УДК 65.012.8 (045)

Skibitska L.I.
Senior Lecturer, Department of Management
foreign trade enterprises
National Aviation University

ECONOMIC INTELLIGENCE IN CRISIS MANAGEMENT NOW

Statement of the problem. Competitiveness of enterprises are increasingly determined by its ability to rapidly reproduce, grow and update information on the potential and intentions of competitors and conceal its internal information as trade secrets, to provide at least a temporary monopoly on the market. However, the organization of economic intelligence, the use of automated systems for the analysis of data and the organization of counter- intelligence measures for crisis prevention and/or mitigation of symptoms in the domestic business has not yet gained enough attention, which causes a novelty of the study.

To maintain stable operation of the enterprise more important was the presence of timely accurate information not only about the state of the potential of the enterprise, but also the suppliers, competitors, customers, the latest technology, and other settings of the environment. In these circumstances, an important resource, providing efficient operation of the enterprise is the information and communication connections.

However, some aspects of competitive systems (economic) intelligence are currently controversial and sometimes caused by the public reproof. In particular, sometimes ambiguously competitive intelligence work is evaluated in terms of its compliance with ethical and legal standards. Doubts exactly the kinds that have not been dispelled, became a stumbling block for a number of companies who have not decided on the creation of such services.

The above determines the relevance and novelty of a scientific research problem.

Analysis of recent research and publications. The problems of economic security business in crisis management at the time worked on such foreign scholars as R. Ackoff, I. Ansoff, K. Bowman, E. Brigham, R. Heath, A. Shtanhret, G.L. Azoev, Gradov A.P., A.P. Chelenkov, A.M. Kutsenko, L.O. Lihonenko, O.V. Moroz, Z.E. Shershnova.

The aim of the paper is the rationale for the organization of economic intelligence in the enterprise, defining the concept of a systematic approach to the protection of trade secrets and confidential information and counterintelligence organizations.

Statement of main content. "We no longer live in the information age - says L. Kahaner, author of "Competitive Intelligence". - We live in an age of exploratio".

Thus, competitive intelligence (CI) is a powerful tool for market research, and currently is a discipline that is booming, which occurred at the intersection of economics, law and specific intelligence disciplines. Raman difference from industrial espionage is that it is only through existing state laws, and their results are obtained by analytic processing a huge number of various public information materials from various sources.

We have already mentioned that the CI gives the best results if it is organized as a continuous process.

First, the structure of the intelligence cycle already requires a process. When organizing a large-scale intelligence system in your company should strive to extend beyond the scope of cooperation and involvement of as many people.

Second, even if a very successful working of view of official duty as a CI -person senior management, the system of intelligence gathering can sometimes be seen in another part of the company as a kind of "spyware executive agency". Providing access to the CI only managers of the highest level, you can sometimes "lose" employees who would like to receive the materials CI and effectively use them in their work. Moreover, avoiding some of the employees of the company to the material of the CI, they can repel willingness to submit to the CI system collected their own information.

You can create an effective system of management, have a highly skilled, have a high scientific and technical potential, have an extensive distribution network, but it will not be important if the CEO will not be able to detect external threats and risks that can put us in a difficult position [6]. To identify risks and create divisions CI. In many large companies such units are located in the service of strategic planning that reports directly to management. CI business unit is most effective if its main task is to support strategic information planning company. Other companies raman units can be part of each independent department that is subordinate to the first vice-president, or directly president, who coordinates their activities.

It is advisable not to place the CI in the service of marketing, sales, research departments and other independent structural units of the company, not related to each other. In such cases it is difficult to implement cooperation and coordination of the CI.

After all, does not matter where the unit is locate CI. Important as organized coordination of its work and how information flows circulating within the company. In some companies, information circulates in a closed circuit in the finished form is available on the lower level, that is being sent to each employee (which it is necessary to perform production duties), others - on the contrary, information is collected on the lower level is passed "up" (unclosed loop) and rarely comes to every employee of the company. From research on the development of the concept of CI conducted by *Learning Corporation*, it follows that such an organization (the second model) bring intelligence reports to employees does not benefit the company [7].

For maximum efficiency unit should be CI is quite high status in the company, the employees treated him with respect and saw him as their protector and champion of the interests of the company. However, this unit should be accessible to everyone in the company working within its competence, rather than perform tasks for the benefit of any one department.

