Lex Humana, v. 15, n.2, 2023, ISSN 2175-0947

CYBERCRIMES IN THE GLOBAL SECURITY SYSTEM IN MODERN CONDITIONS

CIBERCRIMES NO SISTEMA DE SEGURANÇA GLOBAL EM CONDIÇÕES MODERNAS

KOSTIANTYN BUHAICHUK
Kharkiv National University of Internal Affairs, 61000, Kharkiv, Ukraine
klbugaychuk@gmail.com

WOLODYMYR WARAWA
University of Customs and Finance
Ukraine
warawa@ukr.net

TETIANA BATRACHENKO
University of Customs and Finance, 49000, DNIPRO, Ukraine
tatianabatrachenko@gmail.com

BOGDANA CHERNIAVSKA
National Academy of Management, 03151, Kyiv, Ukraine
bogdana54321@gmail.com

VOLODYMYR KONDEL
Poltava V.G. Korolenko National Pedagogical University, 36000, Poltava, Ukraine
vkondel@i.ua

Received: 15 Jan 2023
Accepted: 05 Mar 2023
Published: 14 Mar 2023

Corresponding Author:
vkondel@i.ua

Abstract: The development of the information and digital world determines the formation of new public requests, firstly, to ensure the security of cyberspace. The development of social tasks that can be solved using information technologies is constantly growing, therefore the number of cybercrimes is increasing, and their specifics are changing. An analysis of the development trend of cybersecurity and cybercrime showed that the number and scale of cyberattacks will continue to grow. Accordingly, the purpose of the article is to find the development directions of approaches to ensuring security in cyberspace in accordance with modern global challenges. The article determines that new global challenges have significantly changed the system of people's life conducting financial transactions, trade, receiving services (administrative, communal, social, and household, etc.), and providing communication systems. In the conditions of the pandemic, the processes of all spheres of human activity only spread. The analysis of digitalization models for ensuring cybersecurity is presented in the article but needs clarification and further development, which relates to new global challenges in the security architecture in the world and on the European continent. The article considers approaches to ensuring the effectiveness of cybersecurity in new social conditions. The article uses the methods of control charts to conduct a sociological survey to rank the factors of influence on the cause-and-effect relationships of cybersecurity. The put-forward hypothesis regarding the structuring of influencing factors allows us to systematize directions for further research. The projection of the trend line of the number of cyberattacks and the number of subjects subjected to cyberattacks in the analyzed period determines the scaling and complication of protection processes both at the company level and at the state level.

Keywords: Cybercrime. Cyber-attacks. Cyber security. Information technology. National security.

Resumo: O desenvolvimento da informação e do mundo digital determina a formação de novos pedidos públicos, em primeiro lugar, para garantir a segurança do ciberespaço. O desenvolvimento

de tarefas sociais que podem ser resolvidas utilizando as tecnologias da informação está em constante crescimento, portanto, o número de cibercrimes está aumentando, e suas especificidades estão mudando. Uma análise da tendência de desenvolvimento da segurança cibernética e dos crimes cibernéticos mostrou que o número e a escala dos ataques cibernéticos continuarão a crescer. Assim, o objetivo do artigo é encontrar as direções de desenvolvimento de abordagens para garantir a segurança no ciberespaço, de acordo com os modernos desafios globais. O artigo determina que novos desafios globais mudaram significativamente o sistema de vida das pessoas, conduzindo transações financeiras, comércio, recebendo serviços (administrativos, comunitários, sociais e domésticos, etc.), e fornecendo sistemas de comunicação. Nas condições da pandemia, os processos de todas as esferas da atividade humana só se espalharam. A análise dos modelos de digitalização para garantir a segurança cibernética é apresentada no artigo, mas necessita de esclarecimento e desenvolvimento adicional, que se relaciona com os novos desafios globais na arquitetura de segurança no mundo e no continente europeu. O artigo considera abordagens para garantir a eficácia da segurança cibernética em novas condições sociais. O artigo usa os métodos de gráficos de controle para conduzir uma pesquisa sociológica para classificar os fatores de influência nas relações de causa e efeito da cibersegurança. A hipótese de adiamento em relação à estruturação dos fatores de influência nos permite sistematizar direções para futuras pesquisas. A projeção da linha de tendência do número de ciberataques e do número de sujeitos submetidos a ciberataques no período analisado determina a escala e a complicação dos processos de proteção tanto a nível da empresa quanto a nível do estado.

Palavras-chave: Cibercriminalidade. Ataques cibernéticos. Segurança cibernética. Tecnologia da informação. Segurança nacional.

