International Journal of Management, IT & Engineering
Vol. 12 Issue 11, November 2022,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CYBER RISK MANAGEMENT ISSUES AGAINST CRISIS IN CORPORATE STRUCTURES

ALIQULOV AZIZ HAYDARJONOVICH

Abstract

This article covers organizational and methodological issues of establishing a cyber risk management system in corporate structures and forming new ideas. Based on this, the methods of determining the stages of combating cyber risk in corporate structures and developing management measures against cyber risk were considered. In addition, the content and essence of modern practice of innovative management against cyber risk in corporate structures was researched.

Keywords:
cyber security, risk management, cyber attack, cyber threat, corporate structure, cyberrisk assessment

Author correspondence:
ALIQULOV AZIZ HAYDARJONOVICH
Doctoral student at the department of"Regional economy and management",National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan,
Email:aziz100792@mail.ru

INTRODUCTION

In modern society, the number of cyber attacks on corporate structures is doubling.As a result, attacks that cause extreme damage are becoming commonplace.Cause of cyber attacks, the financial costs of the enterprise are increasing and causing the biggest losses. In addition, another trend is that the increase in the number of cyber attacks on critical infrastructure and strategic industrial facilities can lead to the failure of systems that support human life and the emergence of global man-made disasters.Therefore, risk management against cyber threats is one of the priorities for the development of organizations around the world and is absolutely necessary for their further activities.Objectives and approaches to cyber risk management in corporate structures, the objective of any organization has certain indicators that describe the results of its activity.

For example, for commercial enterprises, it is profit, increase capitalization, market share or turnover, and for public organizations, it is the provision of public services to the population and solving management problems.In any case, regardless of the purpose of the organization's activities, it is possible to facilitate the achievement of the intended goal by focusing on information security.At the same time, each organization assesses cyber risks in its own way, depending on the line of activity.Thus, the goal of cyber risk management is to keep them at an acceptable level for the organization.To solve this problem, organizations create integrated cyber security systems.When creating such systems, the issue of choosing protection tools that ensure the reduction of information security risks identified during the analysis without excessive costs for the implementation and support of these tools is on the agenda.The analysis of cyber risks in corporate structures allows the

formation of a set of necessary and sufficient information security tools, as well as the identification of organizational measures aimed at reducing cyber risks in corporate structures and the development of the architecture of the information security system, which is the most effective for the specific activities of the organization and is aimed at reducing its risks.

All cyber risks are characterized by two parameters: the damage that can be caused to the organization and the probability of its implementation.Using a combination of these two features for risk analysis allows comparing risks with different levels of damage and probability.As a result, minimization of cyber risks that may occur in the corporate structure, development of management decisions against cyber threats, and prevention of possible negative consequences create an opportunity to monitor the management process.Identification, analysis and assessment of cyber risks in corporate structures is based on the identification and analysis of vulnerabilities that may be affected by the risks and threats inherent in their assets, and their implementation can be through the identification of these vulnerabilities.

Also, the assessment of cyber risk methods used in corporate structures is based on its methodology, the model of the attacker, information about the organization's business processes and other factors related to the implementation of the risk, for example, the political, economic, market or social situation in the environment of the organization's activities, preliminary data for their assessment can be used as.

The advantage of the quantitative approach in corporate structures is the accuracy of the risk assessment, the visibility of the results and the ability to compare the value of the risk expressed in money with the amount of investment required to respond to this risk, the disadvantages are complexity, high labor intensity and execution time.

The level of cyber risk acceptable to a corporate organization determines the criteria used in the decision to accept or eliminate the risk.Based on this criterion, it is determined which risks identified in the future will be taken for granted and excluded from further consideration, and which will undergo additional analysis and be included in the risk response plan, and will be classified as follows:

Cyber risk avoidance;
Cyber risk acceptance;
Cyberrisk transfer;
Reducing cyber risk;
Countering cyber threats;
Description of cyber security classification measures;

A project team will be established to analyze and assess cyber security risks, including:

- At the same time, the project team in corporate structures does not attempt to obtain or develop accurate numbers to estimate the probability or magnitude of annual losses due to the implementation of cyber security threats in corporate structures, unless the data is available to determine the cororative management factors.Instead of calculating exact numbers, the team relies on their collective knowledge of threats and vulnerabilities and their impact on the organization's core operations.Requires excessive time and effort to develop, document, and verify accurate and detailed cybersecurity risk assessments;
- Risk documentation becomes excessively voluminous, which greatly complicates its practical application;

- An accurate assessment of the probability of losses and threats is necessary to rank cyber risks in corporate structures and set priorities for their resolution;
- Thus, in corporate structures, a list of high-level cyber security risks is identified in relation to the main activities of the organization. After the risks are identified and assessed, the project team defines the safeguards that can be applied to mitigate each of the cyber security risks in the identified corporate structures.

