Annali d'Italia
Scientific Journal of Italy

ANNALI D'ITALIA

SCIENTIFIC JOURNAL OF ITALY

2021 (18)
VOL. 1

Annali d'Italia
Scientific Journal of Italy

ANNALI D'ITALIA

SCIENTIFIC JOURNAL OF ITALY

2021 (18)
VOL. 2

№18 2021

Annali d'Italia

VOL. 1

ISSN 3572-2436

Annali d'Italia (Italy's scientific journal) is a peer-reviewed European journal covering top themes and problems in various fields of science.

The journal offers authors the opportunity to make their research accessible to everyone, opening their work to a wider audience.

500 copies
Annali d'Italia
50134, Via Carlo Pisacane, 10, Florence, Italy
email: info@anditalia.com
site: https://www.anditalia.com/

CONTENT

BIOLOGICAL SCIENCES

ECONOMIC SCIENCES

MEDICAL SCIENCES

PHYSICAL SCIENCES

TECHNICAL SCIENCES

TECHNICAL SCIENCES

RESEARCH OF PROBLEMS OF PROTECTION OF ECONOMIC AND ENTREPRENEURIAL INFORMATION

Zelinska O.
Candidate of Technical Sciences,
Associate Professor of
the Department of Computer
Science and Economic Cybernetics,
Vinnytsia National Agrarian University
(Vinnytsia)

ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАХИСТУ ЕКОНОМІЧНОЇ ТА ПІДПРИЄМНИЦЬКОЇ ІНФОРМАЦІЇ

Зелінська О.В.
кандидат технічних наук,
доцент кафедри комп'ютерних наук
та економічної кібернетики
Вінницький національний аграрний університет
(м. Вінниця)

Abstract

The purpose of the article is to study the problems of protection of economic and entrepreneurial information, identify areas, mechanisms to improve information protection.

To achieve this goal it is necessary to solve the following separate tasks: to analyze the theoretical provisions of the basics of modeling for the purposes of information security; show the criteria and conditions for the use of functional models for information security systems.

Анотація

Метою статті є дослідження проблем захисту економічної та підприємницької інформації, визначення напрямів, механізмів для підвищення захисту інформації.

Для досягнення вказаної мети необхідно вирішити такі окремі завдання: проаналізувати теоретичні положення основ моделювання для цілей забезпечення інформаційної безпеки; показати критерії і умови застосування функціональних моделей для систем забезпечення інформаційної безпеки.

Keywords: information technologies, information security, information protection, database.
Ключові слова: інформаційні технології, інформаційна безпека, захист інформації, база даних.

The main results of the research. Nowadays, information has an extraordinary value, which can be determined not only by the amount of work spent on its creation, but also the amount of profit received from its possible implementation. The problem of modernity is the protection of information, reliable provision of preservation and establishment of the status of use. The formation of the information society has both positive and negative consequences: the transfer of significant information has accelerated, its processing and implementation has accelerated, but concerns are associated with the expansion of illegal collection and use of information, unauthorized access to information resources, illegal copying of information in electronic systems, theft of information from archives, banks and databases, violation of information processing technologies, launch of virus programs, reduction and modification of data in information systems, viewing information in the technical channels of its source, manipulation of society and individual consciousness. The transition of society to information has changed the status of information - it can be not only a means of security, but also a threat and danger.

One of the main priorities is the development of the information society and the introduction of the latest information and communication technologies in all spheres of public life. This is due to the urgency of information security of the interests of person, society and the state as a whole. For a long time, the understanding of information security in scientific and regulatory sources was identified only with information security, which significantly narrowed its essence. That is why of a number of issues devoted to the problem of information security, the most studied and researched aspects are information security (information security).

Various aspects of information security of the enterprise and improvement of its management are investigated in the works of many domestic and foreign scientists, in particular the definition of information security of the enterprise, analysis of threats and indicators of information security are covered in the works of O.F. Belova, O.I. Baranovsky, M.A. Bendikova, M.M. Yermoshenko, Y.A. Zhalila, T.T. Kovalchuk, G.V. Kozachenko, N.O. Lohanova, O.M. Lyashenko, B.I. Muntiyan, E.A. Oleynikov, S.K. Reverchuk and others.

The purpose of the article is to study the problems of protection of economic and business information,

identify areas, mechanisms for improving information protection.