1. Introduction

The development of the digital world involves a shift in emphasis from issues of social development to problems of information and digital provision of society, which becomes one of the main requests. The development of information technologies involves the transition of the population from traditional to remote work formats, which affects most areas of human life: shopping, work, study, recreation, leisure, receiving news information, making payments, maintaining bank accounts, and providing administrative or communal services. All life processes are digitized, which requires the search for safe mechanisms for the implementation of such processes in digital spaces. The main source of competitiveness of the country and individual businesses are digital technologies and the degree of their implementation in practical activities. Today, there are 4.66 billion Internet users in the world, which is more than 59.5% of the global population. This indicator grows in geometric progression. Most Internet users are classified as young and middle-aged; therefore, it is reasonable to predict an increase in the growth rate of the number of Internet users in the world. As the number of Internet users grows, the needs and requests for receiving digital services and using digital resources will grow. Most of Internet usage is associated with the need to create and work with personal data, including financial data. In

2021, more than 20 billion payments and other personal data were recorded on the Internet. The main task of organizing cyber security systems is to protect personal data and reduce the possibility of their leakage. In the past year alone, 1.2 billion data breaches have been recorded, the majority of which are in the healthcare sector. This specificity is related to the Corona Virus pandemic, but any other industry that has potentially hackable data can be attacked. The number of information leaks shows the great relevance of the processes of finding effective methods of data protection and combating cyber-attacks. Therefore, the article has high relevance and practical importance.

The purpose of the article. Therefore, the purpose of the article is to develop proposals for ensuring the security of personal data and preventing cyberattacks by accumulating informational and analytical support that characterizes cause-and-effect relationships and trends in the development of cyber security in the world. To achieve the goal of the study, the following tasks were performed:

- an analysis of theoretical approaches and methodological support of the concept of cyber security was carried out,
- the trend of the development of security processes in cyberspace is determined,
- the results of the number and causes of leaks of personal data were analyzed,
- the development trend of personal data leakage processes was developed and mathematically substantiated and modeling of the structure of the causes of such leaks was carried out,
- proposals were developed to ensure cyber security in the global security architecture, considering modern challenges and perspectives.

2. Literature review

The development of information technologies and the digitalization of life support processes at all levels determine the relevance of research work aimed at protecting information support processes. Despite the automation of digital processes, the human factor is always decisive in any direction of social development. Analyzing the degrees and results of human influence on the processes of information provision and digitization, the practical significance of a separate direction of finding ways to ensure cyber security was

developed and substantiated. This direction studies the issue of the human factor in digitalization processes, considering how intentional interference in the work of information systems, their damage, accidental leaks of information, leaks of information due to the lack of necessary knowledge and competencies, as well as the deliberate design of digital systems aimed at criminal purposes. It is advisable to consider the human factor in the information provision system from the point of view of technical-technological, socio-economic, socio-political, and psychological aspects. The issue of ensuring digitization processes with technical and technological tools determines the need for the population to develop appropriate digital skills and competencies that help not only navigate the digital space, and use its advantages in everyday life, but also ensure the security of one's own information. For example, such tools can be a system for developing a password, two-factor identification, notification systems, and systems for entering programs using biometric data, which can be implemented only if the public is aware of such procedures and understands the need for their use. Socio-economic aspects of the development of digital processes consist of the level of education, qualifications of the population (the higher the level of the Soviet, the more effective the information protection tools work), as well as the definition of the population's standard of living. The development of information technologies, accordingly, the development of systems for the protection of information technologies and personal data takes place in developed countries. Developing countries have a lower level of use of digital technologies, but also a significantly lower level of cyber security. Poor countries have the lowest levels of information security, yet the small number of digital operations that take place in these countries are virtually immune to outside interference in cyberspace. Socio-political factors consist in ensuring national security by limiting opportunities to intervene in national systems of defense, finance, banking, provision of administrative services, social security, etc. The psychological aspect consists of the development of separate hypotheses of psychological response to certain digital processes by analyzing the human factor using various behavioral and social-cognitive theories. Behavioral factors affecting behavior in ensuring cyber security in organizations whose activities are related to the collection, processing, analysis, evaluation, and use of personal data are studied. Thus, a structural and logical scheme of cause-and-effect relationships of the influence of human factors on the processes of ensuring cyber security in organizations was formed [AL-Nuaimi, M.N. (2022)].