LITERATURE REVIEW

During the session of analysis and assessment of information security risks against cyber threats in corporate structures in modern literature, the project team conducts brainstorming exercises, which identify the weak points of objects, the possibility of potential threats to confidentiality, integrity and availability, which have been considered in the field of analysis for years.

What is being done is the damage caused to the main activity of the management. Instead of calculating exact numbers, the team relies on their collective knowledge of threats and vulnerabilities and their impact on the organization's core operations.

It can be used as a starting point to define governance in corporate structures, prioritizing the most cost-effective controls that provide maximum effectiveness at financial cost against cyber risk.Based on the proposed cyber security measures by corporate management, a risk mitigation action plan is drawn up and approved by the organization's management.

For example, (H. M. Government 2016) According to the Government, the importance of cyber security in corporate structures cannot be ignored, because any cyber attack on them will have a major impact on the security of corporate structures, for example, harming its economic stability.

In addition, the opinions of other scholars are interpreted: K. Renaud and G R.S. Weir (2016).Cyber risk in enterprise structures describing cybersecurity threats in large and medium-sized enterprises can be a key solution in helping to understand the basic concept of cyber security in large and medium-sized enterprises.Corporate cyber risk management in corporate structures is usually at risk of cyber-attacks such as data breach, data destruction and denial of access to data.This can have a negative impact on the activities of any corporate managements.

The analysis of the literature on this issue shows that all the problems of establishing corporate governance against cyber risks in corporate structures can be grouped into:

C.T. Berry and R.L. Berry, (2018)estimating the cost of a cyber attack is a real challenge in corporate governance against cyber risks in corporate structures, as some cyber incidents have not yet been announced or are still invisible.In most cases, the root cause includes weak defense techniques, less experience, unknown outsourcing, and outdated security practices used by small, medium-sized businesses in corporate structures compared to larger firms.While some small and medium-sized businesses may recognize the possibility of cyberattacks, they may fall victim to these incidents due to a lack of skills, resources, and indecision.

At this stage, in the process of analyzing cyber risks information risks in corporate structures, a series of interviews are held with interested parties, including those responsible for the operation, administration, security and use of the assets under risk analysis.As a result, a formalized description of the area, its boundaries, and the composition of persons participating in the risk analysis are determined for further research.

M. Bada, A. M. Sasse, and J. R. C. Nurse (2019)corporate entities need to be aware of the consequences of cyber security and try to address it, as this awareness can lead them

to adopt appropriate behaviors.A study conducted in corporate structures showed that they need more information about possible vulnerabilities than implementing self-assessed risk assessment tools, so they should immediately develop the content of their special awareness programs.

Meanwhile, Abraham C., Chatterjee D., and Sims R.R. (2019) The cyber risk assessment layer in corporate structures plays a central role in the cyber risk management system.Provides a three-step approach to understanding, assessing and mitigating cyber security risks.

1.Risk identification that pinpoints potential cybersecurity threats, vulnerabilities, and attacks against cyber risks in corporate structures;

2.Risk quantification, which determines the magnitude and frequency of cyber-attacks and prioritizes attack types against cyber risks in corporate governance.

3.A cyber risk investment analysis that examines the cost-benefit and investment decisions of cyber investments in cyber risk infrastructure in corporate structures.

At the same time, Hernandez-Ramos, J.L. Scarmeta, and A.F. Toward (2019)who expressed their opinions about the use of various strategies against cyber threats in corporate structures.For example, improving cybersecurity in corporate governance requires manual tasks, expanding employee knowledge and tools, and addressing risks with vendors and other third parties.Device security certification is critical to device adoption, but the dynamic and heterogeneous nature of devices makes developing a cybersecurity certification system technically and legally complex.

Additionally, Jason Kick (2014) argues against cyber risk in corporate structures: in corporate governance, attacks on information systems and the digital infrastructure of one or more sectors of the economy come from various sources and include denial-of-service attacks.In the service, the spread of malicious viruses that damage the network of the corporate management and use security gaps to access confidential information, as well as fake e-mails with requests for confidential information from an unsuspecting employee, phishing, motivated cyber security attackers in threat modeling during exercises and the identification of the attack vector stimulate the active work of listeners.