Information has been valued at all times. To own it there were murders, wars. Nowadays it is of no less value. This value can be determined not only by the amount of labor spent on its creation, but also the amount of profit received from its possible implementation.

The problem of information protection: reliable provision of its preservation and establishment of the status of use - is one of the most important problems of our time.

The goals of the enterprise information protection system are:

- prevention of leakage, theft, loss, distortion, forgery of information;
- prevention of threats to the security of the individual, enterprise, society, state;
- prevention of unauthorized actions to destroy, modify, distort, copy, block information;
- prevention of other forms of illegal interference in information resources and systems, ensuring the legal regime of documented information as an object of property;
- protection of the constitutional rights of citizens to privacy and confidentiality of personal data available in information systems;
- preservation, confidentiality of documented information in accordance with the law.

An integral part of the effective functioning of any organization or institution is not only to ensure the movement of information flows, but also the proper level of their protection, which is part of information security. The most common approach to "information security" is the creation of conditions for storage, processing and transmission of information, in which the probability of leakage, modification or destruction will be minimal and will meet the requirements set by the organization. According to the Law of Ukraine "On Information" of October 2, 1992 № 2657-12 as amended, information may be open or restricted, which in turn provides for its division into confidential, secret and official information [4].

Confidential information is information that is in the possession, use or disposal of individuals or legal entities and is disseminated at their request. Individuals and legal entities that have information of professional, business, industrial, banking, commercial and other nature or which is the subject of their professional, business, industrial, banking, commercial and other interest and does not violate the secrecy provided by law, independently establish access. to it, including its belonging to the category of confidential and introduce a system and methods of its protection.

The exception is information, the concealment of which endangers human life and health. Information that contains a secret provided by law, the disclosure of which may harm a person, society or state is classified as secret.

Official information is considered to be information contained in internal organizational correspondence, memos, orders, regulations, instructions related to the development of the organization's strategy, the process of making production, personnel, financial, marketing or other decisions. In order to properly protect information and ensure information security, access to it is restricted, and a system of its protection is organized.

The latter, in turn, when using computer information systems and technologies, is implemented through organizational, legislative, physical and software and hardware. Influence on security of processes of accumulation, storage and use of the information in the organization is carried out by such factors as:

- quality of organization of paper and electronic document circulation;
- level of professional training;
- available software and hardware;
- computer technologies of information transfer organization and protection.

The requirements for information security are also significantly influenced by the competitive environment in which the organization operates, the profitability of this business segment and the size of the organization itself. These factors create potential threats to information, which can be both accidental and intentional. Accidental threats are mostly caused by the loss of information or its confidentiality due to software failure or incompetence (negligence) of the organization's staff. The occurrence of intentional threats is related to attempts to gain unauthorized access to information in order to use or destroy it.

The use of computer hardware, software, and networking technologies has greatly expanded the organization's unauthorized access to information resources, leading to a new type of crime related to industrial espionage. Features of this type of crime are related to:

- relative comfort (preparation and commission of a crime is carried out almost at the "workplace");
- availability (constant reduction in the cost of crime);
- a wide geography of possibilities of committing a crime;
- the remoteness of the object of criminal encroachment from the crime scene;
- the difficulty of identifying, recording and extracting forensic information (crime scene) in the performance of investigative actions for its use as material evidence.

Taking into account the peculiarities of crime in the information sphere and determining the factors influencing information security, organizations assess its level.

The process of ensuring information security of the organization is implemented through the interaction of three subsystems, namely:

- subsystem of information support of the management process (collection of necessary information, its processing, systematization, evaluation and analysis, transfer to decision makers);
- subsystem for protection of the internal information environment (analysis of threats to information security, planning and development of measures to ensure it);

- subsystem for diagnosing the level of information security (assessment of the effectiveness of protection of the internal information environment).

These subsystems are connected and mutually determined by software and hardware, through which technical ("electronic key", information technology, etc.) and cryptographic methods of protection are implemented. The use of a set of defined methods provides encryption of information, control of the integrity of databases and software, authentication of electronic documents and establishment of their authorship, as well as protection of programs and databases from unauthorized copying and use. Technical methods are aimed at ensuring document management and implementation of management through the use of information technology (user interface, method of building a network). The latter requires the use of various means of network protection of information: firewalls, intrusion detection systems, means of creating virtual private networks, as well as means of security analysis.