Management of the processes of ensuring the cyber security of organizations is related to the protection of the personal data of clients and ensuring the confidentiality of information. Considering cyber security as an element of strategic management, it is precisely determined that the management of cyber security consists in the implementation of functions of planning, organization, and control. These functions determine the development and assessment of the system of indicators for ensuring cyber security, the establishment of those responsible for their implementation and the terms of implementation, and the implementation of organizational measures aimed at technical, technological, and resource support for the implementation of the tasks set in the plans. The control system provides for the comparison of planned and actual resulting indicators to identify deviations and develop corrective management decisions. This approach to the definition and theoretical and methodological understanding of cyber security processes is aimed at ensuring the competitiveness of organizations in the conditions of global business challenges [Tuna, A.A. and Türkmendağ, Z. (2022)].

The banking sector is the most vulnerable to cyber-attacks. The financial data of customers must be reliably protected, which determines not only the financial security of the institution but also the creation of an image of a reliable, safe, stable banking institution that has additional bonuses over competitors. Analyzing information leaks in banking systems, several authors note that the human factor is crucial in ensuring the security of banking operations. The influence of human factors on the cyber security of the banking system can be divided into two factors: the human factor of the employees of the banking system, and the human factor of the users of the banking system. If the first category is more typical of issues of technical and technological organization of cyber security. It is important for consumers to be familiar with the processes of electronic banking and to understand the possibilities for protecting personal data and financial data. The development of the electronic banking system determines the relevance of the processes of increasing the digital literacy of the population [TN, N. and Shailendra Kulkarni, M. (2022)]. These processes become especially relevant in the conditions of quarantine restrictions caused by the global pandemic and military actions in the center of Europe, which were provoked by the full-scale military aggression of the Russian Federation. An important task of researching cyber security processes, considering new global challenges, is the early detection of cyber-attacks and the development of effective countermeasures

aimed at preventing and eliminating the negative consequences of external influences on business processes [TN, N. and Shailendra Kulkarni, M. (2022)].

Business processes that are translated into digital formats are subject to special cyber security. Digital business development is the main form of competitiveness in the new conditions of modern economic development. However, the disadvantage of digitization is the need to develop conceptual approaches and methodological foundations for ensuring the security of processes within the framework of business development and operation. It is interesting to study the role of online platforms in the withdrawal and money laundering system during attacks on businesses. The study, which was conducted based on the analysis of the results of interviews with representatives of the cyber security field, whose main task is the prevention and prevention of cyber-attacks, allowed us to develop a hypothesis that the prevention of money laundering processes is the basis of ensuring cyber security. The veracity of the hypothesis was proven by analyzing the development trends of several companies that used methods of monitoring and checking the operation of online platforms when conducting financial transactions [Wronka, C. (2022)].

Cybersecurity issues are relevant not only at the level of individual consumers and businesses. The national security of the country today is directly related to ensuring the security of digital processes and information technologies. Cybersecurity issues determine the potential for the development of social, economic, and political processes. Global challenges of information development began to take shape already in the 1980s, when information support technologies began to develop, from the 1990s Internet processes gained active development, and with the beginning of the 21st century and the development of international communication systems, the processes of digital and information security acquired a global character. It is interesting to study the digital conflicts that arise in the business infrastructure, which consists in a detailed study of the infrastructure of business processes, the use of digital technologies when using the infrastructure, the determination of problematic aspects (digital conflicts) in the implementation of measures and business processes in cyberspace [Tamer, G., Tetik, G. and Oktay, S. (2022)].

Analyzing the approaches to determining the methodological basis of cyber security, three groups of approaches were accumulated: holistic, proactive, and adaptive. The grouping of approaches was carried out by analyzing the specifics of cyber-attacks that

were carried out on companies operating in different spheres of economic activity, so the cyber security management model developed based on the analysis can be considered unified. A comprehensive approach determines the consideration of the threat when carrying out cyber-attacks both for consumers (service characteristics) and for the company itself (financial, reputational, technical, and technological characteristics). A holistic approach to combating cyberattacks examines the interrelationships of a system of factors influencing cyber security. Proactive approaches determine opportunities to prevent cyberattacks, so they are focused on the development of security mechanisms before hacking, attacks, or data leaks. The adaptive approach has a flexible response system to challenges in accordance with the tasks set before the cyber warfare system. As a result of the analysis of research approaches, a dynamic end-to-end model of the cyber security service system was developed. The module has a cyclic nature and works in the "client-service-feedback-correction of deviations" system. Such a cyclical process allows to build up the experience of cyber risk management, which leads to a system of continuous improvement of the cyber security management system [Thomas, G. and Sule, M.-J. (2022)].

