CONTENTS

INTRODUCTION

The issues of economic, corporate and information security are of great importance for society, since corporations are the main employers, the main taxpayers, bear the social burden and the well-being and stability of both states and the peoples living in them depend on the sustainability and stability of corporations.

A corporation is understood in a broad sense as a community of people united to achieve a common goal, which can include both a commercial corporation created to make a profit and non-profit corporations — public, political, religious organizations that have a huge impact on the political and social situation in society.

There is also an inverse relationship - crisis phenomena in the corporate environment cause global crises in the economic, political, social sphere, examples of which can be observed enough from the Great Depression of the 20s and 30s of the XX century, the trigger for which was the collapse of corporate stock prices on the stock market, to the crisis of 2008, which was launched by the crisis of corporations in the financial and insurance sectors. We observed the same picture throughout the post-Soviet space in the 1990s, when the mass closure of manufacturing enterprises, including city-forming ones, the crisis of non-payments, delays in salary payments for months and even years caused the most acute political and social problems — a drop in the population's income, an increase in crime, an increase in mortality, a drop in the birth rate, mass migration of residents from their countries. Thus, the importance of corporate security issues continues to be preserved and in light of the impending new wave of the world global economic crisis, its relevance is only increasing. The monograph reveals both corporate governance in natural, ordinary conditions and the main threats to corporate security, describes the factors of the external and internal environment that affect corporate security both positively and negatively.

CHAPTER 1
The role and importance of corporate security in ensuring stability in the development of society

The concept of economic security, the relevance of problems of economic security, trends in the development of social and economic relations, the influence of economic security on the socio-economic development of society and the state.

There are quite a few definitions of the term "Security". The first type of definition is currently supported by the majority of scientists and corresponds to the concept of the term "security" set out in Art. 1 of the Federal Law "On Security" № 2446-1 of March 5, 1992: "Security is the state of protection of the vital interests of the individual, society and state from internal and external threats"[1].

This approach can be conditionally called "static", since the term "state" itself assumes a certain static character.

The second type of definition of the concept of security, is based on the fact that "security is not any state, as stated in the first approach above. To protect oneself means to create conditions that can be controlled and in which it is possible to manage, it is possible to carry out one's activities." Hence, the conclusion follows: "security is not a state of protecting the interests of a subject, security in general is not anyone's state. Security is the conditions of existence of a subject, controlled by him."[2] This type of definition can be called dynamic.

A corporation should be understood as an association, community, union, or group of persons. Therefore, we have the right to consider any collection of people engaged in joint activities as a corporation. At the same time, any organization or business structure can be considered as a systemic entity.

Thus, we can define corporate security as the state of a corporation as a system (its main subsystems), in which the

[1] Federal Law "On Security" N 2446–1 of March 5, 1992.

[2] Borodin I. A. Fundamentals of corporate security psychology. — M.: Higher School of Psychology, 2004.

likelihood of actualization of factors threatening its existence is minimized.

Hazards are possible or real phenomena, events and processes that can cause material or moral damage to the corporation and business activities.

A threat is a potential or actual action by attackers that can cause material or moral damage to the company and its personnel.

Danger can take on different forms. It can be in the form of intentions, planning actions and their implementation with the aim of destroying, weakening, taking over a company, etc.

Threat as a real sign of danger is an essential characteristic of security. Threat and the fight against it are the essence of security. Thus, corporate security should be understood not as the absence of danger, but as protection from it.

There are internal and external security threats that can be directed at personnel, material, financial and information resources of the company.

Internal security threats should be understood as the inability for self-preservation and self-development, the weakness of the innovation factor, the ineffectiveness of the corporate governance system, and the inability to establish an optimal balance of interests to resolve contradictions and conflicts between stakeholders.

External security threats include:

– the unfavorable state of the country's economy;
– natural disasters and man-made disasters;
– imperfection of legislation;
– unfair competition;
– corruption;
– organized crime.

Depending on the severity of the consequences, threats with high, significant, medium and low severity of consequences are distinguished.