A firewall is a program or device designed to check data coming over a network. A firewall or firewall is a "firewall" between a network adapter and an operating system. Before the operating system can be processed, any IP packet undergoes strict control according to specified rules and exceptions. Intrusion Detection Systems (IDS) are used to detect and record unauthorized access attempts both externally and internally. Using special mechanisms, intrusion detection systems are able to prevent malicious actions and block a specific attacker by his IP address.

Virtual Private Network (VPN) tools are designed to organize secure data transmission channels through an insecure environment that provides transparent transmission of information on local networks, while maintaining its confidentiality and integrity through dynamic encryption. Security analysis tools provide constant analysis of corporate network security and identification of possible channels for information threats. Their use allows you to prevent possible attacks on the corporate network, optimize the cost of protecting information and monitor the current state of network security. Antivirus software is a separate means of protecting information from loss or damage, as well as misuse. Its tasks are to detect and neutralize computer viruses in order to protect information and ensure the working condition of software and hardware.

There are several types of special programs that can detect and neutralize computer viruses:

- detector programs (search for virus-specific signatures in RAM and files and issue a message when detected);

- Doctor programs (or phages) find virus-infected files and deactivate the body of the virus program.

For effective work require constant updating of anti-virus databases);

- Auditor programs (based on comparing the initial state of programs, directories and system areas of the disk, when the computer is not infected with a virus, with the current. Detected changes are displayed on the monitor screen);

- filter programs ("guards" - designed to detect suspicious actions in the computer, typical of viruses);

- vaccine programs (immunizers - modify the program or disk so that it does not affect their work, and the virus recognizes them as already infected).

Regardless of the anti-virus software used, information security tools, implemented information and communication technologies, it is important for the organization to back up information, create copies of databases.

The scheme of management of the process of information security in the stock market is presented in Fig.1.1. From a practical point of view, management is an infrastructure service (Fig. 1.1). There should be an information and telecommunication system (infrastructure service) between the electronic trading platform and the Internet, which accepts attacks, which are recorded by tester programs and submit information to the script analyzer, as well as at the same time after their reflection using the control function u (s), authorizes the electronic platform for bidding.

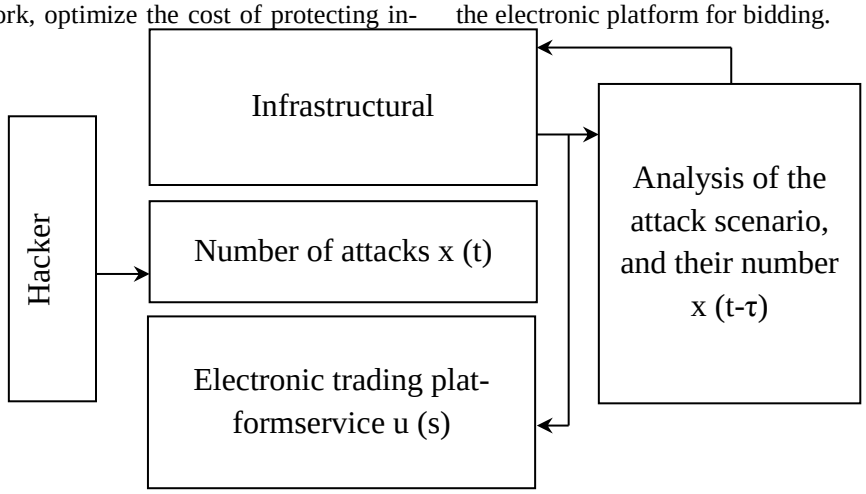


Fig. 1.1 Management of the information protection process
The source is formed on the basis of [2]

This process is continuous. The attack scenario analyzer is a framework in which the base of knowledge about attack scenarios is created and formation of new functions for counteraction for infrastructure service is carried out.

One of the main internal functional components of enterprise security is information. It consists in the implementation of effective information and analytical support of economic activity of the enterprise. Appropriate services of the enterprise perform certain functions, which together characterize the process of creating and protecting the information component of enterprise security.

These include: collection of all types of information on the activities of a business entity; analysis of the received information with obligatory observance of the generally accepted principles and methods; forecasting trends in scientific and technological, economic and political processes; assessment of the level of economic security for all components and in general; development of recommendations for raising this level at a specific business entity; other activities for the development of the information component of economic security.

