DOI: 10.63550/ICEIP.2025.76.39.012

Features of Strategic Planning in Enterprise Information Security Risk Management

Mikhail Vitalievich Afanasyev[a], Urazbakhtina Liliya Ravilevna[b], Dyudina Olga Vladimirovna[c]
Department of Economics and Production Organization Kazan State Power Engineering University, 51 Krasnoselskaya street, Kazan, Russia
mixail.afanasev.98@inbox.ru, strat.men@yandex.ru, olga_dyudina@mail.ru

Keywords: Information security, strategic planning, digitalization, risk management, data protection methodology, sustainable development of the company.

Abstract: This article is devoted to analyzing the features of strategic planning in the context of information security risk management. The main approaches, tools and models that allow integrating information security risk management into the overall strategic planning process are reviewed. Advances in the Internet of Things, cloud technology and artificial intelligence make risk management more complex, but at the same time, effective strategic planning is the foundation of a robust risk management framework. Recommendations for adapting strategies to enhance digital transformation are offered, with examples of implementation and expected results. The study identifies the main cybersecurity risks to enterprises and describes key principles for managing these risks. The results of the study allow us to develop an architecture of recommendations for information security risk management.

[a] https://orcid.org/0009-0004-8430-2344
[b] https://orcid.org/0009-0000-8062-2165
[c] https://orcid.org/0000-0002-5483-3652

1 INTRODUCTION

The implementation of information security risk management factors into a company's strategy plays a critical role in increasing the company's resilience in today's realities. The information security industry in Russia is demonstrating constant and rapid growth, with the domestic cybersecurity market growing by 30% in 2024, and as of 2019, according to MTS Web Services research, the market will grow by almost 440 billion rubles.

The Russian information security market is in the stage of active development. The functionality of this area is not limited to individual areas, but is constantly expanding, as more and more processes are undergoing digitalization, and virtually every company is becoming a potential consumer of information security services, regardless of the product it manufactures (Lipatnikov, 2024).

Information security is a system for preventing unauthorized external influence on information in electronic or physical form. The main purpose of information security is to ensure the protection, integrity and confidentiality of data.

The relevance of the topic is also confirmed by the growing number of external threats to the domestic market and the increasing requirements for data protection directly from the companies themselves and the state. This is due to the fact that information security risks are critical for most companies.

The process of development of the information security market in Russia is accompanied by:

- Increase in the number of attacks on data storage and processing infrastructure;
- Stricter legal rules and regulations;
- Increase in the number of vulnerabilities related to the development of hacking technologies;
- Increase in the number of data breaches, both as a result of cyberattacks and internal intervention by a company employee.

It is important to emphasize that one of the most important factors of information security in a company is the level of information security culture among employees. Creating such a culture must start with managers and reach subordinates from the «top down». Building a security culture is the basis for protecting the company from social engineering threats, threats of working with suspicious files and allows employees to take necessary security measures in a timely manner.

Russian companies have started to actively use the new NGFW (Next Generation Firewall) data protection concept, which combines many different protection methods in one gadget (Kosinskaya,2024). According to a study by InfoWatch Group in 2023, in 82.6% of cases, the cause of information leakage in a company is a hacker attack (Neves,2023). In the same study, company experts noted that the overall rate of intentional violations was 98%, but most employee violations are accidental work errors.

This topic is actively researched in Russia, which also confirms its relevance. The authors Shabaeva S.V. and Shabaev A.I. emphasize the importance of the idea that at the moment there is no single approach to creating a digital transformation strategy, which should include a security strategy taking into account the specifics of the industry (Shabaeva ,2024). The article by Mirgaleeva I.V., Shamsutdinova M.R. and Bogdanov A.A. highlights the issue of the importance of information security at all levels in the enterprise, and for the successful functioning of the strategy safe and the company is obliged to look for its weaknesses and pick them up itself (Mirgaleeva, 2022). The work of Dmitrieva M.A. and Shedko Y.N. reflects the importance of introducing strategic audit of the company, approval of budgeting cycles and strategy approval at the same time (Dmitrieva, 2022). In Drozdova D.V.'s study, the key component to protect enterprises from cyberattacks is the complete replacement of tired defense systems, the use of only technologically modern methods of protection, based on the concept of NGFW, and the formation of a common methodology and regulatory framework for information security risk management. (Drozdova, 2024) . In the article by A. V. Solominsky, V. A. Zhelezin, A. D. Mirgorodsky, S. Krasnobaev, and N.M. Kolotilina the authors emphasize the importance of protection and processing of data coming to the company from third parties, as such data are subject to various risks, so to protect this kind of data, the company needs to implement automated security and privacy management programs (Solominskiy,2023).