Numerous of studies by scientists are devoted to the development of methodological approaches to minimizing negative results in the event of cyber-attacks. The results of cyber-attacks can be non-fulfillment of contractual obligations, violation of human and citizen rights and freedoms in the system of restricting access to personal data. Realized cyber-attacks carry financial, legal, technological, and financial threats. In the research, it is proposed to apply the technology of predicting the consequences of cyber-attacks, which relates to the use of the F&S method. Such a system is an element of the company's risk management. The method has an adaptive nature to the market situation and is focused on the end users of services, that is, it has a client-oriented component. Numerous authors considered the possibilities of using the method in the system of ensuring national security. In particular, the researchers created models for the application of cyber-attack forecasting methods in the field of migration, executive power, infrastructural and transport security, and the food market based on the analysis of the experience of cyber protection systems in 177 countries of the world. The possibilities of using insurance systems as an element of combating cyberattacks are considered. The experience of the USA shows that the combination of technical and technological and insurance methods of financial protection has a great practical effect. In particular, the

cybersecurity insurance industry in the US was estimated to be worth US$7.36 billion in 2021, with constant growth. The formation of the trend line allowed us to determine that this indicator will be 27.83 billion USD in 2026, with an annual growth rate of 24.30%. Among the technical and technological factors, directions for the development of digitization processes, in particular cloud services, big data, mobile platforms, the Internet of Things, and artificial intelligence, have been determined. Researchers have developed proposals for the introduction of the developed proposals into the system of regulatory and legal support [Chhabra Roy, N. and Prabhakaran, S. (2021), Kaswan, K.S., Dhatterwal, J.S., Kumar, S. and Lal, S. (2022)].

Analyzing the goals of cyberattacks, the authors determined that cybercrimes can be related to the theft of personal data for the purpose of financial fraud, fraud, or blackmail. Also, cybercrimes in the field of national security were separately highlighted. Consideration of the specifics of these groups of cybercrimes determined the conditions for the development of methodical approaches to combating cyberattacks. Among the methods of conducting cyber-attacks, the following were identified: introduction of malicious software, spyware and phishing methods, attacks aimed at service interruptions, and others. All these forms of crimes in cyberspace can be used for both groups of cybercrimes: personal, aimed at the personal data of a person, and state, aimed at destroying or damaging the implementation of state administration functions.

Today, cyber-attacks are used for political and terrorist purposes. The term cyberwar has become generally accepted - conducting cyberattacks on objects that are important for the system of national security and state administration for the purpose of political influence. The term cyber war is used mostly in the analysis of national security, however, due to the use of similar attacks by business competitors, the concept of cyber war has entered operational business processes that characterize the unfair competition of competitors. Before the beginning of the full-scale military aggression of the Russian Federation against Ukraine, numerous cyberattacks on the national system of economic, financial, military, and civil support were observed. A similar example can be given with the intervention of hackers in the electoral process in the USA during the last presidential election of the country. Therefore, analyzing examples of cyber-attacks as elements of cyber war, the reasons (motives) of such attacks were identified: military, civilian, and ideological motives, espionage, sabotage, propaganda, interference in state administration systems, etc. Analyzing business cyber security processes, it is advisable to identify the

following most affected information systems and tools: e-mail, messengers, digital banking, online conferences and digital methods of production, and social networks. Therefore, when developing recommendations for the prevention and minimization of the consequences of cyberwars both at the national and at the level of the business environment, it is advisable to consider the experience described above for the development of a strategy and specific practical solutions [Asbaş, C. and Tuzlukaya. (2022)].

As mentioned above, the financial system is one of the main systems that suffer from cyber-attacks. The development of fraudulent schemes is also closely related to the spread of currency transactions in cyberspace, which became possible after the introduction of cryptocurrencies and the creation of cryptocurrency cyber exchanges. Among fraudsters, schemes for blocking accounts, withdrawing funds, manipulating prices when selling currencies on blockchains are popular. The development of digital asset markets and the low level of skills of working with such platforms and resources among the population leads to an increase in the number of frauds with cryptocurrency exchanges, crypto wallets, and platforms. Several authors analyzed journalistic articles devoted to fraud with cryptocurrencies, on the basis of which the main schemes of cyberattacks were determined. In particular, the problems of the anonymity of criminals in cyberspace, which makes it difficult to find them, and the imperfect system of regulatory and legal support for the protection of personal data and information resources were identified [Dupuis, D., Smith, D. and Gleason, K. (2021)].