The company constantly receives streams of information that differ in the sources of their formation. It is necessary to separate:

1) open official information;

2) probable non-confidential information obtained through informal contacts of the company's employees with the media of such information;

3) probable non-confidential information obtained through informal contacts of the company's employees with the media of such information. Operational implementation of measures for the development and protection of the information component of economic security is carried out by the consistent implementation of a certain set of works.

There are five areas:

1) collection of various types of necessary information;

2) processing and systematization of the received information;

3) analysis of the received information;

4) protection of the information environment of the enterprise, covering: measures to protect the business entity from industrial espionage by competitors or other legal entities and individuals; technical protection of premises, transport, negotiations, various documentation from unauthorized access of interested legal entities and individuals to confidential information; gathering information on potential initiators of industrial espionage and taking the necessary precautions to stop such attempts;

5) external information activities [5].

There is an opinion among modern entrepreneurs that using the basic rules of safety, you can achieve significant success in business. These include: intelligence; professionalism in establishing contacts (minimum time and effort to find the information needed to establish contact); manager's qualification (spending time only on the right people); ability to overcome obstacles, search for options and workarounds to solve problems; the ability to complete the operation even with a negative result (still better than no result).

Information is a means by which intelligence influences the conduct and development of any firm's policy and security, which is presented in a timely manner orally or in writing to the firm's management. Today, all commercial structures of developed countries have in their staff units that deal with information activities. In some firms it is an information-analytical department, in others - a marketing department, to which the company's management, along with others, assigns information-analytical tasks, or the commercial intelligence department.

Often it all depends on the level of understanding of the company's management of the importance of information and analytical work for the safety of all aspects of any commercial structure. The main task - collecting information:

1) about the economic condition of the company, region, country, countries in which there are partners. And the political situation in the region and the country; about the moral and psychological climate in the team;

2) about competitors and methods of competition (criminal structures and possible terrorist threats); on setting tasks for testing potential partners, customers, competitors;

3) development of programs to combat industrial espionage, terrorist threats and other methods of unfair competition;

4) development of programs for disinformation of competitors through the media, information and telecommunications channels, suppliers, associates, partners, customers by organizing the pseudo-infiltration of confidential information; development of programs for the protection of confidential information.

In fig. 1.1 shows a sample structure of the information-analytical unit [1], the task of which is information processing. The first important operation is the analysis, which serves as an additional filter that rejects unnecessary and that is protection against noise without reason. This operation is to determine the importance, accuracy and significance of information. Information is important if it is related, that is, related to the elements of the database, and if it is able to contribute to the organization. When the contribution is significant and direct, the information requires urgent action. Irrelevant information should be excluded to avoid wasting time and energy. It is not always easy to determine whether information is true or false, especially if it contains information about events that have not yet occurred. There are two criteria by which you can judge the accuracy of the information, the reliability of the source and the information itself.

The main criterion of plausibility is to seek confirmation from other sources, if possible - from an independent one. Information can be important and accurate and at the same time useless because it is insufficient to understand and act. Business intelligence refers to data about the environment and competitors analyzed in order to use them in a specific situation. Neither an individual nor an organization can operate effectively in a competitive environment without a deep understanding of the environment or without up-to-date information

about what is happening in it. The type of information required depends on the type of company, its competitive environment and many other characteristics of the firm and its environment.

Today, almost all Ukrainian business to one degree or another has shadowy sides: tax evasion, double-entry bookkeeping, keeping the actual volume of supplies, non-cash transactions through one-day firms, and others. In such a situation, the firm may become hostage to a criminal entity that takes control of the firm and may use it to launder its own illegally obtained funds. Therefore, it is necessary to constantly have information about the ratio of forces and the division of spheres of influence in the region in which the firm is located, in the market niche occupied by the firm [2].

The need for information varies depending on the activities carried out or planned. The company can have long-term (strategic) plans, tactical or short-term, plans and current operations, all of which require well-verified information. Today, the vast majority of business information can be obtained from open sources without violating ethical standards. The security system of each enterprise is completely individual. Its completeness and effectiveness depend on the existing legal framework in the country, on the amount of material, technical and financial resources allocated by the heads of enterprises, on the understanding of employees of the importance of business security. Reliable protection of information security of the enterprise is possible only with a comprehensive and systematic approach to its organization, so there is such a thing as "information security system of the enterprise".