A quantitative assessment of security threats can be made using a methodology that is based on calculating the damage coefficient (Ku), the value of which allows you to make a decision on more effective protection of your own economic interests.

To calculate the damage coefficient, the following data is used: actual losses (AL); loss mitigation costs (LMC); Loss compensation costs (CLC).

The sum of these values characterizes the actual value of losses (VLT), that is:

$$\text{Fiberboard} = AL + LMC + CLC.$$

The ratio of the actual amount of losses and the enterprise's (company's) own resources is the damage coefficient:

$$Ku = \text{fiberboard} / Q,,$$

where Ku — is the damage coefficient;

Q — volume of own resources.

Economic security includes many regulations and systems, such as: protection of trade secrets; internal work with employees in order to prevent negative phenomena; internal counterintelligence, and official investigations into security-threatening signals and facts; information and analytical work in the interests of security; technical and physical protection.

As a result of a critical analysis of the definitions of various scientists, the authors came to the conclusion that security is the result of the implementation of a set of organizational, managerial, regime, technical, preventive and propaganda measures that help ensure reliable protection of vital interests and the fundamental foundations of the existence of a corporation from internal and external threats , in which the company's management has the opportunity to independently determine the nature and forms of production or other activities to ensure the production of goods and services in volumes that contribute to the effective functioning and sustainable development of the corporation.

This definition synthesizes all three approaches to the study of corporate security — through interests, sustainability and independence.

Thus, we can define security as the state of a corporation, state, society as a system (its main subsystems), in which the likelihood of actualization of factors threatening its existence is minimized.

Principles and meaning of economic security.

The basic principles of economic security of the state, society, and enterprise are[3]:

– complexity, or consistency;
– timeliness;
– continuity;
– legality;
– planning;
– economy;
– interaction of personnel at different management levels;
– combination of openness and confidentiality;
– personnel competence.

A more detailed examination of the presented principles of economic security allows us to identify their main characteristics.

The principle of complexity involves the formation of an enterprise security system, which will subsequently ensure its protection, in particular employees, property, information (including classified as a trade secret), various areas of activity from existing threats and dangers (in the external and internal environment of the enterprise), force — major circumstances.

From the above it follows that the economic security system, its components, means, forces must meet the requirements of sufficiency to ensure personnel, economic, scientific, technical and other types of security.

It should be noted that the process of ensuring the economic security of an enterprise should involve not only direct employees, but also specialized services and enterprise personnel.

The program for ensuring the economic security of an enterprise is an organizational form of integrated use of the forces of existing resources (material, labor) of the enterprise. The principle of timeliness is characterized by the fact that the enterprise at all stages of the life cycle takes measures to eliminate the negative impact and damage to its functioning. The

[3] Zerkalov D. V. Economic security. Monograph. — K.: Osnova, 2011. — P. 165.

implementation of this principle is economically more profitable than eliminating the resulting negative consequences (damage)

The principle of continuity is that the construction of an enterprise security system should be carried out in such a way that the functioning is constant and protects its interests in the fight against intruders at a certain level of risk. The principle of legality lies in the fact that any work in the field of ensuring corporate security of an enterprise must be carried out on the basis of current Russian legislation, which means that contradictions with legislative norms are not allowed. Measures to ensure corporate security developed independently must also be implemented within the framework of current Russian regulations.

The principle of planning characterizes the organization of the economic security system, which allows all participants in the production process to carry out their activities consistently, systematically, with strict fulfillment of assigned tasks.

The principle of economy lies in the fact that the construction of an enterprise security system should be carried out in such a way that the invested costs for its operation are economically feasible (from the standpoint of economic efficiency), their size is optimal, that is, it does not exceed the economic meaning of the application.

The principle of interaction is that ensuring the security of an enterprise requires the coordinated activities of all persons involved in the process. The personnel management structure must clearly define job responsibilities, and each employee must clearly know their competencies. The principle of interaction, of course, also contributes to the characterization of the process of identifying and establishing business contacts, in addition, to coordinating actions with external organizations that can provide assistance in ensuring corporate security.