A.D. Shkradyuk's research describes the importance of applying security assessment of information system by means of penetration testing, the key task of pentest is to find vulnerabilities and system or network, which are further improved in order to ensure reliable data security (Shkradyuk, 2022). The study of Ismagilov I.R., Akhmetshina R.I. and Gulmanova E.A. emphasizes the need for independent modeling of security threats to the critical information infrastructure of the company, the meaning of this modeling is to find all the conditions and factors that can potentially carry danger to the system, or are already dangerous (Ismagilov, 2022). From the point of view of the state, the Decree of the President of the Russian Federation of 21.07.2020 N 474 "On the National Development Goals of the Russian Federation until 2030" highlights the tasks of creating for companies and households a sustainable and secure infrastructure for uninterrupted work with large amounts of data, which reflects the importance of the topic at all levels in the state. The state is constantly adapting the regulatory framework to the realities, in the Decree of the President of the Russian Federation dated June 13, 2024 N 500 "On Amendments to the Decree of the President of the Russian Federation dated May 1, 2022 N 250 'On Additional Measures to Ensure Information Security of the Russian Federation' was prohibited to public authorities and companies of strategic level to use information security services and services of companies from unfriendly countries, in order to protect national interests and accelerate the pace of development of the domestic market.

2 AIMS AND OBJECTIVES OF THE STUDY

The purpose of the study is to examine the specifics of applying strategic planning for information security risk management in a company.

The objectives of the study are to:

- Conduct research on literature sources on the topic of the study;
- Consider the factors that are important to consider when forming a strategy;
- Consider the existing approaches and models of strategic planning in the management of information security risks of the company;
- To offer practical recommendations on the integration of risk management.

3 METHODS

The research methodology is based on the methods of system analysis and mathematical modeling. Comparative analysis of publicly available data and reports of domestic and foreign companies formed the basis for assessing possible risks as well as identifying positive factors. Conducting a study at a small business enterprise «Les I Sad». Utilizing methods for evaluating the security of information systems.

4 RESULTS

The modern theory of information security risk management is based on an interdisciplinary approach that combines management, information technology and applied mathematics, the key task of applying strategic planning in the company is to minimize information security risks, ensure the protection of company databases and ensure the stable functioning of company processes from external impact (Mezina, 2024). In 2024, the demand for information security has increased significantly, along with the number of external threats, according to the research of InfoWatch Expert-Analytical Center, the number of leaks from 2022 to 2023 increased by 61.5%, and in 2024 this value continued its growth.

When forming a strategy, it is important to take into account:

- Increased growth of attacks on company infrastructure through the use of bots, hackers' use of a huge number of Internet of Things devices (Suldin, 2023).
- Use of zero-trust methods. With this method, the system distrusts the device at every step, and every interaction with it. The system assesses the risk with each contact with the device. This method also works the other way around, where a company employee uses zero trust on every file and document.
- Increase in social engineering cyberattacks. As more and more hacker attacks are being repelled automatically by large companies, the "human factor" is always present.
- The need for companies to create data security-oriented architectures.
- Development and protection of domestic software.

- Implementation of corrective actions in the strategy - actions aimed at changing the strategy at certain stages of time (key points), in order to achieve flexibility of the strategy.
- Identification of information by level of criticality in the company.
- «The "newness" of cyber threats. Considering the evolution of cyberattacks on company information chains.
- Compliance with Russian requirements to data protection standards, monitoring of standards updates.
- Risks associated with partners, working with partner ecosystems and contractors.
- Reputational risks. Successful cyberattacks and information leaks significantly affect the company's reputation and the trust of customers and investors.

Considering the above factors when shaping a company's strategy can maximize positive impact and effective database protection. Depending on the industry, companies use different methods and approaches in risk management. Having ISO/IEC 27001 certification in many industries is a legal and regulatory requirement for data protection.

Table 1: Strategic planning approaches and models in information security risk management.

Name of approach	**Description of Strategies**		
	Description	***Advantages***	***Examples of applications***
ISO 27001	An international standard for information security management that provides a framework for protecting information.	System approach, compatibility with business objectives.	Banking, government agencies, quality management, food, medical products and medical devices, management systems (Koryakin, 2024).
NIST Cybersecurity Framework	A cybersecurity governance model based on five key functions: Identify, Protect, Detect, Respond, Recover.	Flexibility, adaptability to different industries	Technology companies, government, non-profit organizations, industry of all kinds.
SWOT-Analysis	A strategic planning tool for assessing internal and external factors affecting information security.	Simplicity, clarity.	Strategic planning in any industry.
Probability and impact matrix	A model that prioritizes risks based on their likelihood and consequences.	Focusing on critical threats.	IT infrastructure, critical systems.
Script analysis	A method for predicting possible threat scenarios and developing appropriate strategies.	Preparing for different scenarios	Energy, transport
COBIT Framework	IT process management model including information security aspects.	Integration of IT and business.	Large corporations, consulting companies, risk management.
Methods of big data analysis and AI	Using machine learning technologies to analyze threats and detect anomalies.	High precision, automation.	Cybersecurity, analytics platforms.