RESEARCH METHODS

The methodology used in this study was to study the issues of improving cyber risk capabilities in corporate management, and used analysis, synthesis, and abstract-logical and critical thinking, as well as generalization methods.As a result, the above-mentioned methods are effectively used in the development of conclusions and suggestions on the use of digital technologies, licensed software products that are well protected against cyber risks in corporate enterprises.

ANALYSIS AND RESULTS

At present, in the economic literature, the authors use the concept of "cyber risk" more often in corporate structures.Relative to this industry, the vulnerability of critical infrastructure to external and internal cyberattacks in a corporate structure increases as its dependence on information technology increases.These attacks can include cyberattacks that threaten a nation's economy, public works, communications systems, computer networks, and other critical infrastructure.In such conditions, it is necessary to develop and manage cyber risk infrastructures in corporate structures.

The interconnection of information and cyber systems in corporate management creates additional risks in the field of information security, therefore, management of system risks in corporate management requires cooperation and information sharing, encourages the search for new methods and tools for monitoring, identifying and neutralizing cyber threats.Systemic risks are interconnected and spread across

interdependent systems, overcoming the limits of situational awareness or operational control. Risks are especially dangerous in finance, public administration.

Systemic risk begins with a distributed vulnerable state that changes with the complexity of social and technological systems. A source of risk may be the dependence on information and communication technologies of interconnected systems that support an expanding range of applications.In corporate governance, system risk can be used by an attacker to destabilize or destroy critical functions. Individual triggering events accumulate and lead to escalating adverse consequences as damage increases.As a result, there are cascading effects that can affect both individual corporate information systems and the digital infrastructure of one or more sectors of the economy.

In corporate management, the kramm methodology against cyber risk is used and can be divided into the following:

•A time-proven method that has accumulated extensive experience and professional competence against cyber risk in corporate management; kramm application results are recognized by international institutions and corporate organizations;

•The existence of a clear formalized description of cyber risk methodology in corporate management minimizes the possibility of errors in the implementation of risk analysis and management processes;

•The availability of risk analysis automation tools in the corporate management process allows to minimize labor costs and time for risk analysis and management activities;

•Catalogs of threats, vulnerabilities, consequences, information security measures simplify the requirements for special knowledge and skills of direct performers of risk analysis and management activities;

•High complexity and labor intensity of initial data collection, which requires the involvement of significant resources inside or outside the corporate organization;

• Significant resources and time are spent on implementing information risk analysis and management processes against cyber risk;

• Involvement of a large number of interested parties requires significant costs for the organization of joint work, communication and coordination of results in the corporate organization;

• The impossibility of evaluating cyber risks in monetary terms makes it difficult to use the results of information security risk assessment in the feasibility study of investments required for the introduction of information security tools and methods.