Cyber spaces have received special development in the conditions of the coronavirus pandemic. Due to the need to reduce household contacts, most of the actions usual for a person have moved to the virtual space: remote work, making purchases in stores, receiving administrative services, etc. Such an impetus gave a powerful scaling to the processes of information development and the transition to virtual platforms. Accordingly, the number of cyberattacks on resources that are of interest to fraudsters has also increased. Firstly, the pandemic changed the system of relations between employees and management. It is worth talking about the search for effective mechanisms in the organization of the work process in a virtual format, which includes updating the processes of planning, work organization and control. Numerous of authors conducted a study of the problems of ensuring an effective business management system in the context of a pandemic by conducting interviews among representatives of various sectors of the

economy. In the period from November 2020 to February 2021, which is the most active period of quarantine restrictions in the world, a survey of managers and employees was conducted. It was determined that those companies that were able to establish effective work in the conditions of the pandemic with remote access cause more trust in employees, accordingly, are more resistant to external challenges, which affects the competitiveness of business in conditions of external challenges. Such companies did not lose the productivity of employees, but the employees in the interview noted that they have a negative psychological state due to the distance from the workplace and, accordingly, the inability to fully analyze and understand the current situation in the company. So, the authors of the study determined the following factors that influence the formation of the perception of work processes by employees under the condition of remote work: economic, social, financial, psychological, corporate [Panteli, N., Nurse, J.R.C., Collins, E. and Williams, N. (2022)].

The development of remote processes in the business environment implies the spread of problems with cyber-attacks. Changing concepts of management decision-making have identified threats of attacks on decision-making centers and communication setup centers, as well as communication flows. In research, scientists try to adapt traditional psychological and forensic theories to new challenges [Ma, K.W.F. and McKinnon, T. (2022)]. Analyzing financial systems, it is worth noting that the correlation analysis determined the most negative effects of cybercrimes specifically on financial institutions at the global and national levels [Wronka, C. (2022)].

Based on the theory of planned behavior, the relationships of a set of influencing factors on people's attitude to ensuring security in cyberspace were determined. The analysis was carried out based on the determination of psychological characteristics and deviations caused by quarantine restrictions. Based on the survey of respondents, a model of the relationship between psychological factors and the results of cyber security was developed. Among such factors, the following were identified: stress resistance, skills in the professional sphere, soft skills, awareness of cyber security and mechanisms and tools for protection against cyber-attacks [Alsmadi, D., Maqousi, A. and Abuhussein, T. (2022)].

Separately, it is advisable to determine the role of social networks in the development of cyber-attacks. The spread of social networks is massive. With the development of the Internet environment, a numerous of communication processes moved to the virtual world, which ensured the formation of communication centers - social

networks, where people can exchange information, communicate, share experiences, learn, and have fun in a remote format. The process of involvement in social networks is especially relevant among young people and teenagers. Due to the lack of effective cyber security systems and the lack of effective legal protection of personal data, social network accounts are constantly attacked and can be used for fraud, crimes, extortion, etc. Since the spread of social networks is the greatest among teenagers and young people, it is appropriate to evaluate the factors that influence the spread of crime in cyberspace among young people, in particular, these factors are: individual, parental, social, economic and political factors. In addition to directly influencing factors on the formation of criminal acts, it is advisable to consider similar aspects regarding the involvement of youth and teenagers in criminal schemes. For example, closed communities aimed at driving teenagers to suicide are widespread in the network. Under the conditions of the teenager's period and difficult life circumstances of teenagers in a certain period, a person may be prone to such actions and be included in certain processes in the virtual world, which may lead to negative consequences. The development of the coronavirus infection and the introduction of quarantine restrictions only scaled such processes. Information and communication technologies have changed, and people have increased civic participation and interaction with these technologies. By conducting a survey among young people using a Likert scale, numerous authors determined causal patterns and modeled constructive equations to ensure the protection of young people in social networks through the use of psychological and technological measures [Li, Y., Li, J., Fan, Q. and Wang, Z. (2022)].

Therefore, the analysis of literary sources made it possible to identify trends in the increase in the volume of cybercrimes in the world, which is related both to technological development, the spread of access to the Internet and social networks, and the scaling of remote processes due to the quarantine restrictions of the pandemic. An important practical task is to find effective mechanisms for combating cybercrimes, both in the field of their prevention and in terms of minimizing their consequences.

