Olena A. Sorokivska

ECONOMIC SECURITY OF UKRAINIAN ENTERPRISES IN CONDITIONS OF INFORMATION WAR

Annotation

The article investigates the factors of information aggression, its occurrence and influence on the economic security of enterprises, specifies the notion of information security of an enterprise, summarizes all types of information aggression and factors of its impact on entrepreneurs, as well as deals with the consequences of information war in Ukraine.

Keywords: economic security of enterprise, information security, information aggression, information war, raider attack

Олена А. Сороківська

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Анотація

У статті досліджено фактори прояву інформаційної агресії та її влив 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, рейдерська атака.

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, рейдерская атака.

Setting of a problem and its connection with significant scientific and practical tasks. The economic functioning of Ukrainian enterprises is rather challenged today due to the country being involved in the hybrid war. The problem aspects of such a war as well as its influence on the activity of entrepreneurs may be analyzed on different levels. The parameters of the economic equity and possibilities of domestic enterprise development are to a considerable extent dependent on the information and communication conditions of their economic reality.

Nowadays, it proves to be quite difficult to define the very border where the war starts and finishes. Analyzing the content and role of information in the modern world, the American researcher M. McLuhan (1967) suggests an interesting thesis statement, “Real total war has become information war”. M. McLuhan (1967) was the first to emphasize on the fact that economic relations and affairs are becoming more and more similar to the process of exchanging knowledge rather than goods. The mass media communication means are becoming the new “natural resources” contributing to the social wealth. Therefore, the struggle for money capital, sales markets and etc. are becoming less important than access to information resource and knowledge. Thus, wars are led in information space and by means of information weapon.

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 second term is wide-spread in Russia where it has come to mean "the 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, Petrenko, Frolov, 2003).

Information wars have acquired paramount importance during XX century when newspapers, radio and later television became real information media and the information they spread became mass information. In 20-s 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 the Czech Republic. In 30-s, information wars ceased to be a mere supplement to armed ones, and became an independent phenomenon instead. An example may be given: the German-Austrian radio war of 1933-34 concerning the issue of including Austria into Reich. It was the time when the term "information space" was born.

Analysis of recent relevant research and publications. The information war as a social and philosophical problem stirred interest as early as the mid XX. This issue was referred to by A. Toffler (2000), F. Fukuyama (2002), P. Lazarsfeld (1968), H. Lasswell (1946, 1950), and H. Pocheptsov (2001). The contribution of the last one 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 the information was as a communication technology of influence on the collective consciousness with the aim of changing cognitive structure in order 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 was influence on the level of the economic security of domestic enterprises.

Key research findings and their reasoning. Nowadays, the information war has changed the environment of domestic enterprises activity. These changes are primarily related to two major aspects of the economic security of entrepreneurs:

1) collecting, classifying and processing necessary information about the environment (competitors, suppliers, consumers, political, economic, as well as political and 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 oftentimes perceives information resources as a secondary type of resources giving priority to material basis of enterprises. However, non-material resources of an enterprise are the ones under attack in the era of information war.

The notion of information war is defined by the 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, the 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 factors.

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 whose implementation may have a negative impact on the security of information space of an entrepreneur. The 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 the 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 authority;
- instability of the political situation and redistribution of property between financial and industrial groups;
- import of espionage technologies and capital from the Russian Federation where they can no longer be useful owing to improvement in the current legislation.

According to expert assessment, 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 thousand entrepreneurs have become victims of information attacks in Ukraine so far. The annual raider redistribution of property reaches the average of 2 – 3 billion US dollars (Varnalii, 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 the companies and their assets are sold to interested parties at high prices or left in own business);
- investment factoring companies acting on behalf of the sponsor.

The market of raider companies in Ukraine contains 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 of the aggressors' actions regarding the victim company.

The department working on hostile takeover projects makes use of the above-mentioned departments 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 ones:

- weakness of the legal system;
- incompleteness of the judicial authority;
- corruption of the authority;
- absence of state-based institutes to provide effective protection of the owner's rights;
- a low level of the legal culture;
- legal nihilism of both entrepreneurs and authority representatives;
- ambiguous background of privatization of strategic economic entities.

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 regarding activity of strategic enterprises conduct their activity in Ukraine;
- the information attacks are system problem in Ukraine. The number of seizures of domestic enterprises reaches 3000 annually. An information attack precedes every seizure;
- the efficiency of information attacks is over 90%;

- according to the expert evaluation, the annual merging figure (without privatization) is over 3 billion US dollars;

- according to the expert evaluation, the raider's average income rate in Ukraine is about 1000%. Therefore, the costs of information resources are significant (Vanalii, 2014);

- the next stage of the 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 redistribution of property. According to the survey of "The Centre for Researching Corporate Relations" (The Centre for Corporate Research, 2014), "Pryvat" business-group is regarded as the biggest Ukrainian raider by 100% experts, "Finances and Credit Group" – by 54.6 %, and "Alfa-Group" – by 45.5 %.

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

- negative influence on the entrepreneurial climate;
- destabilization of domestic enterprises;
- ruining of labour collectives and social conflicts;
- formation of unfavourable investment climate and international image of the entire country, etc.

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

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

- to timely provide the managers with complete and reliable information regarding the external environment of the enterprise; to determine the factors of enterprise risk;

- to effectively organize informational works including same function duplication by different subdivisions;

- to work on both short-term and long-term predictions of environmental influence on the economic activity of the enterprise; to develop recommendations concerning the localization and neutralization of available risks.

- to enhance the favorable and reduce the unfavorable influence of the environment on the economic activity of the enterprise;

- to search for new ideas, technological innovations, methods etc. to be implemented at the enterprise, and making the enterprise competitive.

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

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

References:

1. Варналій З.П., Мазур І.І. Рейдерство в Україні: передумови та шляхи подолання // Стратегічні пріоритети. – 2007. – №2(3). – С. 131-136.

2. 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.

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article – Юридичний журнал.

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

5. Результати експертного опитування „Центру дослідження корпоративних відносин” [Електронний ресурс]. – Режим доступу: http://www.corporativ.info – Центр дослідження корпоративних відносин.

6. Тоффлер Е. Третя хвиля. – Київ: Видавничий дім «Всесвіт», 2000. – 480 с.

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

8. Lasswell H. D., Smith B. L. Propaganda, Communication and Public Opinion Hardcover. – Princeton University Press; 1st edition, – 1946. – p. 435.

9. Lasswell H. D. World Politics and Personal InsecurityPaperback. – The Free Press, 1950. – 238 p.

10. Lazarsfeld P. An episode in the history of social research // Perspectives in American history, 1968. – 272 p.

11.Luhan M. Hot & Cool. – Signet Books. – NY: The New American Library Inc., 1967. – 286 p.