The principle of combining transparency and confidentiality is that all key activities in the field of ensuring economic security must be communicated to each employee individually in a short time and strictly carried out by each employee, which will allow for the prompt and timely identification and prevention of both real and potential threats and danger. However, we must not forget that some methods, means, forces and methods of

ensuring corporate security must be kept secret (commercial and official secrets), which means that access to them should be open only to certain employees. Such a strategy will make it possible to combat various threats and promptly prevent damage caused to the enterprise.

The principle of competence is that safety should be a key objective for an enterprise, and not a secondary one. Issues of ensuring corporate security should be dealt with by professionals in this field who have management skills.

The concept of security policy is understood as a system of decisions, views, and actions in the field of corporate security that create favorable environment and conditions for obtaining the necessary final results. Consequently, the ongoing economic security policy affects the implementation of the production program, the release of competitive products (goods, services, works), increasing production efficiency, property growth, and obtaining the necessary profit.

The concept of economic security strategy is understood as a set of the most significant management decisions that are aimed at ensuring the safe functioning of the enterprise. Thus, we can conclude that the corporate security system of an enterprise is a limited set of interconnected components that ensure its security and the achievement of a strategic goal. The components of this system are the object and subject of security, the mechanism for ensuring it, as well as certain practical actions.

The object of economic security is everything that is aimed at ensuring corporate security, in particular[4]:

1) various activities of the enterprise (managerial, commercial, production, supply);

2) resources and property of the enterprise (information, material and technical, financial, intellectual);

3) enterprise personnel (all departments).

Subjects of economic security are understood as persons, services, divisions, departments, bodies, institutions directly engaged in the process of ensuring corporate security of the

[4] Kushnir I. V. Goals of the financial policy of an enterprise: a course of lectures / I. V. Kushnir. — M.: Ivan Kushnir Institute of Economics and Law, 2010. — P. 44.

enterprise. Due to the fact that the number of corporate security subjects is large, it is advisable to divide them into two groups:

1) services directly involved in ensuring corporate security of the enterprise;

2) external organizations and bodies. The goal of corporate security is to protect the enterprise from all kinds of threats from various angles.

In this connection, it is necessary to highlight the main elements of the corporate security system (*Fig. 1.*)

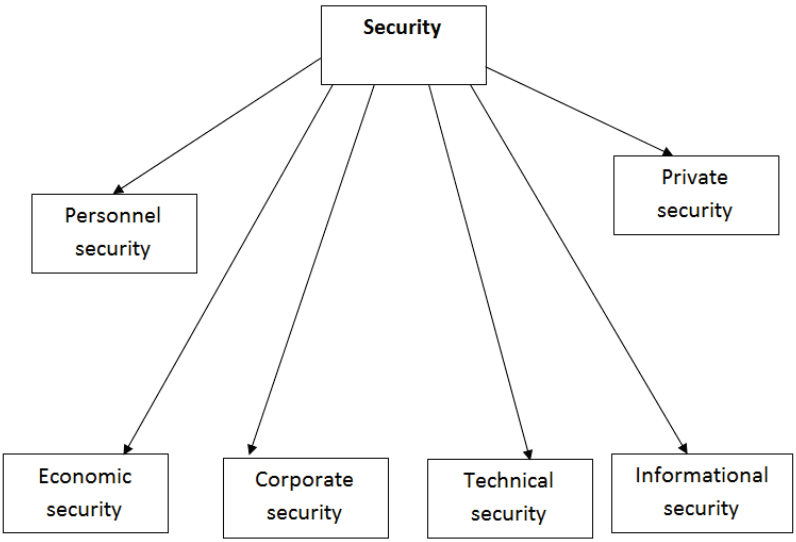

Fig. 1. Elements of the security system
(Developed by the author)

1) Personnel security. Due to the fact that most of the problems of enterprises are related to the human factor, providing protection against industrial espionage, hackers, disclosure of trade secrets, incompetence of employees, etc., personnel security is identified as a separate, important component of corporate security.

2) Information security. The concept of enterprise information security refers to the state of security of information flows and information resources of the enterprise.

