Olena A. Sorokivska[1]

ECONOMIC SECURITY OF UKRAINIAN ENTERPRISES UNDER INFORMATION WAR

The article investigates the factors of information aggression, its occurrence and influence on the economic security of enterprises, specifying the notion of information security of an enterprise and summarizing the types of information aggression and factors of its impact on business entities. Consequences of information war in Ukraine are also described.

Keywords: *enterprise economic security; information security; information aggression; information war.*

Олена А. Сороківська

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

У статті досліджено фактори прояву інформаційної агресії та її вплив на економічну безпеку підприємств, уточнено поняття інформаційної безпеки підприємства, систематизовано види інформаційної агресії та чинники її впливу на розвиток суб'єктів господарювання, розглянуто наслідки інформаційної війни в Україні.

Ключові слова: *економічна безпека підприємства; інформаційна безпека; інформаційна агресія; інформаційна війна.*

Літ. 11.

Елена А. Сорокивская

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ УКРАИНЫ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

В статье исследованы факторы проявления информационной агрессии и ее влияние на экономическую безопасность предприятий, уточнено понятие информационной безопасности предприятия, систематизированы виды информационной агрессии и факторы ее влияния на развитие субъектов хозяйствования, рассмотрены последствия информационной войны в Украине.

Ключевые слова: *экономическая безопасность предприятия; информационная безопасность; информационная агрессия; информационная война.*

Problem statement. Economic functioning of Ukrainian enterprises is rather challenged today due to the country being involved in "hybrid war". The problem aspects of such a war as well as its influence on the activity of various business entities may be analyzed on different levels. The parameters of economic equity and possibilities of domestic enterprise development are to a considerable extent dependent on information and communication conditions of economic reality.

Nowadays, it proves to be quite difficult to define the very border where the war starts and finishes. Analyzing the contents and the role of information in today's world, the American researcher M. McLuhan (1967) suggests an interesting statement: "Real total war has become information war". M. McLuhan (1967) was the first to emphasize the fact that economic relations and affairs are becoming more and more similar to the process of exchanging knowledge rather than goods. Mass media communication means are becoming the new "natural resources" contributing to social wealth. Therefore, the struggle for money capital, sales markets etc. are becom-

[1] Ternopil Ivan Puluj National Technical University, Ukraine.

ing less important than access to information and knowledge. Thus, wars are led in information space and by means of information weapons.

The ambiguity of the word "warfare" that may be interpreted as either war, or struggle has stipulated the need to make use of such words as "information war" and "information struggle". The latter is wide-spread in Russia where it has come to mean "competition of social systems in information and psychological spheres regarding certain areas of social relations and establishment of control over strategic resources, and leading to some competitors getting benefits necessary for their further development and others losing them" (Manoilo et al., 2003).

Information wars have acquired paramount importance during the XXth century when newspapers, radio and later television became real information media and the information they spread became mass information. In the 1920s different countries started to air their radio shows on the territories of their "traditional interests". Thus, the USA had radio broadcasting in Latin America countries, Great Britain – on the territories of its colonies, and Germany (fighting for reconsideration of the Treaty of Versailles) – on the territories of Germans in Pomerania and Upper Silesia in Poland, as well as the Sudetes in Czech Republic. In the 1930s, information wars ceased to be a mere supplement to the armed ones, and became an independent phenomenon instead. An example may be given: the German-Austrian radio war of 1933–1934 concerning the issue of including Austria into Reich. It was the time when the term "information space" was born.

Recent research and publications analysis. Information war as a social and philosophical problem stirred interest as early as the mid of XX cent. This issue was referred to by A. Toffler (2000), F. Fukuyama (2002), P. Lazarsfeld (1968), H. Lasswell and B. Smith (1946), H. Lasswell (1950), H. Pocheptsov (2001). The contribution of the latter is of considerable importance as his ideas were presented not only as scientific research, but also as information of publicistic texts for vast audience. H.H. Pocheptsov (2001) defines information war as a communication technology of influence on collective consciousness with the aim of changing cognitive structure to control the changes of people's behavior.

