ORGANIZATIONAL MEASURES OF INFORMATION SECURITY FROM INDUSTRIAL ESPIONAGE

Abstract: The world is now dominated by globalization and technologization, which is driving the world to change and obey these trends. With the development of information technologies, more sophisticated methods of surveillance have begun to be introduced, both for states as a whole and for individuals. Industrial espionage operates in various sectors of society, but it is often used either by enterprises or by state intelligence agencies. The importance of the information sphere in ensuring the security of society is growing. Through it, a significant part of threats not only to the national security of the state, but also to the economic well-being of institutions and enterprises is realized. The main purpose of the measures taken at the management level of the organization is to form a program of work in the field of information security and ensure its implementation, allocating the necessary resources and constantly monitoring the state of affairs. It should be noted, however, that industrial espionage remains and will remain a powerful tool for state intelligence, the purpose of which is to directly violate the laws of foreign states in the interests and on behalf of their country. The importance of solving the problem of ensuring the reliability of information is also confirmed by the cost of protective measures. Therefore, our research is more relevant than ever at nowadays.

Keywords: Industrial Espionage; Information Security; Competitive Intelligence; Organizational Measures.
Пестов Максим
Студент
Уральский федеральный университет
Россия, г. Екатеринбург

Научный руководитель: Ковалева Александра Георгиевна

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ПРОМЫШЛЕННОГО ШПИОНАЖА

Аннотация: В настоящее время в мире доминируют глобализация и технологизация, которые побуждают мир к изменениям и повиновению этим тенденциям. С развитием информационных технологий стали внедряться более сложные методы наблюдения, как для государств в целом, так и для отдельных лиц. Промышленный шпионаж действует в различных секторах общества, но часто используется либо предприятиями, либо государственными разведывательными службами. Значение информационной сферы в обеспечении безопасности жизнедеятельности общества все возрастает. Через нее реализуется значительная часть угроз не только национальной безопасности государства, но и экономическому благополучию учреждений и предприятий. Главная цель мер, предпринимаемых на уровне управления организацией, - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и постоянно контролируя состояние дел. Однако следует отметить, что промышленный шпионаж остается и будет оставаться мощным инструментом государственной разведки, целью которой является прямое нарушение законов иностранных государств в интересах и от имени своей страны. Важность решения проблемы по обеспечению надежности информации также подтверждается затратами на защитные мероприятия. Поэтому в настоящее время наши исследования актуальны как никогда.
According to the Turkish scientist Tanju Colakoglu, industrial espionage is a form of unfair competition in which information constituting a commercial, official or other secret protected by law is illegally obtained, used or disclosed in order to obtain business advantages and material benefits. The main purpose of industrial espionage is to save time and money to catch up with a leading competitor or to ensure that a competitor does not fall behind in the future if he has developed or is developing a new promising technology, as well as to enter new markets for the company [1].

Industrial espionage remains and will remain a powerful tool of state intelligence, the purpose of which is a direct violation of the laws of foreign states in the interests and on behalf of their country. However, the choice in favor of competitive intelligence is becoming more and more popular at the enterprise level, as the enterprise does not have the authority of state intelligence, so in case of failure of industrial espionage operation it is risky to be held criminally liable, as well as to bear reputational risks [2, 3].

According to Russian researchers, in our country industrial espionage is carried out in order to gain market share, counterfeit goods, discredit or eliminate competitors, disrupt negotiations on contracts, resell trade secrets, blackmail certain persons, create conditions for the preparation and conduct of terrorist and sabotage actions. Therefore, it is important for companies to comply with organizational measures to protect information from industrial espionage [3].

Information security is a set of measures taken by the owner of information to protect his rights to own and dispose of information, to create conditions restricting its dissemination and excluding access to classified information and its carriers.

Complexity of maintenance of protection of the information demands creation of the special service which is carrying out realisation of all protective actions and first of all the organizational plan. Structure, number and composition of security service of the company are determined by real needs (degree of influence of loss of confidential information on performance indicators) [3, 4].
If there is a security service in place, the process of organizing information security passes through the following steps.

The first stage consists in definition that it is necessary to protect. The analysis is spent on following directions:

- Analyzing what information first of all needs in protection;
- Definition the most important elements of the protected information;
- Definition term of a life of the critical information;
- Definition the key elements of information reflecting the nature of protected information;
- Classification of indicators by functional zones of the enterprise (production and technological processes, system of material and technical support of production, subdivisions, management) [2, 3, 4].

The second stage is reduced to the identification of threats:

- Determining who may be interested in the protected information;
- Evaluating the methods used by competitors to obtain this information;
- Evaluating the likely channels of information leakage;
- Developing the system of measures to suppress the actions of a competitor.

The third stage is to analyze the efficiency of the accepted and constantly operating subsystems of safety provision (physical safety of the documentation, reliability of the personnel, safety of communication lines used for transfer of the confidential information, etc.).

The fourth stage is to define the necessary protection measures are. On the basis of the first three stages of analytical studies the necessary additional measures and means to ensure the safety of the enterprise are determined [2, 3, 4].

On the fifth stage the company's managers consider the submitted proposals for all necessary safety measures and calculation of their cost and effectiveness.

The sixth stage consists of the following tasks. The control is carried out and the implemented security measures are brought to the attention of the firm's personnel [2, 3, 4].
In conclusion, our research considers the main organizational measures to protect information from industrial espionage, and also defines its concept and objectives. Obviously, the compliance with these rules by the company reduces the risk of becoming a victim of such attacks, but does not ensure absolute security, as there is still a need to protect information from the hardware point of view.

**REFERENCES**