson Polytechnic College
of Odessa National Polytechnic University

The article substantiates the relevance of the measures' system implementation for the formation of the commercial information protection market in Ukraine. Models of information security processes in computer systems, which allow to determine (evaluate) the general characteristics of the noted systems and processes; the main means, methods and directions of commercial information protection, as well as the problems of protecting information in enterprises are reflected in the article. The need to create different protection systems using mathematical models and methods for protecting commercial information in an entrepreneurial environment has been investigated. Necessity of creating an organizational and economic mechanism for providing the enterprise information security is proved. Specialized anti-bullying software, employees monitoring programs, for example, the American company Spector Soft Corporation, is proposed to use against insiders.

Key words: *information protection, mathematical methods, models, commercial activity, enterprise, insider, software.*

В статье обоснована актуальность внедрения системы мероприятий по формированию рынка услуг защиты коммерческой информации в Украине. Рассмотрены модели процессов защиты коммерческой информации в компьютерных системах, которые позволяют определять (оценивать) общие характеристики отмеченных систем и процессов; основные средства, методы и направления защиты коммерческой информации, а также проблемы защиты информации на предприятиях. Исследована потребность в создании разных систем защиты с использованием математических моделей и методов процессов защиты коммерческой информации в условиях предпринимательства. Доказана необходимость создания организационно-экономического механизма обеспечения информационной безопасности предприятия. Для борьбы с инсайдерами предложены специализированное программное обеспечение антишпионского предназначения, программы мониторинга сотрудников, например американская кампания "Spector Soft Corporation".

Ключевые слова: *защита информации, математические методы, модели, коммерческая деятельность, предприятие, инсайдер, программное обеспечение.*

У статті відображено моделі процесів захисту інформації в комп'ютерних системах, які дають змогу визначати (оцінювати) загальні характеристики зазначених систем і процесів. Основне призначення загальних моделей полягає у створенні передумов для об'єктивного оцінювання загального стану комп'ютерної системи щодо заходів вразливості або рівня захищеності інформації в ній. Розглянуто основні засоби, методи й напрями захисту комерційної інформації, сучасні проблеми захисту інформації підприємств. Досліджено сутність понять «інформаційна безпека», «інформаційна безпека підприємства». Класифіковано основні джерела та суб'єкти загроз, методи й засоби щодо усунення загроз для інформаційних систем. Доведено необхідність створення організаційно-економічного механізму забезпечення інформаційної безпеки підприємства. Досліджено потребу створення різних систем захисту з урахуванням використання математичних моделей та методів процесів захисту комерційної інформації в умовах підприємства, особливостей та умов їхнього функціонування. Розглянуто основні засоби, методи та напрями захисту маркетингової інформації, а також висвітлено регулювання цього питання на державному рівні. Запропоновано систему заходів з формування ринку послуг із захисту комерційної інформації в Україні. Виділено цілу низку джерел загроз інформаційній безпеці сучасного підприємства. Визначено суб'єкти, з боку яких може бути загроза інформаційним системам підприємства. Зроблено висновок, що з огляду на поширення інформаційних технологій у повсякденному житті кожна людина дедалі частіше стикається з необхідністю захисту комерційної інформації, тому питання інформаційної безпеки стає таким важливим та актуальним. Пов'язано це зі зростанням можливостей обчислювальної техніки, адже розвиток засобів, методів та форм автоматизації процесів оброблення інформації робить інформацію набагато вразливішою. Для боротьби з інсайдерами запропоновано спеціалізоване програмне забезпечення антишпигунського призначення, програми моніторингу співробітників, наприклад американська кампанія "Spector Soft Corporation".