The information security system of the enterprise is a set of organizational and managerial, technical, preventive measures aimed at the quantitative implementation of the protection of the interests of the enterprise from external and internal threats. For the leaders of any enterprise, taking care of its safety is the most important duty, because in the event of its collapse, there will be nothing to manage. It is necessary to closely monitor not only the processes that take place in the environment, but also no less attention should be paid to the analysis of the system itself.

It is mandatory to quickly assess the quality of work, constant verification of the input information, the reliability of all elements of the system. Any enterprise, having development goals, performs the functions of providing consumers with its services or products. Information security is a characteristic that is based on the relationship between the system and the environment, both external and internal [4].

Information security of the enterprise should be assessed taking into account the conditions, restrictions and criteria of all major participants in its production and economic activities, namely: the state, competitors, consumers.

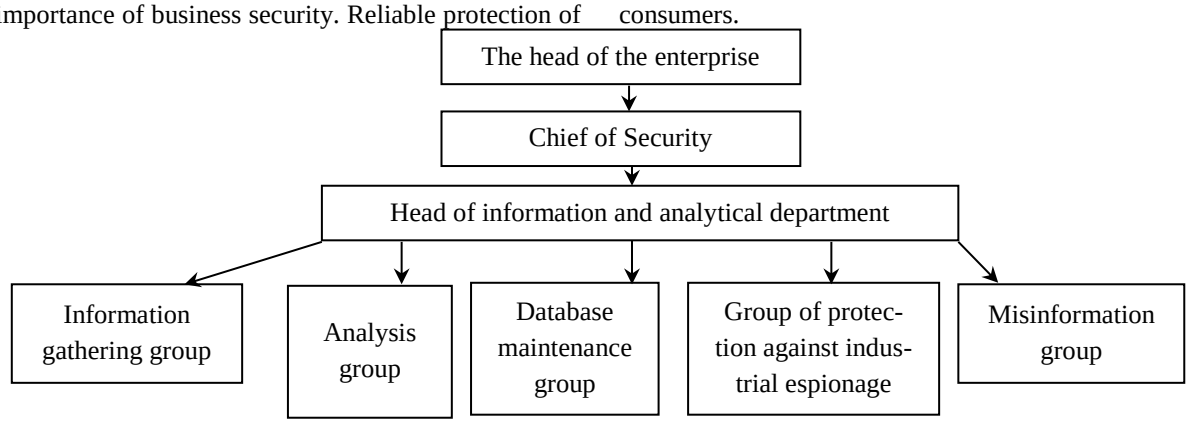


Fig. 1.2. Sample structure of information-analytical unit

The source is formed on the basis of [4]

From all the above we can conclude that for Ukrainian enterprises the most significant problems of the current stage of reforms are:

- lack of funds for technical re-equipment;
- irregular work;
- lack of contracts, orders;
- unemployment;
- large receivables.

The following steps can be proposed to strengthen the information security of Ukrainian enterprises:

- change of the system of remuneration of personnel; creation of new organizational and production structures;
- active participation in international exhibitions, seminars;
- within the framework of resource security - improvement of the settlement system; increase labor productivity;
- increase investment in resource conservation; stimulation of the "resource" direction;
- within the framework of economic security - application of the principle of observance of critical terms of crediting.

The main purpose of information security management is to ensure the most efficient operation, the most productive operation of the operating system and economic use of resources, ensuring a certain level of staff life and quality of business processes, as well as constant stimulation of existing capacity and its stable development [4]. Based on the analysis of the accumulated empirical material, it is possible to make generalizations at the level of theoretical principles of information security organization as a function. The organization of security is conditionally divided into three levels.