3. Methodology

The article uses methods of literature review, which made it possible to highlight previously unresolved parts of the research, to determine their relevance and practical significance. The population's requests for finding mechanisms to combat cyberattacks in

the face of global challenges have been studied. An analysis of psychological-cognitive and technical-technological models of the formation of the interdependence of external and internal factors on the processes of prevention and minimization of the consequences of cybercrimes was carried out. By conducting a sociological survey among information technology managers, a collection of influencing factors on cyber security processes was developed and their dynamics were determined to analyze cause-and-effect relationships. The sample consisted of 200 respondents - representatives of the field of information technologies throughout Ukraine. The main requirements for respondents were work experience of 5 years or more, direct work in information resource protection systems, specialized basic higher education. The sociological survey was conducted by means of questionnaires and the development of control charts. The results of the sociological survey made it possible to determine the information and analytical set of factors influencing the results and consequences of cyberattacks, as well as the formation of approaches to their prevention. By modeling the trend line of the development of cyber processes, the prospects for the scaling of cybercrime were determined. The determination of the trend line made it possible to substantiate the hypotheses of the dependence of factors on the scaling of cyber security processes.

4. Results and Discussion

As a result of the conducted research, a questionnaire of sociological survey of respondents was developed in the form of a control chart. The control card is designed for conducting a sociological survey remotely. Accumulation of the results of the literature review determined what was proposed in the control chart for assessing the set of factors influencing the processes of ensuring cyber security, among these factors the following were identified:

- educational and qualification factors – the level of information provision, educational and qualification characteristics of the population regarding the avoidance of cyber fraud by means of personal data protection, information protection, prevention of data leaks,
- psychological factors – the level of psychological preparation and stress resistance in conditions of global challenges,

- technical and technological factors – availability of technological conditions: tools, resources, mechanisms for combating cybercrimes, as well as ensuring cyber security processes with technical means with a high degree of innovation,
- regulatory and legal factors – the presence of effective mechanisms of legal regulation of cyberspace, personal data protection, information protection, information security,
- factors of national security – determination of information protection mechanisms and cyber protection at the level of national security as an element of protection of national interests of both the state as a whole and each of its individual citizens,
- social factors – the influence of the level of social security and the standard of living and the level of the population on the level of cyber security,
- economic factors – the level of influence of the population's income on the formation of conditions for ensuring security in cyberspace.

The structure of the control maps also included the question of the impact of cyber-attacks on the life processes of the population the following factors of influence were determined:

- financial and economic – impact on financial systems, entrepreneurial activity, business conduct, financial obligations, Internet banking, etc.,
- social – impacts on the availability of social services,
- national security – impacts on the processes of protecting the population and territory,
- technical and technological – impacts on technical and technological support in the process of life activities, provision of communal services, transport, electricity, communication, etc.,
- psychological factors – the formation of stressful situations by increasing the volume of cyber-attacks and the lack of realization of the basic human need for protection and security.

The respondents were provided with a control card with recorded factors of influence on the scaling processes of cyberattacks and factors of the consequences of the implementation of cyberattacks. Respondents rated the impact of each factor on a 10-point scale. The ranking scale is presented in table 1.

Therefore, in the research process, only those factors that receive the status of "The most important" and "Important" because of filling out control cards respondents will be analyzed. The results of the respondents' assessment are presented in table. 2

The results of the survey were averaged by conducting an analysis of estimates using the calculation of correlation relationships, which allowed confirmation of the results and reject underestimated and overestimated estimates.

Table 1: Ranking scale for assessing the degree of influence of cause-and-effect relationships on the scaling processes of cybercrime

rating scale	limitation	description
The most important	9-10	factors have a high impact on the scaling of cyber-attacks and cause significant losses
Important	6-8	factors have a significant impact on the scaling of cyber-attacks and cause certain damages
Unimportant	3-5	factors do not have a significant impact on the scaling of cyber-attacks and do not cause significant damage
Importless	0-2	factors may not be considered in the analysis process, as they have no impact on life processes and business processes

The results of the analysis of the control charts determined the directions for the development of recommendations for the prevention of cyber-attacks, in particular:

1. Work in the direction of preventing cyberattacks should be directed, first, to the following factors:

- educational and qualification factors,
- - psychological factors,
- - national security factors,
- - technical and technological factors.

2. Work in the direction of minimizing the effects of cyber-attacks should be directed, first, to the following factors:

- national security,
- financial and economic factors,
- technical and technological factors.

Table 2: Results of a sociological survey assessing the degree of influence of cause-and-effect relationships on the scaling processes of cybercrime

Rating based on the average score	Reasons for scaling up	Average score (maximum 10)	Consequences of scaling	Average score (maximum 10)
1	educational and qualification factors	9	national security	10
2	psychological factors	8	financial and economic factors	9
3	national security factors	8	technical and technological factors	7
4	technical and technological factors	7	social factors	4
5	regulatory and legal factors	4	psychological factors	4
6	social factors	2		
7	economic factors	2		

To determine the relevance of the confirmed hypotheses, the dynamics of the number of cyberattacks were analyzed and a projection of the trend line was developed - figure. 1