3) Personal safety Ensuring personal safety includes three main areas:

– ensuring physical protection;

– providing legal protection;

– providing psychological protection.

4) Economic security. Economic security is ensured in the following areas:

– business intelligence;

– protection against fraud;

– management and minimization of economic risks;

– protection from hostile takeover.

5) Engineering and technical safety. Engineering safety contributes to the physical and organizational safety of the enterprise. Protection through certain technologies against information leakage.

6) Corporate security. Protecting the interests of participants in corporate relations.

Thus, by analyzing the theoretical aspects of the issue, the concept, means and methods of ensuring corporate security of an enterprise were formed.

If you have managed to avoid incidents so far, it is still important to anticipate problems and manage risks effectively. Research incidents your competitors have encountered through industry reports, your local news station or digital publications, and use this information to protect your safety and plan ahead.

The idea of economic security has evolved. In the 90s, the main emphasis was on the protection (security) of entrepreneurs and cooperatives of their property and life, which was due to the high criminalization of business and society. At this moment, a large number of private security companies (PSC) appear and the institution of bodyguards emerges. This gave the expected result. The number of criminal actions against entrepreneurs and property has decreased significantly.

Gradually, as market relations developed and measures of legal regulation of the market strengthened, the emphasis began to shift to the economic sphere. Corruption and tax pressure prevented entrepreneurs from developing quickly. During this period, there was practically not a single enterprise that operated without violating the current legislation. As a result,

a lot of “black” and “gray” tax minimization schemes appear. Naturally, in this state of affairs, regulatory and law enforcement agencies have become a serious “threat factor” for business. Formally, the use of such schemes can be classified as a system of measures to ensure economic security.

The second important phenomenon was the crisis of non-payments and the need for action to repay debts, usually by force. Law enforcement officials also contributed to their implementation. To solve this range of problems, security services were created at enterprises and firms, which were entrusted with the responsibility of ensuring, first of all, economic and information security.

“At the same time, serious personnel changes took place in the security forces. Some employees quit, some moved to the tax police and other newly formed structures. Supply created demand. Most of those dismissed found use of their experience and knowledge in private security companies and commercial structures as heads of security services. It should be noted that the main selection criterion was the number of connections in law enforcement agencies remaining with the candidate for the position. Using this method of “old connections” it was possible to find the necessary contacts in law enforcement and regulatory authorities. The second effective method of avoiding sanctions was payoffs.”[5]

As market relations developed, management methods also changed. Accordingly, security measures had to be improved. There is an objective need for a conceptual change in corporate security. The basis of the new concept was the systematic approach.

Any organization can be represented in accordance with it as a special case of an open system. There are two groups of factors in the external environment: positive, that is, facilitating the activities of the corporation, and negative, complicating its activities. Negative ones are called threat factors because of the danger they contain.

---

[5] Borodin I. A. Fundamentals of corporate security psychology. — M.: Higher School of Psychology, 2004.

The peculiarity of threat factors is that, being objectively determined, they cannot be controlled by security services. Thus, corporations need to develop an effective system of countermeasures

In connection with the development of market relations in Russia, the economic environment is changing significantly, and the primary tasks of enterprise managers include monitoring the dynamics of the environment, identifying threats and mechanisms for responding to them, taking into account these dynamics. This is important in conditions where individual elements of the environment or the environment as a whole show aggressiveness towards enterprises.

For survival and effective operation, it is necessary to take into account the interests of other business entities, their plans for the enterprise, the possibility of aggressive intentions, up to reaching an extreme of aggressiveness — the development and implementation of plans for a hostile takeover, which in most cases leads to the cessation of the existence of the organization, business structure as an independent economic entity.

The increase in the number of threats to economic security harms not only individual private interests, but also public interests, as it reduces the stability of civil turnover, worsens the investment climate in Russia and contributes to the growth of monopolization of certain industries and markets. We must not forget about the important role of business structures in replenishing the budgets of three levels — municipal, constituent entities of the Russian Federation, the Russian Federation, as well as in the share of employment of manufacturers and related enterprises. Threats to corporate security will not only cause a decrease in budget revenues, but will also cause a sharp increase in unemployment, a decrease in the level of income of the population, and, as a result, a social explosion in the regions and in the country as a whole.