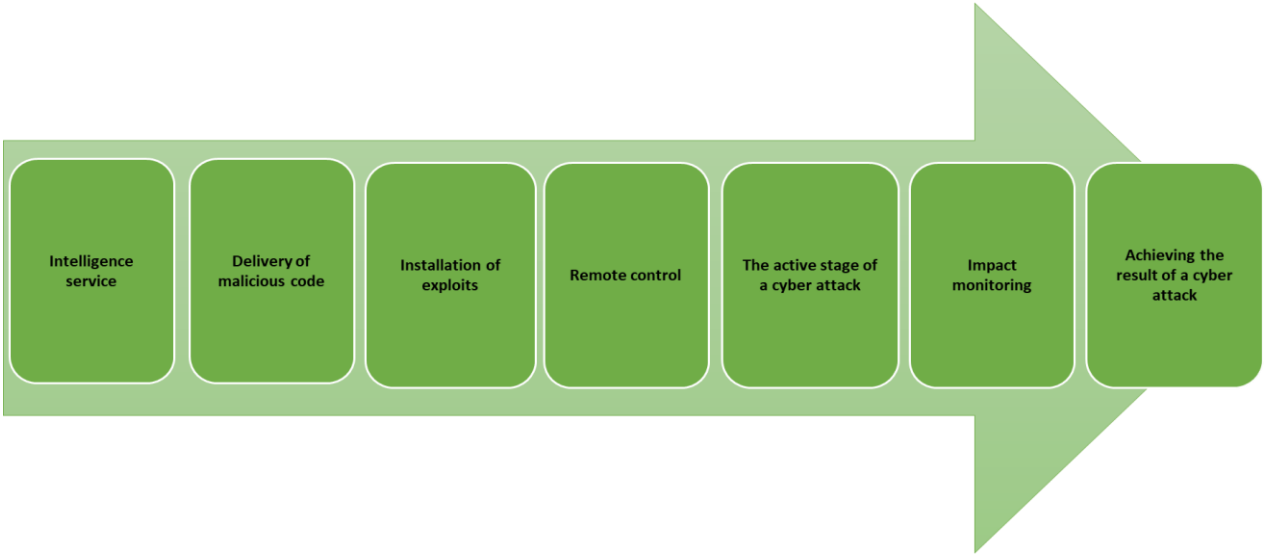


Figure 1.General scheme and classification of cyber attack in corporate management
[1]

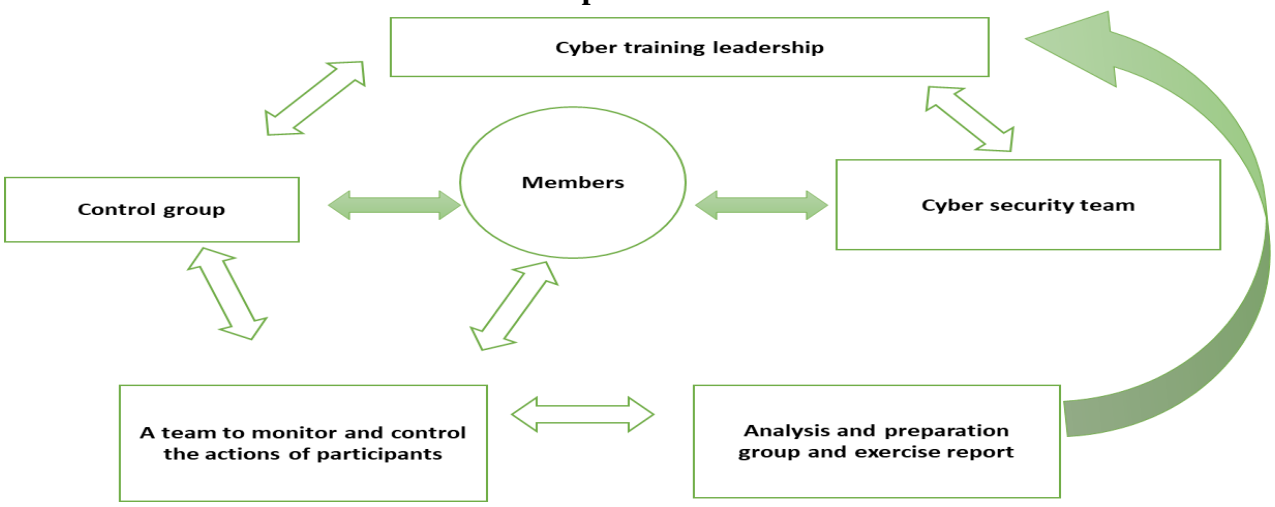
The rapid implementation of information technologies against cyber risks in the proposed corporate management makes it more urgent to study, generalize and analyze abroad in many areas of human activity. Improving local systems for responding to cyber incidents involves developing cyber risk practices and learning how to model learning environments in corporate structures and learn how to deal with simulated cyber attacks.

In corporate governance, cyberattacks are usually detected using signature, behavioral, combined, and other methods. In today's cyber-attack landscape, the creation of intelligent defenses that enable the detection of targeted attacks in the early stages of execution is at the fore.A distinctive feature of a cyber attack is its operation through interaction with the global cyberspace, which has a devastating effect on state and municipal systems, economic objects without directly entering the state territory.

In a cyber attack, it is possible to target an attacker, remotely control and switch to operational mode, malfunctions in automated work and disable objects. It is especially dangerous to transfer an object to a critical mode of operation, which will lead to its destruction. Simulating cyberattacks is an important stage of training in cyberspace training. Modeling is based on the formalization of a logical chain: the interaction of a set of detected software vulnerabilities, relevant threats, possible scenarios of threat implementation, possible cyber-physical consequences of quantitative assessment of cyber security risks.

In educational technical tasks, a number of restrictions are introduced to ensure the safety of real processes, which facilitates the formalization process. Using cyber technologies in the new economic environment, by simulating real security events and threat dynamics, one of the experimental methods is to create realistic scenarios of cyber attacks on target systems in a simulation environment, to facilitate the training of experts in choosing the most appropriate responses, the scenarios are mainly simulated or simulated networks.