Ключові слова: *захист інформації, математичні методи, моделі, комерційна діяльність, підприємство, інсайдер, програмне забезпечення.*

Formulation of the problem. Problems in providing information security in the modern world are growing in the same way as increasing threats, such as unauthorized destruction, replacement, copying, blocking of the authorized data access. Therefore, the information that organizations, firms or corporations own and use needs to be constantly protected. Recently the development and implementation of new methods and technologies for the processing, transmission and storage of information has considerably increased, which has caused the globalization of telecommunication networks. The rapid deployment of new generation networks contributes to the role and importance of providing information security, which is an integral part of the enterprise's business, conducted in a new way.

Common models of processes for protecting commercial information in computer systems are those that allow us to determine and evaluate the general characteristics of these systems and processes.

The purpose of general models is to create the prerequisites for an objective assessment of the computer system general state in terms of vulnerability degree or information security level in it.

The need for such assessments appears in the analysis of the general situation in order to develop strategic decisions in the organization of information protection [7, p. 154].

Analysis of recent research and publications. A large number of scientific achievements of native scholars should be noted among the most important

studies covering various aspects of the information society formation and information security in its general meaning. Among them there are O. Baranov, V. Behma, K. Bieliakov, V. Bakumenko, V. Havlovskyi, I. Havrylov, V. Herasymenko, O. Hladkivskyi, M. Hutsaliuk, V. Domariev, M. Zhulynskyi, L. Zadorozhna, O. Zinchenko, V. Malinko, V. Malynovskyi, D. Olshanskyi, V. Petryk, V. Popov, O. Laktionova, H. Lazariev, A. Marushchak, V. Tsymbaliuk, M. Shvets. The foreign scholars N. Wiener, B. Rolker, L.J. Hoffman, C. Shannon should also be mentioned.

Setting task. The aim of the article is to define from the theoretical point of view the notion of the enterprise information security in accordance with modern tendencies of the newest management technologies introduction, to substantiate the priority tasks, which are aimed to preserve and protect the information in telecommunication networks of general use. The usage of mathematical methods and models of information security also is to be considered. The principles concerning organization of the enterprise telecommunication networks information security is to be substantiated.

Presentation of the main research material. To achieve market success, the company needs relevant, reliable and exhaustive information about customers, competitors, suppliers, and intermediaries. The value of the information is in creating the preconditions for gaining competitive advantages, helping to reduce the level of commercial risk, to determine and take into account changes in the surrounding business environment.

Taking into account that commercial information, is defined as a collection of data, messages, information, characterizing the business environment, objects, phenomena, processes, communications that need to be collected, transmitted and processed to make managerial decisions [11, p. 5], it is identified as the resource. Many scholars [11, p. 7] apply a resource approach to the notion of information. Therefore, for each firm it is important to maintain competitive advantages on the market, which is the question of confidentiality that is the protection of information from the opponents.

One can distinguish a number of the threats sources to a modern enterprise information security:

– illegal activity of some economic structures in the field of the formation, dissemination and information usage;

– violations of established rules on information collecting, processing and transferring;

– intentional actions and unintentional mistakes of information systems personnel;

– errors in the information systems design;

– hardware and software failures in information and telecommunication systems, etc. [8].

It is also necessary to take into account that the threat to information systems of the enterprise may come from the following entities:

– employees of the enterprise using their official position (when the legal rights of the position are used for illegal transactions with information);

– employees of the enterprise who are not entitled by virtue of their official duties, but who have unauthorized access to the confidential information;

– persons who are not connected by the current employment agreement (contract).

Unfortunately, one of the most important threats to companies from the point of view of information security is their own employees, who are called insiders. Insiders are employees who deliberately, due to negligence or ignorance, cause the leakage of confidential information to which they have access in order to perform their official duties. The greatest damage is caused by those who sell data to the competitors of the company. To struggle with this, there is specialized anti-scam software, employee monitoring program; for example, the Spector Soft Corporation [5] developed the Spector 360 product, which is intended for centralized employee monitoring. The anti-insider program explores how employees use their computers and the Internet. Spector 360 allows you to inspect the entire organization through graphic charts.