Analytical information produced CI unit should be closed to all outsiders, but accessible to every employee of the company (to the extent that it applies).

Although the main purpose of the CI - support management decision-making, formed somehow Raman system can help companies solve many other problems, such as:

1. Predicting changes in the market. Companies that focus their efforts on the CI track market changes rarely fall suddenly in trouble because of the events that affect their business. Conversely, companies that have no such attention may soon become bankrupt.
2. Predicting the actions of competitors.
3. Identify new or potential competitors.

4. The study of successes and failures of competitors.

5. Search and study of firms alleged to buying (merging).

6. Learning new technologies, products and processes.

7. Monitoring changes in the political, legislative and regulatory areas that affect business.

8. Starting a business. Competitive intelligence can not only help to decide on a new activity or diversification, but also will provide a critical baseline information for its development.

9. Outdoor view of their activities. Many companies, especially large ones, think limited without going beyond their own limits. Their working methods are traditional and outdated; CI provides new ideas and concepts. It makes the eyes focus on the external world and determine the location of the company in a competitive environment.

10. Help in the application of advanced management tools. Some companies are experiencing difficulties in deployment and maintenance of such expensive technology management as "a comprehensive quality management", the introduction of corporate management information, and «the transition to the new technology «or» system of customer satisfaction. One reason - the lack of information.

Aims and objectives of the CI is largely similar goals and objectives of classical intelligence, whose analytical materials used in the formation and implementation of public policy or planning military operations, but the scale of tasks are quite different. The main applications CI - a market. The main purpose of the CI is the systematic tracking publicly available information about competitors, analysis of the data and decision based on their management decisions. Create a CI of competitive intelligence - is the trend of time and the only way to survive in the fierce competition - is considered by many corporate executives in the United States. CI allows predicting changes in the markets, spending forecast the actions of competitors, identify new or potential competitors, to monitor the emergence of new "explosive" technologies and the political and financial risks.

Conclusions from the analysis of Raman data can be used for tactical decisions and strategic directions for the study of the firm or corporation as a whole. CI makes extensive use of methods and techniques of strategic management, which allows obtaining a comprehensive understanding of the market situation and specifying the position to which a company can claim it through the comparison of their competitive status with the competitiveness of other entities operating in the same market. Many competitive intelligence and derives from the arsenal of marketers whose focus is primarily on the identification and analysis of consumer demand in a particular market segment. So the officers involved in the CI, especially, collecting reports about the competitive environment and specific competitors (including potential) and their analysis. They simulate further treatment after market. CI, like a powerful radar, picking up new trends in the business, track opportunities that arise, and warns of the dangers looming.

However, some aspects of the Raman sometimes controversial and cause some reproach from the public. In particular, sometimes mixed CI valued work in terms of its compliance with ethical and legal standards. Doubts exactly the kind that have not been dispelled, became a stumbling block for a number of companies that have not dared to create such services.

Meanwhile, using various, sometimes not very correct, collection methods - from the front "combing" Internet channels to digging in trash their rivals - analysts Service accumulating data from almost all the major issues for the management of the company - from development teams new products and the level of production costs of its production to the personal characteristics and professional qualities of leaders and experts of competing companies, as well as motives adoption of certain management decisions. After all, sometimes even random information can be very valuable [4].

With the current abundance of information, streamlined flow of income is not the same home help in solving the problems facing CI. Finally, with the expansion of the Internet and the advent of computer databases, information has become a cheap and quite affordable the goods, and for the sake of getting no sense to burden corporate structure is one large unit. Objective CI is mainly to help the management of the company learn from this abundant information flow only necessary for decision-making data.

The concept of a systematic approach to protect confidential information received name - the "method OPSEC" (Operation Security). This approach has been developed by U.S. experts during the Vietnam War, to improve the protection of confidential information and reduce the cost of its preservation. According to the author's method - known American specialist in security Pattokkosa A., OPSEC is effective concealment of intentions, plans, events, technology, allowing you to constantly be "one step ahead the enemy". Application of this method in the field of civil post means supporting the competitiveness of products, financial situation. The method is to stop, prevent or limit the leakage of the part information (most sensitive), which can give a competitor an opportunity to "learn" or "calculate" that makes your company or plan to, and eventually beat it on the market [5].

The process of protecting information by using OPSEC is divided into seven stages.