Figure 2. Scheme of cyber risk management through team building method in corporate structures[2]



[1]researcher development
[2]It was prepared based on the author's research

Foreign experiences against cyber risks in corporate management help to improve the quality of direct information exchange during the response to cyber attacks, and to form a collective ability to repel cyber attacks.Ultimately, the speed and efficiency of information exchange in responding to an incident affects the ability of responders to minimize the consequences and respond to the incident in a timely manner.

A model of organizing cyber exercises was developed as a result of studying foreign experience, analyzing scientific publications and reports published by foreign journals on cyber exercises in the context of increased risk of cyber attacks.Based on the study of foreign experience in conducting cyber exercises to combat cyber threats against protected information resources in the context of increasing complexity of interdependence and interdependence of corporate governance, substantiates the relevance of solving the scientific problem of assessing the risk of offense and draws the following conclusions:

1.On a modern organizational and technological research platform to conduct cyber risk exercises in corporate management, analyze threats, inform participants, interested parties and organizations about new threats and their consequences, development trends, take preventive measures by identifying them and improving their toolsprevent cyber attacks.

2.Exercises against cyber risks in corporate management allow objectively studying, monitoring and evaluating in a controlled environment the foreseeable large-scale effects on the interconnected and interconnected distributed information and cyber-physical infrastructures of society, corporate management and other organizations.

3.When ensuring information security in corporate management, the main attention should be paid to taking into account the interdependence of a large number of cyber incidents and communications, coordination and cooperation of the response measures of the interested corporate structure and private organizations.

4.In corporate settings, threat and communication analysis enables security professionals to identify early problems, enabling organizations to analyze incidents and identify malicious certificates and ransomware to protect their networks.

5.The development and introduction of common terminology in corporate structures serves to improve coordination in the field of information security and increase the efficiency of information exchange.