In addition, we will analyze the concept of “information protection”, which is understood in the work [10, p. 67] as a set of measures for providing the physical integrity of information, preventing unauthorized changes and getting data and its characteristics are data reliability, confidentiality, integrity and availability of information.

Information security is safety (state of safety) of the individual, society and state basic interests in the field of information, including information and telecommunication information infrastructure and the actual information and its parameters, such as completeness, objectivity, accessibility and confidentiality.

The tasks of the information system (IS) protecting can be divided into several levels, namely:

1) well-timed provision of decision-making processes with reliable information on the basis of data entered into the IS data:

– sufficient data completeness;

– the initial data authenticity;

– sufficient speed of decision-making;

– availability;

– the response guarantee after receiving the request;

2) the enterprise’s competitiveness providing:

– confidentiality saving;

– the intruder misinformation.

All this complex will enable to form a commercial information protection system as a software and hardware complex, into which anti-insider program should be included.

Among the key areas of information security in IS there is the technical protection of information, which

is divided into two major classes, namely: information protection systems from unauthorized access (UAA) and information protection systems from leakage through technical channels.

UAA protection is carried out in different components of the IS:

1) applied and system software;
2) hardware part of the workstations servers;
3) communication equipment and communication channels;
4) the perimeter of the IS.

The protection of information, providing information security should be of a systemic nature, that is, different means of protection should be applied simultaneously and under common control.

The information protection objectives in the system can be represented as an organization of optimal functioning.

In this case, the concept of optimal functioning can be formulated in accordance with statements of optimization tasks: for given resources to ensure maximum results, or provide the desired result with minimal costs [6, p.230].

Fig. 1 shows a general model of the choosing information security systems process.

The model uses the following notation:

– **C** is the financial means, which the opponent possesses;

– **{L}** is multitude estimates of system losses, in case of successful implementation of information threats;

– **{LZ}** is multitude estimates of system losses in the case of information protection means application;

– **{MR}** is multitude system resource usage parameters;

– **{P}** is multitude violators;

– **T** is time, which an attacking party has for realization of the threats;

– **{TS}** is technological system functioning scheme;

– **{U}** is multitude information threats;

– **{Z}** is multitude means of information protection;

– **r** is vector of information protection means usage in the system.

We formulate the tasks that must be solved for the information system protection means choice [6, p. 235]:

– to develop a model for the functioning of the system and a model for using its resources;

– to build a model of a probable opponent, evaluate his capabilities;

– to develop a model of system information threats;

– to develop a model for estimating losses.

Based on the opponent capabilities, as well as on the model of threats, it is necessary to build a reliable model for allocating resources to protect information.

Let us study the formal description of each of these models [3, p. 54].

The model of the system functioning can be formally represented as a function:

$$F \rightarrow \{TS\}, \quad (1)$$

where **{TS}** is a formal description of the system functioning technology.

