

## **Leontij Hryhorowycz Czystokletow**

### **THREATS TO INFORMATION SECURITY IN THE AREA OF ADMINISTRATIVE AND LEGAL SECURITY OF BUSSINES ENTITIES IN UKRAINE**

#### **Abstract**

Based on the theoretical and practical aspects, studied was most pressing issues related to information security threats in the area of administrative and legal security of business entities in Ukraine. Classification of threats and the concept of administrative and legal information security entities was formulated.

#### **Keywords**

information security, business security, administrative and legal support, security threats activities.

#### **Defining the problem**

Taking into account importance and significance, which humanity draw from the informational field, current political, economic and social development of our society mostly depends on qualitative, reliable and efficient obtaining information in order to make numerous important decisions that are being made on different levels – starting with the Verkhovna Rada of Ukraine to an ordinary citizen. Immense flows of information literally flood the people. Scientific knowledge, according to expert assessments, doubles every five years. What was said above finds its confirmation in fact, that according to data of world's internet statistic, Europe has more than 476 million of Internet users, what accounts for 58,3% of the people in continent and 22,7% users in the whole world. In the period 2000-2011 the numbers of Internet users worldwide has increased almost three and a half times, what means that in June 2011 the number of them reached 353,1% of amount from 2000. The most powerful Internet using countries

are: Germany, Russia, Great Britain, Turkey. Ukraine locates on 9<sup>th</sup> position having more than 15 million of users [1].

### **Analysis of publications on which the article is based**

One needs to notice that enough attention has not been paid to solving the issues related to searching effective ways of counteracting the threats to information security in area of administrative and legal security of activity of business entities in Ukraine as to a separate field of scientific researches. Particular attention was drawn to works of such scholars as: R. B. Tarasenko, W. A. Łużecy, O. P. Wojtowicz, A. D. Kożuchiwskyj, L. I. Seweryn, I. B. Trehubenko, O. I. Motlach, R. A. Kalużnyj, W. S. Cymbaliuk and others.

### **The aim of the research**

On the basis of issues mentioned above and a short analysis of scientific sources, which relates to the subject, this article aims to theoretically substantiate of scientific position on nature and elements of emerging threats that negatively influences the information security in the area of administrative and legal ensuring the security of activity of business entities.

### **The basic content of the study**

Analyzing problems of administrative and legal ensuring the security of activity of business entities, one needs to focus on such important aspect, as Information Security (further IS). For it is the source of violation of IS.

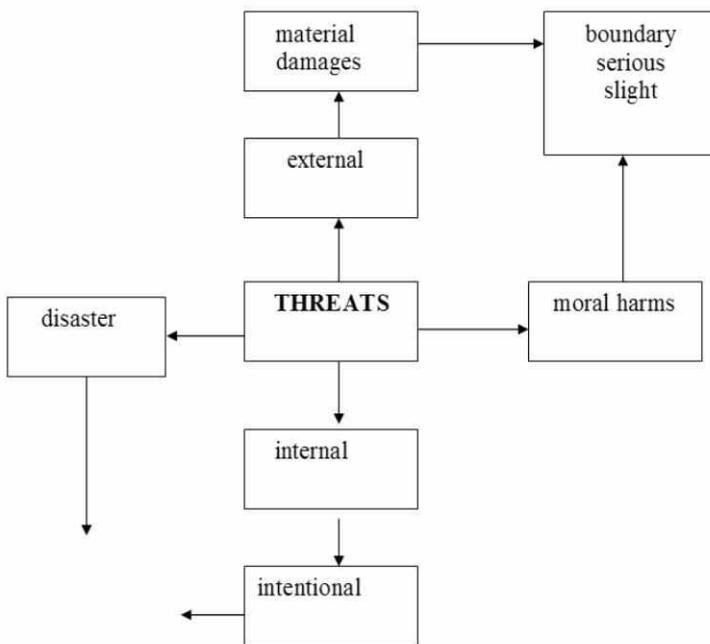
R. B. Tarasenko defines information security threats as a set of conditions and factors that poses danger to underlying interests of an individual, a society, and a state in an informational sphere [2]. In our opinion a concept of informational security threat is to be considered a potentially possible occurrence, act, process or phenomenon that may lead to violation of confidentiality of information, as well as unjustified settling of effort. Usually threats indicates presence of gaps, that is weak points of IS.

However, it is not always the case. For example threats of disruptions in supply of electricity or disconnecting the current, exist due to the dependence of the technology on the power supply.

Ensuring availability, integrity and confidentiality of information sources is one of the main conditions of efficient functioning of a contemporary organization. Such sources includes: contract and agreements; information of financial and technical character; information about new projects and business plans; information about employees; information about intangible assets; accounting calculation data; information about current activity of an organization.