The research goals. The main goal of this research is to define the factors and level of information war influence on the level of economic security of domestic enterprises.

Key research findings. Nowadays, information war has changed the environment of domestic enterprises' activities. These changes are primarily related to two major aspects of economic security of business entities:

1) collecting, classifying and processing necessary information about the environment (competitors, suppliers, consumers, political, economic factors, as well as legal environment);

2) protecting own information from various market counteragents.

Speaking about the first aspect, it should be noted that few Ukrainian enterprises are able to precisely determine the exact type of information they need, organize its efficient search, avoid disinformation, and make good use of information obtained when making decisions and arranging current control of financial and economic activity. The enterprise management often perceives information resources as the secondary type of resources giving priority to material basis of enterprises. However,

non-material resources of enterprises are the ones under attack in the era of information war.

The notion of information war is defined by domestic scholars as a type of information struggle between different subjects (states, non-governmental, economic and other organizations) with a set of activities aimed at harming information sphere of the opposite party and protecting own information security (Petryk, 2011).

It should be mentioned that according to the resource-functional approach, enterprise economic security calls for a mechanism of appropriate control of its material, information, personnel, and technological resources with the aim of their effective use and active resistance against any negative influence.

Using this approach, we may define the term of information security and determine this category as such a level of its protection that does not let information operations, acts of external information aggression, information terrorism, illegal access to information via special technical means, computer crimes and other destructive information influence cause serious damage to the enterprise.

The notion of information security is closely linked to the categories of "information aggression" and "information attack". We suggest the following definition of information aggression: it is a complex of legal and (or) illegal activities the implementation of which may have negative impact on the security of information space of a business entity. Information attack may be defined as a set of legal and (or) illegal actions employed to obtain secret information resources of the enterprise or aimed at spreading disinformation on this enterprise activity.

In recent years information aggression has become more thought-out and vast. It is stipulated by a few factors:

- inadequacy of current legislation, corruption of both executive and judicial authorities;
- instability of political situation and redistribution of property between financial and industrial groups;
- import of espionage technologies and capital from Russian Federation where they can no longer be useful owing to improvement in legislation.

According to experts assessments, about 35–50 professional raider groups are functioning on the territory of Ukraine today. They create conditions for information attacks, intrusion and redistribution of property beyond the law. 3.7 ths entrepreneurs have become victims of information attacks in Ukraine so far. The annual raider redistribution of property reaches the average of 2–3 bln USD (Varnalii and Mazur, 2007).

The following are among the most wide-spread information aggressors:

- oligarchs, as well as financial and industrial groups merging companies and their assets for developing own business or diversifying the existing business empires and creating new holdings;
- investment companies merging other companies via own business (later companies and their assets are sold to interested parties at high prices or left in own business);
- investment factoring companies acting on behalf of a sponsor.

The market of raider companies in Ukraine includes numerous medium and small law firms that have:

- the department of collecting and analyzing information;
- the law department;
- the department of hostile takeover (raiders).

The task of the first two departments lies in collecting a large amount of compromising information. Lawyers thoroughly analyze the documents they receive and develop legal strategies on the actions regarding the "victim" company.

The department working on hostile takeover projects uses the above-mentioned departments work and develops its own strategy. The absence of necessary information and compromising materials poses a serious obstacle and may even lead to refusal from the initial intentions. Thus, information privacy and current legislation awareness may reduce the number of potential aggressors and protect the company.

So, the major factors of information aggression in Ukraine are the following:

- weakness of the legal system;
- incompleteness of the judicial authority;
- corruption;
- absence of state-based institutes to provide effective protection of owners' rights;
- low level of legal culture;
- legal nihilism of both entrepreneurs and authority representatives;
- ambiguous privatization results.