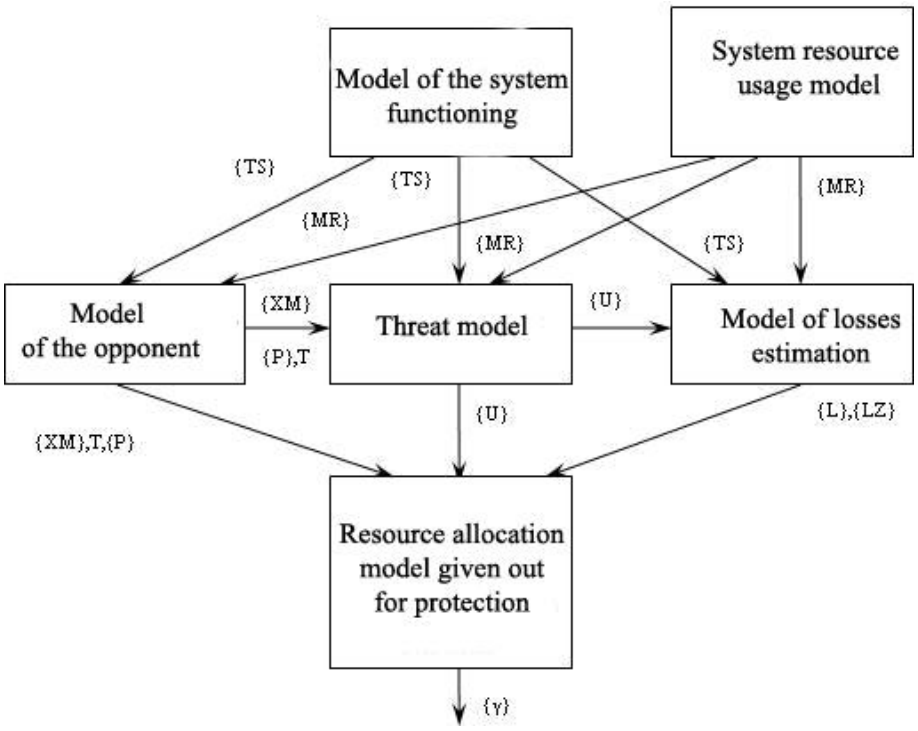

Fig. 1. The general model of the choosing information security means process

The information processing system will act as the output data function.

The result of this function is a formal description of the system's operation technology.

The system resources usage model is a function of:

$$F(\{TS\}) \rightarrow \{MR\}. \quad (2)$$

where **{MR}** is a formal description of the resources used by the system at various stages of information processing.

The model of the opponent represents the following function:

$$F(\{TS\},\{MR\}) \rightarrow (\{P\},C,T,\{XM\}). \quad (3)$$

where **{P}** is multitude of intruders categories; **{XM}** is multitude means for realization of the opponent's destructive actions; **C** is the opponent's financial capabilities; **T** is time, which is at the disposal of the attacking party.

The threat model describes the following functionality:

$$F(\{MR\},\{TS\}) \rightarrow \{U\}, \quad (4)$$

where **{U}** is formally described multitude system information threats.

The model of possible losses estimation is described as follows:

$$F(\{TS\},\{MR\},\{U\}) \rightarrow (\{L\},\{LZ\}). \quad (5)$$

where **{L}** is system losses caused by the threats successful implementation; **{LZ}** is system losses caused by the use of information security means.

Distribution model of resources allocated to protect information:

$$F(\{U\},\{L\},\{LZ\},\{XM\},\{P\},\{Z\},T,C) \rightarrow (r). \quad (6)$$

where **{Z}** is multitude means of information protection.

The order of models interaction. At the first stage, a model of system operation is being developed. The results of this phase will be used in all subsequent information security processes models. The functioning system technology is the result of simulation.

After obtaining a description of the system functioning technology, it is necessary to determine the system resources, that is, to determine what resources are used by the system for solving the problems of processing information. Then, it is necessary to describe the resources use scheme. After that, this scheme is needed to determine the possible objects of intruders' attacks, as well as in the information leakage channels formation, etc. [7, p. 165].

The next step is to develop an opponent's model. This requires the results of the previous stages: the operation technology and the resources use scheme.

The above data will help to classify a potential opponent, which in its turn will allow building an adequate information security system in the future. The multitude of attacker's possible categories is the result of building an opponent's model. After the end of the previous stage, a model of information threats is formed. The starting point for simulation will be the technology of the system's operation and the resource's usage scheme.

The result of this stage of simulation is a list of threats to the information system, as well as ways to implement them.

Each item in the list must contain information about the categories of attackers who can implement the specified threat.

In addition, the properties of information that will be violated in the event of a successful threat implementation should be specified.

After getting the list, it is necessary to build models for estimating losses. To do this, it is necessary to calculate estimates of possible losses that the system may incur for each threat from the list. The starting point for building such a model is the technology of the system's operation, the scheme of the resources' usage, as well as the list of threats to the information system. The list of possible losses is the results of simulation.

Despite using these methods, ensuring information security of an enterprise at an appropriate level is possible only when the information component of economic security is considered as an integral part of the enterprise management process.