Step 1. Analysis of facility protection.

At this point, determine what needs to be protected. Analysis is performed in the following areas:

- is what information needs protection;
- are the most important elements (critical) protected information;
- is determined by the lifetime of critical information (the time required for the implementation of a competitor of the information);
- identifies key elements of information (indicators) that reflect the nature of the protected information;
- indicators are classified by functional areas of the enterprise (industrial and technological processes of logistics production company personnel, finance, management, etc).

Step 2. Identifying threats.

At this stage:

- determines who may be interested in information that is protected;
- assessing methods used to obtain the competitors of this information, and probable uses of weaknesses in the existing enterprise security management system in a particular case;
- developing a system of measures to curb the actions of competitors.

Step 3. Analysis of effectiveness.

At this point, analyzes the effectiveness of adopted and permanent security subsystems (physical security, safety documentation, personnel reliability, security lines, etc). Then simulated the planned operation and consists of a chronological description of events (or their functional relationships), which is necessary to ensure safety. For each event the proposed transaction defined indicators that can serve as starting data to

identify critical information. Identify possible sources of specific information, the analysis of which can lead to the identification of indicators (newspaper articles, press releases, phone calls over insecure channels, a careless attitude to drafts, transfer of unnecessary information, in the course of negotiation and steel stereotypes, patterns of daily work and procedures, etc).

Step 4. Determining the necessary security measures.

During this stage on based on the first three stages of the analytical studies determined necessary additional measures to ensure safety. This list of additional protective measures that can "close" identified vulnerable areas, accompanied by a cost estimate associated with the use of each measure. Comparison of the expected reduction of vulnerability and future costs to evaluate the economic feasibility of the proposed measures.

Step 5. Consideration of proposals for security measures and criteria for performance/value.

At this point, the heads of the firm are considered to offer the necessary security measures and the calculation of their cost and effectiveness.

Step 6. Take steps.

At this stage, the measures implemented additional security measures based on the established priorities.

Step 7. Control of events.

At the final stage of a control and refinement implemented precautions. It is verified the effectiveness of the measures taken, are left unprotected or newly emerging vulnerabilities. Implemented measures are communicated to the optimum level, entered a permanent control over their operation.

Counter-intelligence cycle consists of five phases:

1. Defining security requirements.
2. Evaluation competitors.
3. Assessment of their vulnerability.
4. Development of countermeasures.
5. Implementation of countermeasures.

Unlike intelligence, counter- intelligence target activity is not external and internal environment of the operation of the business.

This environment includes the following elements:

- company management team (director, his deputies, chief accountant, etc.) as potential objects of exploration activities and/or crimes of competitors;
- persons with a support staff that have access to trade secrets (typists, office workers, etc.);
- employees of which there is a risk of potentially criminal elements such reports to help them make crime (guards, drivers of personal vehicles heads , etc.);
- members of the security services;
- previously convicted person from the employees;
- employees of companies whose relatives are competitors;
- previously retired workers;
- persons who by virtue of their duties regularly take visitors enterprise.

Goal Setting and the object counter-intelligence activities to determine the range of possible counterintelligence division of responsibilities, including:

- the fight against economic espionage;
- suppression of crimes against individual employees (or all employees at their workplace);
- to assist law enforcement, court and control supervisors in documenting illegal activities of persons who make criminal offenses and administrative offenses.

Performing the above tasks possible with the next set of counterintelligence functions:

- collection of reports and documents in civil and criminal cases;
- regularly inform the management about causes and conditions conducive to the implementation of offenses by staff;
- documenting the actions of persons detained for administrative transgressions;
- to identify people from the staff that make promoting illegal items (not working at the plant) in the exercise of their crimes;
- exposure of economic (industrial) spyware among staff;
- informing managers of the enterprise and security guards (if refers) on planned crimes against them;
- search news without missing the company's employees;
- creating conditions that preclude eavesdropping conversations in the office;
- setting circumstances disclosure reports, which constitute trade secrets;
- determination of biographical and other data characterizing personality of the company's employees (with their written consent) at the conclusion of their;
- labor contracts;
- search the lost members of property belonging to the enterprise;
- advising on the security company and its personnel.

Regarding ethics in competitive intelligence, it is worthwhile to consider focusing attention on addressing ethical issues in benchmarking.