All such information are mostly stored and processed by automated informational systems, so an outcome of enterprises activity highly depends on stability and security of these systems and actions of their competitors, rivals. Diversification and penetration of new markets, searching for new clients and suppliers, creating new units lead to more complex structures of an organization, which requires improvement of an informational system using new informational technology. But along with building a modern, automated system, the probability of threats of different kinds, which aims to undermine the IS of an enterprise, increases. Threats of IS are usually targeted to undermine entirety, confidentiality, and availability of information. An effect of these threats may be leak, divulgation, distortion (modification) or destruction of an information. At picture 1 presented was the classification of administrative and legal threats to ensuring the informational security of activity of business entities, in accordance with the following criteria:

- source of threats (internal and external);
- character of suffered damage (threats, which cause material or moral harm);
- probability of occurrence;
- causes of rising.



**Pic. 1** Types of threats to administrative and legal ensuring the informational security of activity of entities

Source: elaborated by the author.

*External threats* includes:

- industrial espionage;
- attacks on security system with the intention of stealing, destroying, modifying the information;
- lack of a sufficient number of certified resources of information security on the market;
- imperfection of existing normative and legal base of administrative and legal ensuring the IS;
- activity of dishonest partners and clients.

*Internal threats* includes:

- imperfection of information security systems used;

- obsolete software and means for storing and processing data;
- low qualifications of employees;
- using “pirated” software;
- sabotaging personnel;
- insufficient fire and technical safety of rooms and buildings of an organization.

To internal information threats may be also included subversive activities of competing organizations, which is the enlistment of agents in order to further disorganization of competitor, revenge of employees which are dissatisfied with their salary or with their status in the firm, and other. We hold that in order to minimalizing the risk of such occurrences it is necessary that every employee of an organization is to fulfill the so-called “status of trustworthiness”.

At the same time W. Łużeckyj, O. Wojtowicz, A. Kozuchiwskyj, L. Seweryn, I. Trehubenko claim that every year there is a significant increase of more sophisticated, universal and complicated virus programs, which causes serious damages for both corporate and home users [3].

Usually there are two types of information that requires security and are included in category of confidential information or trading information:

- scientific and technical information that are directly connected with technical documentation and documentation of projects, information about used materials, and description of methods and technics of producing new wares, unique software;
- information, which includes official messages about activity of an organization: financial documentation, plans of future development, directions of modernization of the production, analytical materials of researching the competitors and effectiveness of work on the commodity and services market, information of partners etc.

These two types of information are predominatingly the objects of a computer crimes [4, p. 42]. We notice, that professor R. Kalužnyj has yet in 1992 emphasized a prominent role of computer computational technology in work of organs of internal affairs [5, p. 3].

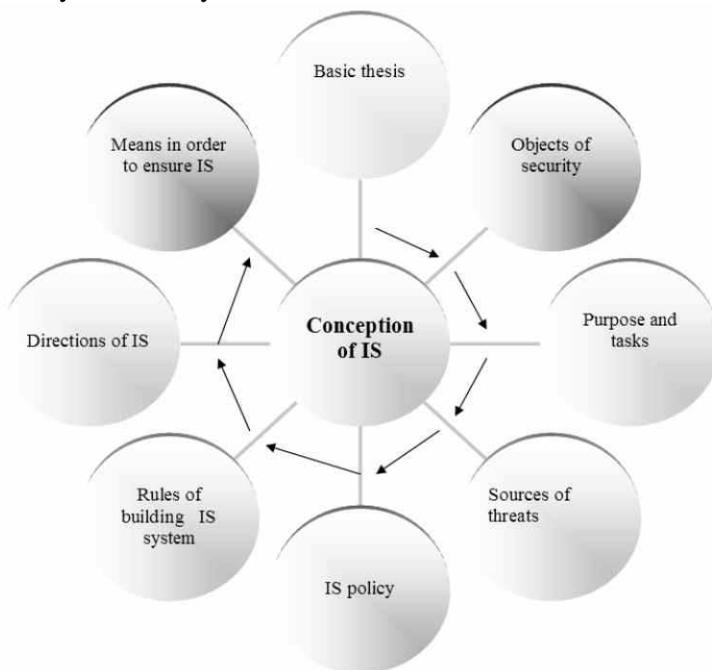
Based on the above, we think, that basic tasks of administrative and legal ensuring IS of any business entity are: creating stabile, efficient trading and productive activity of all units, protection against loss, theft, distortion or destruction of confidential information and trade secrets, embezzlement of costs, prevention of security threats. The IS system is necessary also for improvement of services quality, and security guarantee of an ownership rights, and an interests of clients.