The system approach to the analysis of financial and economic security involves consideration of economic and production activity as a multi-layered structural system. It is based on the studied object integrity principle, that is, the study of its properties as a whole, since the whole (system) has such qualities that none of its constituents possess (see Fig. 2).

The financial and economic security system has all the properties of the cybernetic system, in particular the availability of information channels between its individual elements; multivariate behavior of the system; manageability and purposefulness of the system [9]. The system approach provides the study of as many connections between elements of the system and the objects of the environment as possible, to identify and analyze the most significant of them. One of the main problems of applying a systematic approach to the entrepreneurship economic security study is the correct system specification, the identification of all its essential elements and the establishment of the whole set of relationships between them.

Experience shows that virtually every enterprise has antivirus protection, user authentication systems, access control systems for the information system, etc. That is to say, the potential of protective means is present, but it is not fully realized by enterprises. The overwhelming majority of requirements of information security standards can be realized by means of protection available to firms [8].

Thus, the comprehensive provision of automated systems information security is a collection of cryptography, software, hardware, technical, legal, orga-

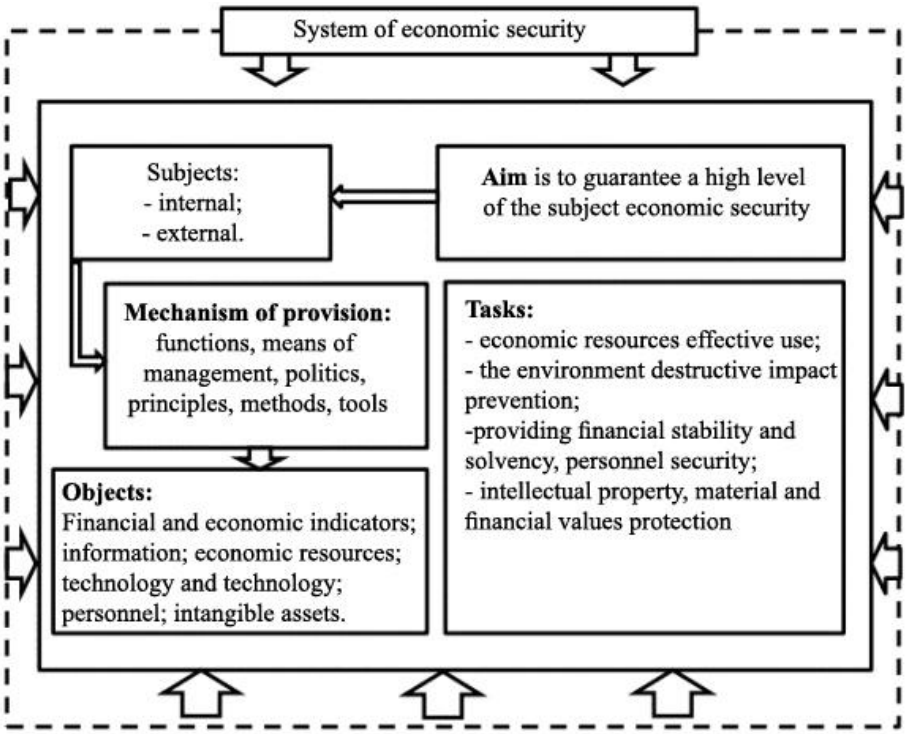

Fig. 2. The entrepreneurship economic security system

nizational methods and means of ensuring the protection of information when it is processed, stored and transmitted using modern computer technology [2, p. 45]. A modern enterprise should be able to formulate an information security policy properly, that is to develop and implement a set of measures for the protection of confidential data and information processes effectively. Such policy provides appropriate requirements for personnel, managers and technical services [2, p. 49].

It is important to define the stages of building an information security policy, namely:

– the registration of all resources to be protected;

– the analysis and creation of a possible threats list for each resource;

– the assessment of each threat occurrence probability;

– the use of measures that allow cost effective protection of the information system [1, p. 356].