Robert C. Camp in his book "Benchmarking - search for the best industrial practices that lead to superior performance" benchmarking process defined as "finding the best practices that lead to the best functioning". David T. Kearns CEO of Xerox Corporation defines benchmarking as "the continuous process of evaluation of products, services and working methods based on comparisons with the strongest competitors or those companies recognized leaders". The ninth edition of the New Dictionary for colleges Webster (Webster) defines benchmarking as "a starting point for which measurements are done" and as "something that serves as a standard (benchmark), with which you can measure something else". For our purposes, benchmarking can be defined as "a systematic method of identifying, understanding and development of products, services, designs, and equipment, processes and business practices of the highest quality to enhance the real work of the organization".

Benchmarking is linked to a number of legal and ethical issues. Generally all competitive intelligence concerns the ethical and legal conflicts. Society is still often considered obscene CI case, a product of "dirty spy craft".

Thus, we present the main provisions of the Code of conduct benchmarking.

1. The principle of legality.

1.1. If refers at least any doubts about legality of action, do not start this action.

1.2. Avoid discussions or actions that could lead to restrictions on the freedom of trade, the market allocation schemes and/or customers, price fixing, the conclusion of agreements, registration or bribes. Do not discuss the problem of costs, if the costs are part of pricing.

1.3. Not searches trade secrets in ways that can be regarded as invalid, including the breach or inducement to breach of obligations to preserve confidentiality. Do not open or use any trade secrets that could be obtained from illegal methods or opened by someone else, in violation of their obligations to preserve confidentiality and to limit their use.

1.4. Do not distribute (either as a consultant or as a client) Benchmarking findings of one study to another company without first obtaining permission of the participants in the original study.

2. The principle of sharing.

2.1. Try to give your partner for benchmarking information of the same kind and quality as you ask of it.

2.2. Install the relationship in advance to understand expectations, eliminate misunderstandings and establish mutual interest in benchmarking.

2.3. Be honest and frank to the end.

3. The principle of confidentiality.

3.1. Think of a mutual exchange of benchmarking as confidential attracted to his people and companies. Information should not extend beyond the partner organizations without prior consent of the partner that shared information.

3.2. The participation of a company in the survey confidential and shall not be communicated without its permission.

4. The principle use.

4.1. Use the information gathered in benchmarking purposes only formulated to improve operations and processes in companies involved in the Benchmarking study.

4.2. Use the name or message benchmarking partner require prior approval of the partner.

4.3. Do not use benchmarking information or any information received as a result Benchmarking exchange for trade or advertising.

4.4. Information about possible contacts provided by the International Benchmarking Clearinghouse, in any form and in any way cannot be used for marketing purposes.

5. The principle of first contact side.

5.1. If possible, mount the contacts for benchmarking through its partners.

5.2. Respect the corporate culture associates and operate in accordance with mutually agreed procedures.

5.3. Take the mutual consent set for benchmarking contact on any message or transfer responsibilities to other parties.

6. Principle contact third party.

6.1. You will receive prior authorization contact before reporting his name in response to a contact request.

6.2. Avoid contact person to notify in open forums without her permission (consent).

7. The principle of training.

7.1. Demonstrate an understanding of the usefulness and effectiveness of benchmarking, pre-prepared before the first contact for benchmarking.

7.2. Rational use during your benchmarking partner, thoroughly prepare for each exchange.

7.3. Helps your benchmarking partners prepare by supplying their questionnaires and summons the day before each visit.

8. The principle conclusion.

8.1. Perform well and on time every commitment given to your partner for benchmarking.

8.2. Finish every Benchmarking study as mutually agreed.

9. Understanding of the principle.

9.1. Try to find out which style of communication and cooperation prefers your partner for benchmarking.

9.2. Observe the accepted style of communication with your partner benchmarking.

9.3. Find out how your benchmarking partner would like you to cultivated and used his information and act in this way.

Commercial structures, along with the organization of data collection on the one hand, it is necessary to protect their information, the system to access the reports, which are trade secrets (CI) businesses (firms) and their security system.

Consider the most common violations of the protection of personal data.