The level of information attacks in Ukraine and their large scope are demonstrated by the following facts:

- at least 40–50 specialized raider groups actively engaged in collecting and processing information on strategic enterprises conduct their activity in Ukraine;
- information attacks are the system problem for Ukraine. The number of seizures of domestic enterprises annually reaches 3000. An information attack precedes every seizure;
- the efficiency of information attacks is over 90%;
- according to expert evaluations, the annual merging figure (without privatization) is over 3 bln USD;
- according to expert evaluations, the raider's average income rate in Ukraine is about 1000%. Therefore, the costs of information resources are significant (Varnalii and Mazur, 2007);
- the next stage of an information attack is illegal actions involving armed units or even employees of law enforcement agencies etc.

Some powerful industrial and financial groups of Ukraine sometimes resort to ordering and organizing information attacks leading to property redistribution. According to the survey of The Centre for Researching Corporate Relations (2014), "Pryvat" business group is regarded as the biggest Ukrainian raider by 100% experts, "Finance and Credit Group" – by 54.6%, and "Alfa-Group" – by 45.5%.

The main negative consequences of the information war in Ukraine are:

- negative influence on entrepreneurial climate;
- destabilization of domestic enterprises;
- ruining staff structures at enterprises and causing social conflicts;
- unfavourable investment climate and poor international image of the entire country etc.

Given the abovementioned facts, the necessity for establishing a special structural subdivision at enterprises is obvious. This subdivision would have the functions of an information centre with the task of collecting, processing and analyzing information enabling company's directors make reasonable and sensible decisions. A subdivision (service) of economic investigation may become such a structural unit for Ukrainian enterprises.

The main goals of such a subdivision would be the following ones:

- timely provide managers with complete and reliable information on the external environment of the enterprise; to determine the factors of risks;
- effectively organize information work excluding functions duplication by other subdivisions;
- work on both short- and long-term predictions of environmental influence on the economic activity of the enterprise; develop recommendations concerning the localization and neutralization of risks;
- enhance the favorable and reduce the unfavorable influence of the environment on the economic activity of the enterprise;
- search for new ideas, technological innovations, methods etc. to be implemented at the enterprise to make it more competitive.

Such a subdivision would provide timely development of preventative measures for protecting information resources and avoiding information and raider attacks.

Conclusions and prospects for further research. The findings of this research demonstrate that the main reasons of information attacks on domestic enterprises are the following ones: seizing their material resources, harming their image and financial status, getting control over financial resources. Further research may lie in finding the ways to solve the problem of raider attacks and illegal seizure of material and non-material resources of domestic enterprises.

References:

Варналій З.П., Мазур І.І. Рейдерство в Україні: передумови та шляхи подолання // Стратегічні пріоритети.– 2007.– №2. – С. 131–136.

Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны: Монография. – М.: Горячая линия – Телеком, 2003. – 541 с.

Петрик В. Сутність інформаційної безпеки держави, суспільства та особи // Юридичний журнал.– 2011 // www.justinian.com.ua.

Почепцов Г.Г. Теория комуникаций. – М.: Ваклер, 2001. – 418 с.

Результати експертного опитування «Центру дослідження корпоративних відносин», 2014 // www.corporativ.info.

Тоффлер Е. Третя хвиля. – К.: Всесвіт, 2000. – 480 с.

Fukuyama, F. (2002). Our PostHuman Future: Consequences of the Biotechnology revolution. International Creative Management, Inc. 349 p.

Lasswell, H.D. (1950). World Politics and Personal Insecurity. The Free Press. 238 p.

Lasswell, H.D., Smith, B.L. (1946). Propaganda, Communication and Public Opinion Hardcover. 1st ed. Princeton University Press. 435 p.

Lazarsfeld, P. (1968). An episode in the history of social research. In: Perspectives in American history. 272 p.

McLuhan, M. (1967). Hot & Cool. Signet Books. NY: The New American Library Inc. 286 p.

Стаття надійшла до редакції 22.06.2015.