Effective management is impossible without the implementation of effective methods of ensuring security at all levels of the hierarchy of social and professional systems, among which the leading role belongs to corporate security. Today, the

requirements for an organization's corporate security system are fundamentally different than before: from ways to adequately respond to threats and challenges to ensuring the potential and mechanisms to prevent them. It is this behavior that makes an organization flexible and invulnerable. The activities of a modern successful organization are based on a general system of sociocultural, moral and ethical values, which acts as the main guideline in the regulation of organizational activity.

Transforming your security approach from reactive to proactive requires a deep understanding of enterprise security, why it matters, and how to build the strongest possible defense. Training your team and committing to continuous improvement prepares your organization for combat and increases the likelihood of victory if and when combat occurs. To help you build the strongest corporate security defense possible, we've developed this guide to describe the key components of corporate security and why it's important, how to create and implement a security plan, improve your existing plan, and protect your bottom line.

Key components of economic security

Before we can develop a security plan or improve an existing one, we need to know the basic elements of security: legality, pre-existing risk, integration and collaboration. These four functions work together to create a strong policy framework, helping to ensure that every part of the enterprise is protected from unnecessary security threats.

• Security defines and implements all necessary legal measures.

The security policy is intended to protect the enterprise from any illegal activity and to provide legal support in the event of incidents. The only way to ensure the success of these goals is to design your policies based on legal precedent. Knowing which laws are most likely to be broken — even unintentionally — and what actions will help protect the enterprise team will help ensure compliance with the law and allow the corporation to operate within the confines of regulation.

• *Security manages security risks in the company.*

Corporate security manages security risks in a company.

According to the latest FBI data for 2019, a robbery occurs every two minutes and a property crime occurs every 4.6 seconds. This only applies to physical crimes. When we consider intellectual property rights violations and data theft or data breaches, the total number of crimes becomes even higher.

No matter what industry your business operates in, risk is inevitable and you could be the victim of a physical or digital incident. An effective corporate security policy reflects an understanding of your risk areas and proactively protects those weak points to avoid breaches.

If you're not sure your current policy fully protects your business, or you're not sure which assets put you at risk, now is the time to look into it. Examine past incidents your business has experienced and look for patterns of similar violations.

If you have managed to avoid incidents so far, it is still important to anticipate problems and manage risks effectively. Research incidents your competitors have encountered through industry reports, your local news station or digital publications, and use this information to protect your safety and plan ahead[6].

As market relations developed, management methods also changed. Accordingly, security measures had to be improved. There is an objective need for a conceptual change in corporate security. The basis of the new concept was the systematic approach.

Any organization can be represented in accordance with it as a special case of an open system. There are two groups of factors in the external environment: positive, that is, facilitating the activities of the corporation, and negative, complicating its activities. Negative ones are called threat factors because of the danger they contain.

No matter what industry a business operates in, risk is inevitable and it is possible to become a victim of a physical or digital incident. An effective corporate security policy reflects an

[6] Zainullin S. B. Tutorial. Corporate security. — M.: RUDN University, 2023.

understanding of your risk areas and proactively protects those weak points to avoid breaches.

If it is not certain that current policies fully protect the enterprise, or it is not known which assets are at greatest risk, then a risk analysis is necessary. To do this, past incidents that the enterprise has encountered are studied and patterns of such violations are identified.

If incidents have been avoided so far, it is still important to anticipate problems and manage risks effectively. You should also research incidents that competitors have encountered through industry reports, a local news station, or digital publications, and use that information to protect your safety and plan ahead.

• Economic security is one of the central activities of the company.

Another indicator of a company with a strong corporate security policy is that every department, team, and employee of that company is trained on the appropriate policies for their position and demonstrates responsibility for security.

Knowing when to use secure connections, protecting information, and reporting incidents as needed all demonstrate ownership. It is necessary to define a common understanding of corporate security as an indicator of its strength in your company.