In order to provide the whole protection of the commercial information, it is necessary to develop a system of measures for the formation of the information security market in Ukraine, namely:

– a program that minimizes the risks of deliberate and accidental leakage of corporate information

– when collecting, transmitting confidential data it is necessary to use encryption technologies;

– the methodical approaches to the organization of the information security services monitoring market.

Conclusions from the study. Thus, the use of information technology greatly improves the efficiency of processes, reduces the cost of their implementation, but leads to new threats to the enterprise operation. While implementing a systemic approach to information security of an enterprise, one should follow the principles of confidentiality, integrity and availability of information, which will improve its effectiveness. Provision of information security should be considered as an integral element of the enterprise management process.

The analysis of existing information security tools has shown that commercial systems should be based on all types of information security measures, including: protection against insiders, security and fire alarm, digital video surveillance, control and access control to the system, which are regulated by the legislative Levels of the Law of Ukraine. Such means should ensure identification and authentication of users, authority distribution to the system access, registration and recording of attempted unauthorized access. One of the most important components of this process should be a qualified choice of information protection means, which should begin with the identification of the main list of threats, the choice of security measures and the existing means of protection, implementation and the information security testing.

After completing all of the above steps, the solution to the problem of choosing information security means is being solved. The result is a binary vector of known information security tools [4, p.118].

The result of the above is an algorithm for solving the problem of information protection means choos-

ing. When constructing this algorithm, it is necessary to take into account such a circumstance: because of the high significance of each of the simulation stages, as well as the high price of making an incorrect decision, it is necessary to provide the possibility of repeating some simulation steps if necessary.

Thus, building a system for information security is a complex and time-consuming process that requires the use of a wide range of knowledge on information security and is an absolute necessity of the present and a guarantee of a commercial information protection high level in the future.

REFERENCES:

1. Batiuk A., Dvulit Z., Obelovska K., Ohorodnik I., Fabri L. (2004) *Informatsiini systemy v menedzhmenti* [Information systems in management]. Lviv : Intelekt-Zakhid (in Ukrainian).

2. Vlasova L. (2007) *Zashchita informatsii* [Information protection]. Khabarovsk : RYTs KhGAEP (in Russian).

3. Gorbunov V. (2004) *Matematicheskie metody v teorii zashchity informatsii* [Mathematical methods in the theory of information protection]. Moskva : AMGK (in Russian).

4. Doroshko V., Azarov O., Shelest M., Yaremchyk Yu. (2003) *Osnovy kompiuternoi stehanohrafii : navchalnyi posibnyk dlia studentiv i aspirantiv* [Basics of computer steganography: a tutorial for students and graduate students]. Vinnytsia : VDTU (in Ukrainian).

5. Infobezpeka.com. Zakhyst vid insaiderіv – porozhnii zvuk abo neobkhidnist [Insider protection – is it an empty sound or need]. Available at: http://www.infobezpeka.com/publications/?id=285 (accessed: 15 January 2019).

6. Konakhovych H., Klymchuk V., Pauk S., Potapov V. (2005) *Zashchita informatsii v telekommunikatsionnykh sistemakh* [Information protection in telecommunication systems]. Kyiv : MK-Press (in Russian).

7. Konakhovich G., Puzyrenko A. *Komp'yuternaya steganografiya. Teoriya i praktika.* [Computer steganography. Theory and practice]. Kyiv : MK-Press (in Russian).

8. Lytvyniuk A. Osnovy informatsiinoi bezpeky. Kompleksna systema zakhystu informatsii: struktura, vstanovlennia ta pidtrymka funktsionuvannia [Fundamentals of Information Security. Integrated information security system: structure, installation and maintenance of the operation]. Available at: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf (accessed: 12 December 2018).

9. Matiev D. Sredstva zashchity informatsii: problema vybora i sootvetstviya [Means of information protection: the problem of choice and compliance]. Available at: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i- sootvetstviya-5386161 (accessed: 25 January 2019).