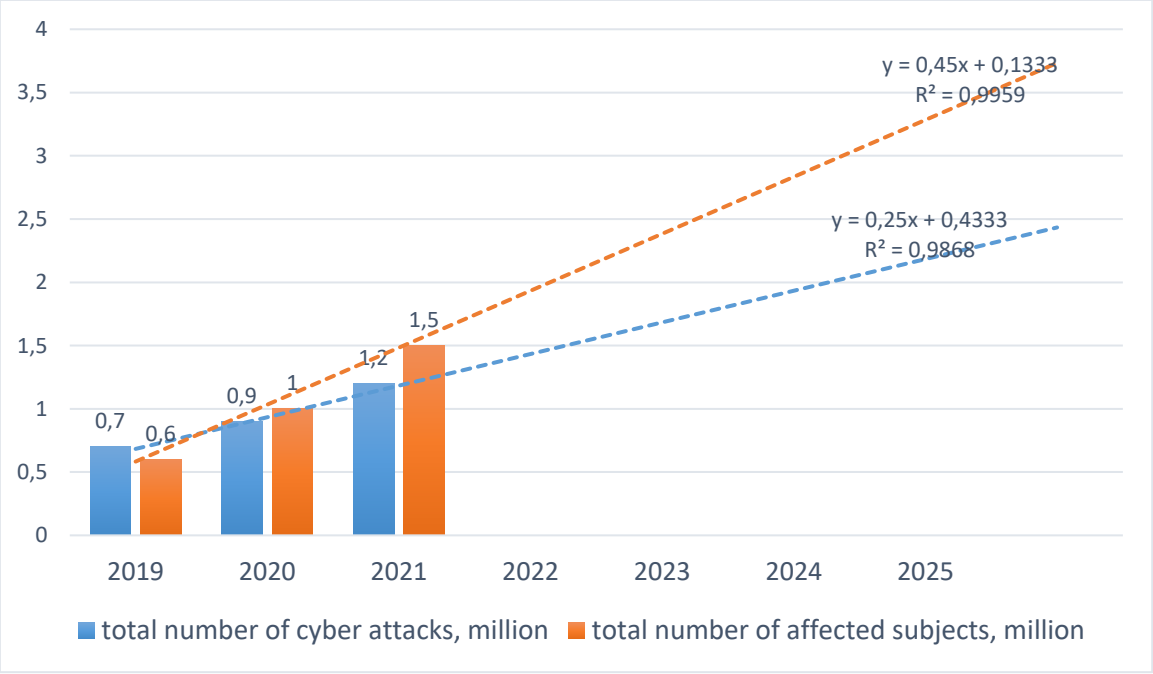

Figure 1. The trend line of cyber-attack scaling processes, 2019-2025 years

In figure 1 presents the trend line and its calculation formulas for two indicators: the total number of cyber-attacks, million and the total number of affected subjects, million. Analysis and projection of the results revealed that the number of cyber-attacks will continue to increase. By 2025, the number of cyber-attacks may increase to almost 2 million per year. There is also a trend towards a significant increase in subjects subject to attacks. If in the period of 2019-2020 several attacks had to be carried out to hack one subject. In 2021, the number of subjects increased significantly compared to the number of attacks, which indicates an increase in their mass and effectiveness.

5. Discussion

As a result of the conducted research, the influencing factors on the scaling of cyber-attacks were selected. The construction of the trend line made it possible to predict the further increase in the number of attacks and the increase in the number of affected subjects, which confirms the great practical value of the analysis of impact factors. Also, by conducting a sociological survey based on the use of the control chart method, the consequential factors of the effects of cyberattacks were determined. As a result of the assessment and analysis, proposals were developed for the implementation of the cyber security system:

- development of programs for training, professional development, and information provision of the population with information about the possibilities of protecting personal data and the basics of cyber security, which will affect the factors of the educational and qualification level and psychological factors that are most relevant when scaling cyber-attacks. The development and implementation of educational and educational programs aim to reach many the population in order to prevent the facts of cybercrime.
- development and introduction of cyber security systems into national military doctrines, formation of military associations aimed at protecting information and management systems,
- development and implementation of technologies aimed at the formation of information protection systems through the development of innovative technical, management and other solutions.