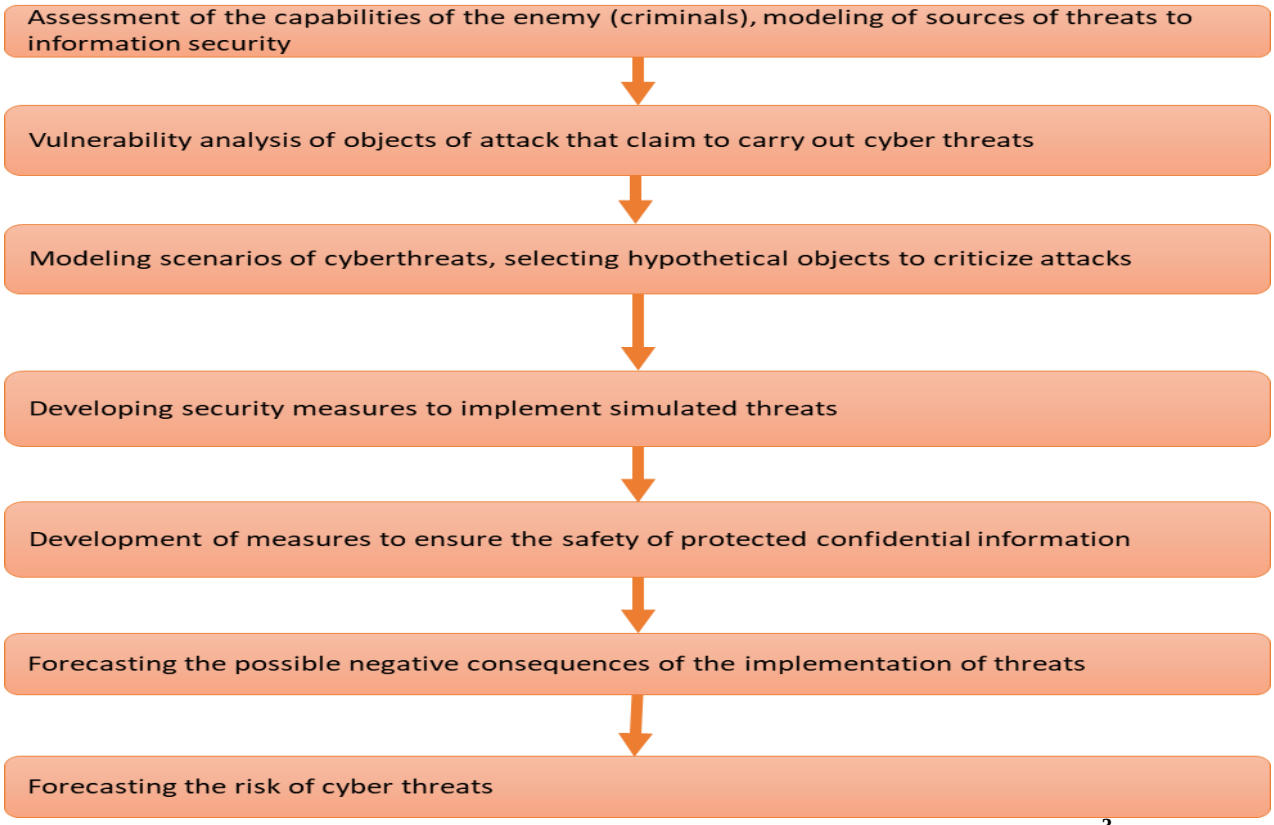


Figure 3.Principles of cyber attack simulation in corporate structures[3]

The method of simulating a cyber attack in corporate structures can be defined as follows.The goals of the simulation during the exercises are to find optimal solutions for a systematic response to the external effects of planned, as a rule, cyber attacks.Also, to evaluate the effectiveness of the decisions taken on the neutralization of cyber threats and to study the sensitivity of the complex.The conditions and factors that undermine the security of the information being processed, and lead to disruption of the systems and networks are determined.

In corporate structures, simulation modeling is aimed at obtaining new knowledge on information security under predetermined conditions when there is preliminary information about the objects of destructive impact on the studied information infrastructure elements in the created educational environment.The model may include a systematic list of information security vulnerabilities that originate from anthropogenic, man-made, or natural sources.The modeling process includes the development of information for the listeners who, after identifying the signs of the incident, make decisions about neutralizing threats and adapting security systems to the changed situation.This requires the use of automated methods to determine the most suitable for their modeling. We propose to present the modeling process in the form of a scenario model for the initiation of cyber threats.

In order to counter cyber threats and protect information assets in corporate management, organizations need to detect and remediate in real-time the security situation against attacks detected on their expanding surface.Nowadays, the essence of cyber

[3]Developed by the researcher

exercises is to test the response to simulated threats. In order to analyze the application of the modeling method in conducting large-scale cyber exercises, it is appropriate to review and summarize foreign experience in corporate management.During strategic exercises in an environment created with security measures, developers propose cyberattack scenarios that are as close as possible to real and potential threats.

CONCLUSIONS

Based on the above analysis, we summarize the conclusions and the achieved results:

It is defined as part of a general management system based on the use of business risk assessment methods for the development, implementation, operation, monitoring, analysis, support and improvement of information security against cyber risk in corporate management.A management system includes, uses, and allocates organizational structure, policies, activity planning, allocation of responsibilities, practices, procedures, processes, and resources.

• A time-proven method that has accumulated extensive experience and professional competence against cyber risk in corporate management; kramm application results are recognized by international institutes and corporate organizations.

•A time-proven method that has accumulated extensive experience and professional competence against cyber risk in corporate structures; kramm application results are recognized by international institutes and corporate managements.

•The availability of risk analysis automation tools in the corporate management process allows to minimize labor costs and time for risk analysis and management activities;

•Catalogs of cyber threats, vulnerabilities, consequences, information security measures in corporate management simplify the requirements for special knowledge and skills of the direct performers of risk analysis and management activities.

REFERENCES

1 I.T.Union, “Series X.Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity,” pp. 2—-3, 2008

2 H.M.Government, “National Cyber Strategy,” p. 43, 2016.

3 K.Renaud and G. R. S. Weir, “Cybersecurity and the Unbearability of Uncertainty,” in 2016 Cybersecurity Cyberforensics Conf. IEEE, 2016, pp. 137–143.

4.C.T. Berry and R. L. Berry, “An initial assessment of small business risk management approaches for cyber security threats,” Int. J. Bus. Contin. Risk Manag., vol. 8, no. 1, pp. 1–10, 2018.

5 M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber security awareness campaigns:Why do they fail to change behaviour?” arXiv Prepr. arXiv1901.02672, 2019.

6 Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, 62(4), 539e548.

7 Matheu, S.N.Hernandez-Ramos, J.L.Skarmeta, A.F.Toward a cybersecurity certification framework for the Internet of Things. IEEE Secur. Priv. 2019, 17, 66–76. [CrossRef]

8.JasonKick.Cyber Exercise Playbook November 2014.URL:http://www.mitre.org/s/pr_14-3929-cyber-execise-playbook.pdf (дата обращения: 18.01.2022).