10. Pasichnyk V., Zhezhnych P., Kravets R., Peleshchyshyn A., Tarasov D. (2006) *Hlobalni informatsiini systemy ta tekhnolohii : modeli efektyvnoho analizu, opratsiuvannia ta zakhystu danykh* [Global Information Systems and Technologies: Models for Effective Analysis, Processing and Data Protection]. Lviv : NU "Lvivska politekhnika" (in Ukrainian).

11. Pinchuk N., Haluzynskyi H., Orlenko N. (1999) *Informatsiini systemy i tekhnolohii v marketynhu* [Information systems and technologies in marketing]. Kyiv : KNEU (in Ukrainian).

Kolenko Violeta
Specialist of the Second Category,
Instructor of Computer Science and Information Technologies Department
Head of the training laboratory
Kherson Polytechnic College of Odessa National Polytechnic University
Nakonechna Viktoriia
Specialist of the Second Category,
Instructor of Management, Economics and Administration Department,
Kherson Polytechnic College of Odessa National Polytechnic University
Anosova Yuliia
Specialist of the Highest Category,
Instructor of the Foreign Language Cycle Committee, Methodologist
Kherson Polytechnic College of Odessa National Polytechnic University

THE MATHEMATICAL MODELS AND METHODS OF COMMERCIAL INFORMATION PROTECTION PROCESSES USAGE IN THE BUSINESS ENVIRONMENT

The purpose of the article. The problem of security without information, so that information with the help of volunteers, organizing organizations, firms, corporations and consuming pushes.

Models of information security processes in computer systems are reflected in the article. They are named so, as they allow determining (estimating) the general characteristics of these systems and processes. The main purpose of common models is to create the prerequisites for an objective assessment of the computer system general state in terms of vulnerability or security level of information in it.

Methodology. The basic means, methods and directions of the commercial information protection, modern information security problems of enterprises are studied. The essence of the information security concept, the enterprise information security is investigated. The main sources and entities of threats, methods and means for eliminating threats to information systems are classified. Necessity of creating an organizational and economic mechanism for providing the enterprise information security is proved.

The need to create different security systems was investigated, taking into account the use of mathematical models and methods of processes for protecting commercial information in the conditions of the enterprise, features and conditions of their operation. The main means, methods and directions of marketing information protection are considered. The regulation of this issue at the state level is highlighted. A system of measures for the market formation of a commercial information protection in Ukraine has been proposed. A number of threats sources to the information security of a modern enterprise are highlighted. Subjects by whom there may be a threat to the enterprise information systems are determined.

It is concluded that from the perspective and spread of the information technologies usage in everyday life, every person is increasingly faced with the need to protect commercial information, which is why the issue of information security becomes so important and relevant. It is connected to the growing capabilities of computer technology. After all, the development of tools, methods and forms of information processing automation processes make information much more vulnerable. Specialized anti-bullying software, employees monitoring programs, for example, the American company Spector Soft Corporation, is proposed to use against insiders.

The notion of “information protection” is analyzed, under which in the work of V. Pasichnyk, P. Zhezhnych, R. Kravets, A. Peleshchyshyn, D. Tarasov “Global Information Systems and Technologies: Models of Effective Analysis, Processing and Data Protection”, is understood as a set of measures to ensure the physical integrity of information, prevent unauthorized changes and data acquisition, and its characteristics are data reliability, confidentiality, integrity and information availability.

The tasks of the information system protection distributed at several levels were defined.

The purpose of the information security is to determine the system which can be provided as an organization for optimal functioning.

Results. The conclusions are that the use of information technology significantly improves the efficiency of processes, reduces the cost of their implementation, but causes new threats to the operation of the enterprise. Implementing a systemic approach to information security of an enterprise should adhere to the principles of confidentiality, integrity and availability of information, which will improve its effectiveness. Provision of information security should be considered as an integral element of the enterprise management process.