• Economic security is implemented in collaboration with other functions and teams.

Economic security must also be a joint effort across the entire enterprise. A chain is only as strong as its weakest link. Maintaining corporate collaboration, such as company-wide training, incident drills, and recognition of teams or employees who go above and beyond to ensure corporate security, will minimize “weak links” that can hinder progress and keep your enterprise united. A corporate security policy is designed to protect the corporation from any illegal activity and to provide legal support when incidents occur.

The only way to ensure the success of these goals is to design your policies based on legal precedent. Knowing which laws are most likely to be broken — even unintentionally — and

what actions will help protect your team will help ensure compliance with the law and allow your business to operate within the confines of regulation.

Ensuring the economic security of a business is necessary for the company's success. Protecting customer data and your business should be a priority for any organization.

Globalization is accompanied by an increase in security risks. This is driving demand for data security professionals and services. It is estimated that more than 4,000 ransomware attacks, 33,000 phishing attacks, and 300,000 new malware infections are detected every day in North America alone. In addition, approximately 780,000 data records are lost due to hacking. In this digital age, cybercriminals are getting better and better at stealing information and bypassing network security.

In this digital age, cybercriminals are getting better and better at stealing information and bypassing network security[7].

Identity theft is also on the rise. If successful, cybercriminals often use stolen data to purchase goods, obtain credit, traffic drugs, or enter a country illegally.

Whether a company is an online retailer, a restaurant, or a law firm, it must take the steps necessary to protect customer data, protect financial records, and prevent cyberattacks.

It is the presence of a security system that will protect the company. Its absence can lead to loss of corporate income and even damage to its reputation. Worse, the owner could end up in jail or lose his business.

Without economic security, a corporation is vulnerable to these threats. Therefore, it is necessary to avoid these threats and install a security system. Apart from hiring corporate security services, the company should also follow the latest security practices.

Let's look at cases of the most high-profile threats to economic security and their consequences[8].

---

[7] What Is Corporate Security? A Complete Guide to Improving Security at Your Company. https://www.resolver.com/blog/corporate-security/

[8] The Most Useful Crisis Management Examples: The Good, Bad, and Ugly Smartsheet Contributor Andy Marker August 19, 2020. https://www.smartsheet.com/content/crisis-management-examples

Example 1: BP Deepwater Horizon

In 2010, the BP Deepwater Horizon drilling rig exploded in the Gulf of Mexico, killing 11 employees and leaking oil for three months. This is the largest oil spill in US history.

The oil spill caused damage to the environment and tourism. The environmental damage was long-lasting — one study estimated damage at $17.2 billion. The spill also caused billions of dollars in negative economic impacts on tourism in the region. Meanwhile, financial losses for the company included the following expenses:

By early 2020, BP had paid out about $70 billion in cleanup costs, legal settlements and fines.

In the two months following the spill, the company's shareholders lost $105 billion as its stock price plummeted.

For some time, the company's survival was in doubt. Its bonds fell in value and the company had to stop paying dividends for three quarters.

In the United States, the BP brand faced a backlash from consumers, and sales at BP gas stations fell by 10 to 40 percent immediately after the spill.

BP has had to cut its business costs for years, leaving it behind rivals such as Shell, whose brand value rose 24 % that year, according to the analysis. BP fell from the world's second-largest oil company in 2010 to fourth, where it remains.

Crisis Management Lesson: Creating a Culture of Safety

Research links the accident to a series of human errors and technical failures in the context of a high-risk corporate culture and weak regulatory oversight. The studies noted overconfidence on BP's part, based on the fact that there had been no deep-water blowout for many years. They also cite a lack of planning for low-probability, high-consequence oil spills.

Operators and managers became accustomed to normal signs of potential problems and ignored weak signals of impending disaster. The rig's alarm systems were disabled and critical equipment was not properly maintained. The UC Berkeley Center for Catastrophic Risk Management blamed a lack of safety culture and short-sighted prioritization. According to the center's report, BP "forgot how to be afraid".