Thus, the State Service of Ukraine on protection of personal data for the outcome of its audits provided information on the main provisions of the legislation on the processing and protection of personal data, which is usually not observed. In particular, among these are the following:

- the owner of personal data must notify the authorized state body with the protection of personal data on every change of information required for registration framework, no later than 10 working days from the occurrence of such change;

- in the company (institution or organization) processing of personal data may exercise only those individuals whose job description or other internal documents of the obligation to implement the processing of personal data;

- the owner of the personal data shall, before committing processing of personal data, obtain the consent of the subject of personal data processing on these data;

- before getting into the subject of consent to the processing of personal data, the owner and/or managers of personal data is necessary to determine if there are other legal grounds for processing personal data. For example, the processing of personal data of employees in order to ensure the implementation of employment does not require consent, but if now gather personal information not covered by labor laws, workers must obtain consent to the processing of such data;

- providing adequate protection areas, which are personal data, both in electronic form and in the form of data files (such as equipment door locks on the premises, cabinets and vaults) [2].

Currently great interest in analytical methods for information exploration exhibit, both public and private (commercial) intelligence. This is due to the fact that the Internet contains a large amount of information that can be operational interest, both for the first and for the second. Therefore, in many countries, particularly in law enforcement Russia (Management "P" Interior, Department of Information Security FSB), the U.S. (FBI) and Germany (indicated) created special analytical intelligence on the Web. Similar units operate in the multinational corporations that increasingly become a "state within a state".

In addition, there are independent research center specializing in "phishing" required data "Digital Ocean". For example, in Western Europe and the United States gather information from the Internet has long become a very lucrative business. According to open press in France currently operates more than a dozen companies, whose task is to study the documents, including tables and figures that exist in the Internet space. As an example, you can bring linguistic engineering company MAAG, which is focused on information and analytical support for key areas of French economy as aerospace, transportation and energy. For global research online uses special "processors for data collection" (in some sources called a "text- analytical system", although the name is not entirely correct, as analyzed not only text but also graphics, drawings, photographs and graphics). In this context, the term "processor" - is part of a program that determines how the program manages and manipulates data.

The processor uses the data collection software, called "robot», which "pulls" the information, using an arsenal of tools and techniques of linguistic, semantic, and statistical analysis. Acting independently collect data processors intercept any of the requested information as soon as it is available online.

Conclusions.

1. In the system of safeguards is essential to the optimal distribution of industrial, commercial, financial and credit reports which are secret enterprise between

specific implementing relevant papers and documents.

2. In the distribution of information on the one hand, it is necessary to provide a particular employee for quality and timely execution of work entrusted to him the full amount of data, on the other hand, exclude the possibility of exploring the musician with redundant, it is not necessary for classified summaries.

3. The concept of a systematic approach to protect confidential information «OPSEC» is effective concealment of intentions, plans, events, technology, allowing you to constantly be "one step ahead the enemy". Application of this method in the field of civil post means supporting the competitiveness of products, financial situation.

4. The distinctive competitive intelligence from industrial espionage is that the CI is exclusively within the existing state laws, and their results are obtained by analytic processing a huge number of various public information materials.

Prospects for further development in this direction. One of the most promising areas of the mentioned problems saw further study of the problems of information and analytic intelligence tools available. This package of measures, many experts and indicate how computer intelligence. Its essence lies in finding and sharing information with computer systems and networks "world wide web", followed by verification and analytical processing.

BIBLIOGRAPHIC LIST:

1. Про інформацію : Закон України // Правда України. – 1992. – 2 жовтня.
2. Лист Державної служби України з питань захисту персональних даних від 05.02.2013 р. № 11/257-13.
3. Азоев Г. Л., Челенков А. П. Конкурентные преимущества фирмы. – М. : ОАО «Типография и новости», 2002.
4. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський, О. М. Юрченко / Під ред. О. П. Снігерьова. – Запоріжжя : ПВКФ «Павел», 2005.
5. Вертузаєв М. С., Голубєв В. О. Захист інформації в комп'ютерних системах / Під ред. О. П. Снігерьова. – Запоріжжя : ВЦ «Павел», 1998.
6. Куценко А. С. Основні проблеми і радикальні шляхи вирішення антикризового управління промисловими підприємствами : монографія / Українська академія наук. – К. : Фенікс, 2006.
7. Некоторые правовые аспекты защиты и использования сведений, накапливаемых в информационных системах // Борьба с преступностью за рубежом. – М. : ВИНИТИ, 1990. – № 7. – С. 63–64; 1992. – № 6. – С. 13–14.