To achieve this goal, above all necessary is:

- categorization of information into confidential information and trade secrets;
- forecasting and early detection of informational security threats, causes and contracts, which may cause financial, material and moral damages;
- creation of such conditions of activity, with the lowest risk of realization of threats to security of information resources, and of causing damages of different kind;
- creation of mechanism and contracts for effective reaction to IS threats, based on legal, organizational and technical means.

Constant increase of rate of development and spread of informational technologies, high competition an current situation of delinquency makes an information the most attractive, because its confidentiality is being determined with conditions of access and is limited to the number of people, who has right to its possession [6, s. 88–91]. Mentioned remarks define the priority issues related to creation in the enterprise a homogenous *system of administrative and legal ensuring of information security of activity of business entities*. IS system of entity, in our opinion, should contain legal, informational and analytical, organizational, physical, engineering and technical, as well as programmatic

means of ensuring security of informational resources. For a full assessments of the situation in the enterprise, in regard to all directions of ensuring IS, in our opinion, it is necessary to elaborate the *Conception of administrative and legal ensuring of informational security of entities* (further also – Conception) (pic. 2), which brings in the systematical approach to the issue of security of information resources and which is a systematized lecture of purposes, tasks, rules of projecting, and a complex of means related to administrative and legal ensuring information security of an entity.



**Pic. 2** Components of conception of administrative and legal ensuring information security of entity.

Source: elaborated by the author.

While elaborating the conception under account must be taken are contemporary organizational and legal methods, and

programmatic and technical measures to prevent external and internal IS threats, as well as the current state of information security and perspectives of development of informational technologies.

Basic rules and needs of the Conception of IS should apply to all employees of an enterprise, who are in any way associated to elaborating, storing, conserving or creating informational resources, which requires protection of its unity, confidentiality and availability, and to other persons from other organizations, who are responsible for actualization and support of software.

The Conception should serve as a basis for:

- creating a uniform policy of ensuring IS in an enterprise;
- coordinating the activity of structural units of an enterprise in order to ensure IS;
- making decisions and undertakings, aimed to prevent, detect and eliminate effects of various IS threats;
- searching for new decisions aimed to improve the ensuring of IS.

## **Conclusions**

As a general scientific category, security can be define, when it is able to withstand the impact of external and internal threats, and when functioning of a whole system does not threaten elements of this system and the external environment.

Taking into account what has been said above, from the position of administrative and legal ensuring security of activity of business entities, information security is the state of informational system, in which it can withstand the internal and external threats without initiating creation of elements of the system and the external environment.

On basis of this, it has to be noticed, that a base for ensuring IS is solution of three problems that are connected with each other: problem of securing information, which is in the system, against the impact of external and internal threats, problem of securing an information against informational threats; problem of

protecting the external and internal environment against the threats of an information, which is in the system.

While examining the basic principles of creating the conception of administrative and legal ensuring of security information of business entities, in our opinion, the most important one of creating this conception is its purposefulness, because lack of purposefulness thwarts other steps of creating the IS system. In order to define an adequate level of protection of informational resources, it is particularly important to examine in the methodological elements of the organizational protection of IS enterprise, that is the content and properties of informational resource at the background of evident threats.

### **References:**

1. Cymbaliuk W. S., *Informational Security of Activity of Businessmen: Determining the Nature and Essence of a Concept and Agreements of Ukraine's Entering to the Informational Society (Global Cybercivilizations)*, Enterprise, Economy and Law, 2007, no. 3, p. 88-91.
2. Internet World Stats, [an electronic resource] available at: <http://www.internetworldstats.com/stats4.htm#europe>
3. Kaluznyj R. A., *Theoretical and practical problems associated with using computers in the system of internal affairs authorities (legal and organizational aspect)*, lecture of PhD dissertation, Kyiv 1992, p. 23, p. 3.
4. Łużeckyj W. A. , Wojtowicz O. P. , Kozuchiwskyj A. D. , Seweryn L. I. , Trehubenko I. B., *Basis of Informational Security*, Cherkasy 2008 [CD-ROM — (Series “Information security”)].
5. Motlach O. I., *Methods of Examining the Computer Crimes: Monography*, Kyiv 2010 p. 42, p. 296.
6. Tarasenko R. B. *Informational Law: Teaching Guide / MIA of the Ukraine*, The Luhansk State University of Internal Affairs named after E. O. Didorenko, 2010 p. 512, [an electronic resource] available at:

<http://www.ukr.vipreshebnik.ru/2012-06-25-18-22-00/563-2011-06-18-18-00-40.html>