The division is based on such a method as sections of the environment in which the information is:

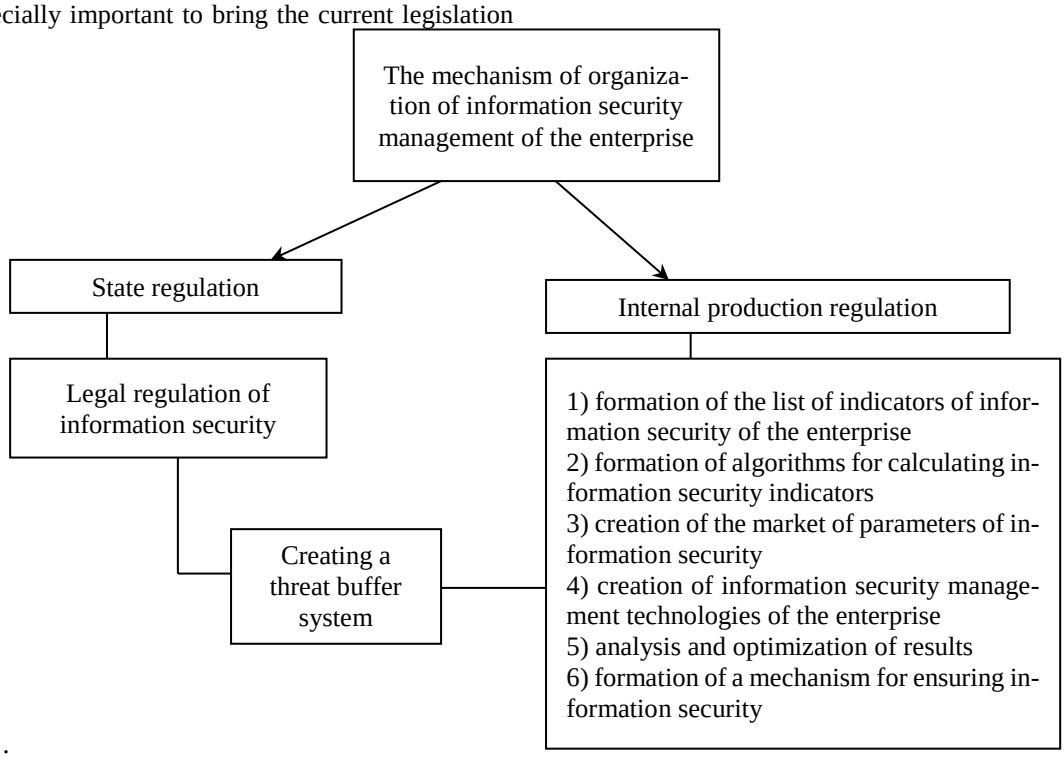
1) social (individual, community of people, state, international community);

2) engineering-technical-logical (machine, hardware-software, automatic);

3) socio-technical (human-machine).

In theory and practice, there are three groups: active means of protection (intelligence, misinformation, etc.); passive means (installation of screens against unauthorized leakage of information, etc.); a set of support tools - an organic combination of the previously mentioned groups for modeling potential (previously unknown in practice) threats.

Information security in the modern world, in which the main product is information, in which this or that information influences the state's tactical and strategic decisions, is the basis of national security. For Ukraine, which aspires to the European Community, it is especially important to bring the current legislation into line with European standards, which provides for the adoption of new laws, improvement and refinement of existing ones. There is also a need to establish a coordination commission on regulatory and legal support of information security of Ukraine, which would be an accumulator of proposals of various public authorities and public organizations in the development of information policy for Ukraine. It is worth noting that Ukraine needs a law "On Information Security", which would regulate public relations in the field of information security, given that information is organized spontaneously, not through regulation by the state, that restrictions on the dissemination of information, even to ensure national security, causes a slowdown in society



.

Fig.1.3. Organization of information security management of the enterprise
The source is based on [7]

This law should define the methods and means of protecting the vital interests of the individual, society, state in the information sphere, outline the principles for the formation of state information security policy, the development of the country's information space.

Information security support is a set of organizational, legal and engineering-technological measures to preserve, protect and defend the vital interests of the subjects of information activities. The concept and essence of information security in the context of informatization of Ukraine as a social phenomenon can be defined as follows: information security in the context of informatization of Ukraine - is public relations to create and maintain the proper functioning of the automated information system (including telecommunications systems); a set of organizational, legal and engineering-technological measures to support, prevent and overcome natural, man-made and sociogenic threats that can disrupt the life of a particular socio-technical information system. Accordingly, these formulations can be adapted to a specific area of public relations, including business.

Список літератури

1. Рабчун Д.І. «Оцінка ефективності інформаційної безпеки з урахуванням економічних показників». Сучасний захист інформації. №4. 2015. С. 91-96

2. Глушак В. В., Новіков О. М. «Метод проектування систем захисту інформації з використанням детермінованої гри „захисник-зловмисник“» Наукові вісті НТУУ «КПІ». №2. 2011. С. 46-53

3. Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В.О. Нормативно-правовий довідник з охорони інформації в Україні. Київ. Україна: ДУІКТ. 2010.