6. Conclusion

As a result of the conducted research, trends in the increase in the number of cybercrimes have been determined. The analysis of literary sources made it possible to determine that the largest number of cybercrimes are aimed at the financial systems of both national and individual companies or financial institutions. In 2020-2021, cyber-attacks on national security systems were of great relevance. Based on the conducted analysis, a set of factors of influence and consequences of cyberattacks was formed, based on the results of a sociological survey, a ranking of factors was carried out using control charts. Determination of the most relevant factors, including the following. Work in the direction of preventing cyberattacks should be directed, first, to the following factors: educational and qualification factors, psychological factors, national security factors, technical and technological factors. Work in the direction of minimizing the effects of cyber-attacks should be directed, first, to the following factors: national security, financial and economic factors, technical and technological factors. These influencing factors are relevant, have practical value and can be applied to the analysis of cyber security processes, which was confirmed by conducting a correlation analysis of the results of a sociological survey. As a result of the research, recommendations were developed regarding the main areas of implementation of measures in the cyber security system: educational and qualification, national security, finance, and technical and technological factors, which can be used in practice to build effective cyber security management systems.

REFERENCES

AL-Nuaimi, M.N. (2022), "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review", Global Knowledge, Memory and Communication, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/GKMC-12-2021-0209

Alsmadi, D., Maqousi, A. and Abuhussein, T. (2022), "Engaging in cybersecurity proactive behavior: awareness in COVID-19 age", Kybernetes, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/K-08-2022-1104

Asbaş, C. and Tuzlukaya. (2022), "Cyberattack and Cyberwarfare Strategies for Businesses", Özsungur, F. (Ed.) Conflict Management in Digital Business, Emerald Publishing Limited, Bingley, pp. 303-328. https://doi.org/10.1108/978-1-80262-773-220221027

Chhabra Roy, N. and Prabhakaran, S. (2023), "Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach", Journal of Financial Crime, Vol. 30 No. 1, pp. 48-85. https://doi.org/10.1108/JFC-12-2021-0274

Dupuis, D., Smith, D. and Gleason, K. (2023), "Old frauds with a new sauce: digital assets and space transition", Journal of Financial Crime, Vol. 30 No. 1, pp. 205-220. https://doi.org/10.1108/JFC-11-2021-0242

Kaswan, K.S., Dhatterwal, J.S., Kumar, S. and Lal, S. (2022), "Cybersecurity Law-based Insurance Market", Sood, K., Dhanaraj, R.K., Balusamy, B., Grima, S. and Uma Maheshwari, R. (Ed.) Big Data: A Game Changer for Insurance Industry (Emerald Studies in Finance, Insurance, and Risk Management), Emerald Publishing Limited, Bingley, pp. 303-321. https://doi.org/10.1108/978-1-80262-605-620221018

Li, Y., Li, J., Fan, Q. and Wang, Z. (2022), "Cybercrime's tendencies of the teenagers in the COVID-19 era: assessing the influence of mobile games, social networks and religious attitudes", Kybernetes, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/K-07-2021-0582

Ma, K.W.F. and McKinnon, T. (2022), "COVID-19 and cyber fraud: emerging threats during the pandemic", Journal of Financial Crime, Vol. 29 No. 2, pp. 433-446. https://doi.org/10.1108/JFC-01-2021-0016

Panteli, N., Nurse, J.R.C., Collins, E. and Williams, N. (2022), "Trust disruption and preservation in the Covid-19 work from home context", Journal of Workplace Learning, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JWL-02-2022-0017

Tamer, G., Tetik, G. and Oktay, S. (2022), "Digital Conflict in Business Infrastructure", Özsungur, F. (Ed.) Conflict Management in Digital Business, Emerald Publishing Limited, Bingley, pp. 147-165. https://doi.org/10.1108/978-1-80262-773-220221011

Thomas, G. and Sule, M.-J. (2022), "A service lens on cybersecurity continuity and management for organizations' subsistence and growth", Organizational Cybersecurity Journal: Practice, Process and People, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/OCJ-09-2021-0025

TN, N. and Shailendra Kulkarni, M. (2022), "Zero click attacks – a new cyber threat for the e-banking sector", Journal of Financial Crime, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JFC-06-2022-0140

Tuna, A.A. and Türkmendağ, Z. (2022), "Cyber Business Management", Özsungur, F. (Ed.) Conflict Management in Digital Business, Emerald Publishing Limited, Bingley, pp. 281-301. https://doi.org/10.1108/978-1-80262-773-220221026

Wronka, C. (2022), "“Cyber-laundering”: the change of money laundering in the digital age", Journal of Money Laundering Control, Vol. 25 No. 2, pp. 330-344. https://doi.org/10.1108/JMLC-04-2021-0035

Wronka, C. (2022), "Impact of COVID-19 on financial institutions: navigating the global emerging patterns of financial crime", Journal of Financial Crime, Vol. 29 No. 2, pp. 476-490. https://doi.org/10.1108/JFC-03-2021-0073