The period of worldwide and total era of data compromise is primarily related to the global stage of digitalization. According to a study by InfoWatch, in 2023, 94.5% of the world's total number of leaks were due to cyberattacks, 1.6% were intentional leaks due to the actions of an internal employee and 2% due to accidental actions of an employee, the remaining 1.9% were due to other unknown reasons. As of 2023, Russia's share in the global distribution of information leaks has almost halved - from 10.8% to 5.7%, but the number of attacks has not significantly decreased, this fact directly indicates the development of the domestic information security market. However, researchers at Verizon have noted an increase in leaks due to hybrid attacks that include both internal and external threats (Budi Gunawan, 2023). In this regard, the importance of control over the company's employees and the implementation of a system that does not allow a single employee access to the entire array of databases is emphasized.

The application of these recommendations on the example of the company «Les i Sad» contributed to:

- Reduced response time to external incidents. With a unified methodology for responding to an external threat, response time was reduced by 70%.
- Reduction of financial losses. Training of information security employees reduced by three times the number of successful phishing and other hacker attacks, and

consequently reduced the company's financial losses.

- Raising the level of employee awareness. Regular trainings and simulations helped to increase the level of awareness of information security issues among employees. This result confirms the need to invest in the human factor, which remains one of the most vulnerable points of the information security system
- Increase in the number of threats identified: The number of threats identified increased by 110% due to the use of modern data analytics technology and educated employees. This shows a significant improvement in the company's ability to predict and prevent incidents and identify threats as quickly as possible.

Table 2: Recommendations for strategic planning in information security risk management.

Recommendation	***Example of realization***	***Expected result***
Development of a single integrated strategy	Integrating information security risk management into digital marketing strategy to prevent customer data breaches	Minimize data leaks and increase customer confidence
Investments in personnel training	Conducting regular cybersecurity trainings and attack simulations.	Reducing the human factor in information security incidents.
Establishment of a centralized monitoring system.	Implementation of SOC (Security Operations Center) for real-time threat analysis and detection.	Reduced response time to incidents.
Regular review of the strategy	Annual risk audit and update of the security policy.	Adapting to new challenges and threats.
Use of modern frameworks	Implementation of ISO 27001 and NIST to establish a structured information security management system	Improving sustainability and process coherence.
Analysis and forecasting based on big data	Using AI to detect anomalies in network traffic.	Preventing potential attacks

An important rule is to increase control over e-mail, as according to Positive Technologies research, 92% of reported cases of malicious messages end up in e-mail, but the popularity of using messengers among scammers is growing rapidly. In 50% of cases, scammers' emails lead to a fake page for data entry.

Recommendations for strategic planning in information security risk management in table 2.

An important rule is to increase control over e-mail, as according to Positive Technologies research, 92% of reported cases of malicious messages end up in e-mail, but the popularity of using messengers among scammers is growing rapidly (Zhmurov, 2023). In 50% of cases, scammers' emails lead to a fake page for data entry.

5 DISCUSSION OF RESULTS

We propose the implementation of a performance table of their security strategy in the company. And tracking results after each strategy update, implementation of new defense methodology. An example is fig. 3. The data in the table demonstrates the effectiveness of implementing strategic planning in information security risk management based on the recommendations proposed in the article.

Any company can modify this table according to its needs. The authors recommend to use for small businesses the term of accounting for the implementation of changes in the strategy -1 year, for medium-sized businesses - 6 months, for large businesses - 3 months. It is recommended to check the relevance of the strategy on a monthly basis, and, if necessary, to correct it.

Internally, you can use an information security index (ISI) that takes into account key security components:

$$\text{ISI}=\frac{C\times W_1+T\times W_2+P\times W_3+R\times W_4}{W_1+W_2+W_3+W_4} \qquad (1)$$

The values in Eq. (1):

- C — assessing the level of compliance with legislative and legal safety requirements;
- T — assessment of the company's technological equipment in the field of information security;
- P — assessment of the level of training and awareness of personnel;
- R — assessing the effectiveness of the risk management strategy;

W1,W2,W3,W4 — weights of values, which reflect their relative importance (by default, the sum of weights is equal to 1. Using this formula allows the company to see the most unprotected parties in security, as well as the overall picture of the security system.

Table 3: An example of demonstrating the effect of implementing the concept of strategic planning.