4. Про інформацію: Закон України Відомості Верховної Ради України (ВВР). 1992. № 48. ст. 650

5. Денисюк В.О. Програмна реалізація стеганографічного алгоритму захисту інформації. Ефективна економіка. 2018. № 4. Режим доступу до журналу : http://www.economy.nayka.com.ua

6. Медведєв М. Г., Пащенко І. О. Теорія ймовірностей та математична статистика. Київ. Ліра-К. 2008.

7. Левченко Є. Г., Рабчун А. О. «Оптимізаційні задачі менеджменту інформаційної безпеки». Сучасний захист інформації. №1 (1). 2010. С. 16-22

8. Platzer A. Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics, USA, Springer, 2010. DOI: 10.1007/978-3-642-14509-4.

9. Moore T., Pym D., Ioannidis C. Economics of Information Security and Privacy, US, Springer, 2010. DOI: 10.1007/978-1-4419-6967-5.

10. Зелінська О. В., Волонтир Л. О. Інформаційно-логістичні системи управління аграрним підприємством. Економіка. Фінанси. Менеджмент: актуальні питання науки і практики. 2018. № 12. 88-96 с.

11. Зелінська О. В., Потапова Н. А., Волонтир Л. О. Інформаційні системи та технології в галузі: навч. посіб. Вінниця: ВНАУ. 2020. 253 с.

References

1. Rabchun D.I. «Otsinka efektyvnosti informatsiinoi bezpeky z urakhuvanniam ekonomichnykh pokaznykiv». Suchasnyi zakhyst informatsii. №4. 2015. S. 91-96

2. Hlushak V. V., Novikov O. M. «Metod proektuvannia system zakhystu informatsii z vykorystanniam determinovanoi hry „zakhysnykzlovmysnyk"» Naukovi visti NTUU «KPI». №2. 2011. S. 46-53

3. Artemov V. Yu., Lienkov O. S., Pashkov A. S., Stadnik O. M., Khoroshko V.O. Normatyvnopravovyi dovidnyk z okhorony informatsii v Ukraini. Kyiv. Ukraina: DUIKT. 2010.

4. Pro informatsiiu: Zakon Ukrainy Vidomosti Verkhovnoi Rady Ukrainy (VVR). 1992. № 48. st. 650

5. Denysiuk V.O. Prohramna realizatsiia stehanohrafichnoho alhorytmu zakhystu informatsii. Efektyvna ekonomika. 2018. № 4. Rezhym dostupu do zhurnalu : http://www.economy.nayka.com.ua

6. Medvediev M. H., Pashchenko I. O. Teoriia ymovirnostei ta matematychna statystyka. Kyiv. Lira-K. 2008.

7. Levchenko Ye. H., Rabchun A. O. «Optymizatsiini zadachi menedzhmentu informatsiinoi bezpeky». Suchasnyi zakhyst informatsii. №1 (1). 2010. S. 16-22

8. Platzer A. Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics, USA, Springer, 2010. DOI: 10.1007/978-3-642-14509-4.

9. Moore T., Pym D., Ioannidis C. Economics of Information Security and Privacy, US, Springer, 2010. DOI: 10.1007/978-1-4419-6967-5.

10. Zelinska O. V., Volontyr L. O. Informatsiinolohistychni systemy upravlinnia ahrarnym pidpryiemstvom. Ekonomika. Finansy. Menedzhment: aktualni pytannia nauky i praktyky. 2018. № 12. 88-96 s.

11. Zelinska O. V., Potapova N. A., Volontyr L. O. Informatsiini systemy ta tekhnolohii v haluzi: navch. posib. Vinnytsia: VNAU. 2020. 253 s.

№18 2021

Annali d'Italia

VOL. 1

ISSN 3572-2436

The journal is registered and published in Italy.
Articles are accepted each month.
Frequency: 12 issues per year.
Format - A4 All articles are reviewed
Free access to the electronic version of journal

500 copies

Annali d'Italia

50134, Via Carlo Pisacane, 10, Florence, Italy

email: info@anditalia.com

site: https://www.anditalia.com/