Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5, 1164-1174
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i5.1819

Information protection and cyber security in the public and financial sectors

Oleksandr Chumak[1*], Serhii Holovkin[2], Oleksandr Piroh[3], Tetiana Pushkar[4], Oleg Diegtiar[5]
[1]Department of National Security, Institute of Security, Interregional Academy of Personnel Management, Kyiv, Ukraine; simstore1102@gmail.com (O. C.)
[2]Department of Criminal Procedure and Forensics, Faculty of Training Specialists for Units of Pre-Trial Investigation, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine; gsvvsg79@gmail.com (S. H.)
[3]Department of Computer Engineering and Cyber Security, Faculty of Information and Computer Technologies, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine; pirogov@ztu.edu.ua (O. P.)
[4]Department of Economics and Marketing, School of Economics and Management, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine; tat_pa@i.ua (T. P.)
[5]Department of Public Management and Administration, Institute of Graduate Studies and Pre-university Education, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine; odegtyar@i.ua (O. D.)

Abstract: The public sector faces increasing challenges in the field of cyber security and information protection, stimulated by the rapid development of digital technologies. A significant increase in the need for reliable protection of state data and information systems requires state institutions to implement complex information protection measures. The purpose of the study is to analyze modern approaches and technologies in the field of cyber security and the use of encryption, cryptography, and the use of cloud technologies that can be used in the public sector for effective information protection. The research methodology involves consideration of strategies that allow to increase the level of security and ensure the protection of critical infrastructure. The results of the study emphasize the need to adapt to the rapidly changing digital environment and involve modern technological solutions to create a reliable information network system in the public sector. The findings of the study draw attention to the importance of global cooperation and increased investment in the field of countering digital attacks, demonstrating examples of effective international cooperation and support in this direction. The need for the integration of international standards and practices in order to create a global digital space has been revealed. A promising area of research is the analysis of the impact of the latest technologies on data storage strategies, which contributes to the identification of ways for further innovations in the industry and the creation of flexible information network systems capable of effectively responding to changing conditions and challenges of modern cyberspace.

Keywords: *Blockchain, Cloud technologies, Cryptography, Cyber security, Encryption, Information protection, Information systems, Public sector.*

1. Introduction

The increasing need for information protection in the public sector is the result of a number of factors that are rapidly changing the modern information landscape. Globalization and intensification of international interaction increase the volume of information exchange between states, which requires state bodies to ensure a high level of confidentiality and integrity of data. The rapid development of digital technologies and their integration into all spheres of public administration increase the potential vectors of attacks for cybercriminals, which puts the issue of updating data protection measures on the agenda. A significant source of the growth in the number and complexity of cyber attacks is their encryption, which is becoming increasingly sophisticated, targeting government information systems for espionage, sabotage or influencing political processes. The spread of information technologies

* Correspondence: simstore1102@gmail.com

among the population and their use for access to public services increases the amount of personal data processed by state bodies, introducing additional requirements for the protection of this information from unauthorized access [1].

Global digitization prompts increased attention to the development and implementation of comprehensive information protection systems, including legislative regulation, organizational measures, technological solutions and improving cyber hygiene among government employees.

The advancement of encryption, cryptography, and cloud technologies opens up new opportunities for ensuring the protection of information in the public sector. Encryption and cryptographic technologies make it possible to ensure the confidentiality of personal data of citizens and state information, protecting them from unauthorized access during transmission over open networks or storage in databases [2].

Cloud technologies offer the flexibility and scalability of resources to meet the computing power and data storage needs of government agencies, while requiring service providers to implement a high level of security and compliance with information protection requirements. Blockchain technology, with its ability to create immutable and transparent transaction registers, offers revolutionary approaches to ensuring integrity and accountability in government data processing, particularly in the areas of voting, property registration and personal identification [3, 4]. The introduction of technologies requires significant investments in IT infrastructure and software development, constant updating of knowledge and skills of specialists in the field of cyber security, adaptation of the legal framework and formation of citizens' trust in new methods of information protection.