Criterion	***Prior to implementation of the strategic planning concept***	***After implementation***	***Change (%)***
Number of successful cyber attacks	50 incidents per year	20 incidents per year	-60%
Incident response time	12 hours	4 hours	-67%
Losses from data breaches, million rubles	30	10	-66%
Level of customer satisfaction (%)	70%	90%	+20%
Compliance with regulatory requirements (%)	70	100	+30%
Information security awareness level of employees (%) (testing, survey)	50	85	+35%
Number of threats identified per year	200	500	+150%
External security audit	-	-	+15%

Companies working with critical information structure must necessarily use all possible modern methods of information protection. The Federation Council together with the Russian Ministry of Digital Technologies in December 2024 began to actively implement work to regulate and legalize the activities of “white hackers”, as part of the formation of a program in the country to search for vulnerabilities in government systems for a reward. The proposal of this bill on the importance of effective information security risk management, and shows the importance of the issue at the level of the country's security and economic and social stability (Mosechkin, 2023).

6 CONCLUSIONS

Data protection is becoming increasingly important from the government, introducing new data protection laws and legal acts, requiring companies to protect user data as much as possible. Effective information security risk management in the context of digital transformation requires a strategic approach based on the integration of information security into the company's management processes. The use of modern tools and models helps minimize risks and ensure sustainable business development. Further research can be directed towards the development of new methods of risk analysis, taking into account the specifics of different industries. Special attention should be paid to the introduction of artificial intelligence technologies and automation of risk management processes.

Application of recommendations on strategic planning in information security risk management allows to form an integrated approach to strategy development, ensuring business sustainability and successful secure implementation of information technologies. Taking each of the above aspects into account helps minimize the risks associated with cyber threats and adapt to dynamic changes in the digital environment.

REFERENCES

Lipatnikov, V. A., Shevchenko, A. A., Melekhov, K. V., Tkachev, D. F., 2024. Methodology for improving the security of data transmission network of critical information infrastructure objects under multi-stage attacks. *Information and Management System.* №. 1 (128). pp. 44-55.

Kosinskaya, A. R., Demkin, D. A., 2024. New Generation Firewalls (NGFW): review, technologies, representatives. *Vestnik nauki.* №7 (76).Information Leaks in the World, 2022-2023. InfoWatch Expert-Analytical Center. 2024.

Neves, A., Araujo, V., 2023. Smart automation in cybersecurity intressts. *Foresight.* № 1(19). pp. 89-97.

Shabaeva, S. V., Shabaev, A. I., 2024. Risks of implementation of digital platforms as an industry aspect of strategizing digital platforms as an industry aspect of strategizing. *Strategizing: Theory and Practice*. №2. pp. 193-207.

Mirgaleeva, I. V., Shamsutdinova, M. R., Bogdanov, A. A., 2022. Risk management of the company in the process of its digitalization. *Vestnik RUK*. №3 (49). pp. 26-31.

Dmitrieva, M.A., Shedko, Y.N., 2023. Digital trends in strategic management and existing IT risks. *Management Sciences*. №2. pp. 6-15.

Drozdova, D. V., 2024. Risk management within the framework of ensuring cyber security of fuel and energy complex enterprises. *Theory and Practice of Modern Science.* №7 (109). pp. 30-41.

Mezina, N. A., Lunev, V. C., 2024. Conceptual and strategic directions of increasing economic security as a factor of sustainable development of enterprises. *Scientific Proceedings of the Free Economic Society of Russia*. №4. pp. 507-517.

Solominskiy, A. V., Zhelezin, V. A., Mirgorodskiy, A. D., Krasnobaev, S. V., Kolotilina, N. M., 2023. Actual trends in the market of information security. *Bulletin of Science and Education.* №8 (139). pp. 22-27.

Suldin, K. N., Madaeva, O. S., Heath, E. V., 2023. Economic security in a commercial organization. *Innovatsionnaya nauka*. №5-2. pp. 85-88.

Koryakin, S.V., Dijo D., 2024. Methods for managing projects for the secure information systems. *ELS.* №30. pp. 184-196.

Gunawan, B., Barito Mulho, R., Abdullah, A.G., 2023. Strategic management of cybersecurity. *Foresight.* № 3 (17). pp. 88-97.

Zhmurov, D.V., 2023. Digital theft: the concept, victims and their classification. *All-Russian Criminological Journal.* № 1 (17). pp. 35-43.

Shkradyuk, A. D., 2022. Security assessment of information systems using penetration testing. *Smart Digital Economy*. № 4. pp. 18-30.

Mosechkin, I.N., 2023. Problems of Criminal-Legal Protection of Critical Information Infrastructure of the Russian Federation. *All-Russian Criminological Journal*. № 1 (17). pp. 22-34.

Ismagilov, I. R., Akhmetshina, R. I., Gilmanova, E. A., 2022. Modeling of security threats in the protection of critical information infrastructure objects. *Economics and Socium.* №2-2 (93). pp. 645-648.