The creation of information security of the global space and the strengthening of investments in this area are the answer to the growing cyber threats that do not know national borders and require concerted efforts at the international level. Cooperation programs between countries, international conferences and agreements serve as a basis for the exchange of information and best practices in the field of combating cyber attacks. Investments in the development of national digital networks emphasize the recognition of the importance of this issue at the state level. In addition to financing the development and implementation of technological solutions, significant resources are directed to training personnel, raising public awareness, and creating legal mechanisms for responding to cyber incidents. The EU Cyber Security Center (ENISA) and the partnership between the G7 countries demonstrate that joint efforts and mutual assistance can significantly increase the level of protection of the information space. Thus, the progression of global cyber security is a response to modern challenges and reflects the understanding that security in the digital world is a shared responsibility of the entire international community, requiring constant efforts, innovation and mutual support.

The issue of information protection and cyber security in the public sector is a top priority for government organizations in the globalized digital world. A study [4] analyzes the impact of growing cyber threats on national security, emphasizing the need to develop comprehensive information strategies that cover technological and organizational areas. The work [5] considers the role of the United States as a leader in the formation of international cyber security standards, pointing to the importance of interstate cooperation in the fight against transnational cyber threats. Considerable attention is paid in the article [6] to investments in software, where budget allocations and the effectiveness of spending money on the protection of information systems are analyzed.

A study [7] highlights the use of cloud technologies in the public sector to ensure the effectiveness of digital solutions. Particularly valuable is the analysis [8] of machine learning in the detection and countermeasures of cyber attacks, which demonstrates the potential of automation in ensuring the cyber protection of government institutions. The work [9] examines in detail the issues of legal regulation of cyberspace, the importance of adapting legislation to the rapidly changing conditions of the digital era, and ensuring the legal security of information in the network. The author [10] believes that a comprehensive approach to the study of cyber security in the public sector should cover technical, strategic, legal and international aspects. The scientist [11] outlined critically important theses for ensuring the stability of state information systems in modern cyberspace. The importance of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

international cooperation is given in the article [12], since the issue of information protection in the public sector is a strategic direction for ensuring integrity.

The work Demertzi et al. analyzes successful examples of joint cyber security initiatives between countries that contribute to improving the global security of the information space [13]. Research [14] on the role of technological innovations in the protection of information of state institutions involves the wide application of modern methods of cryptographic data protection and their orientation towards strengthening national security. The article Knott et al. examines the issue of information security in the context of the digital transformation of government services [15]. The author Ayodeji et al. points out that the integration of the latest digital solutions requires technical and organizational changes through increasing the awareness of personnel on cyber security issues [16]. The study Gjesvik & Szulecki emphasizes the importance of international cooperation and information exchange between state institutions of different countries to effectively counter cross-border cyber threats [17].

Scientific work Vahidi et al. emphasizes that the management of cyber risks in government structures requires the latest infrastructure, which is able to combine advanced technologies and standardization of cyber security processes [18]. The author Limba et al. focuses on challenges, related to the implementation of cloud technologies in the public sector, emphasizing the need to ensure a balance between the convenience of using cloud services and risks to information security [19]. According to Ngoma et al. global cyber threats require governments to develop strategies for global information networks that can effectively respond to and process a large number of requests [20]. Statements Wilson & Fitz refer to the growing role of international norms and standards in harmonizing efforts on digital protection, as it allows to increase the overall level of security of information systems at the international level [21].

Thus, modern scientists emphasize a comprehensive approach to the protection of information in the public sector, including technological innovations, international cooperation and the evolution of the legal field [22]. Further research should focus on examining the impact of emerging technologies, strategies for global collective cyber security. The development of effective mechanisms for the international regulation of cyberspace to ensure the stability and security of state information resources should become a priority task for developed countries [23].

The purpose of the study is to analyze modern challenges and strategies in the field of information protection and cyber security in the public sector, the effectiveness of identifying effective technological solutions for the protection of state data in the face of growing global cyber threats. The problem of the research stems from the need to adapt existing cyber security systems to the rapid development of digital technologies and changes in the nature of cyber attacks, which presents the public sector with the task of protecting information resources. The main task of the research is to assess the potential of the latest technologies and their use to increase the level of cyber security, the possibilities of developing complex strategies. A promising direction of research is the study of the possibilities of international cooperation in the formation of a unified cyber security system, which allows to effectively resist transnational cyber threats. The practical value of the study lies in the expansion of recommendations for government structures regarding the implementation of innovative technologies and methods of information protection, which will contribute to strengthening national security, protecting personal data of citizens and ensuring the stable functioning of state institutions in the digital era.

2. Research Methodolog

To study the cybersecurity market, a comprehensive analysis of current technologies, investment trends and strategic approaches was carried out, paying special attention to the role of the United States of America as a world leader in the field of digital technologies. The research procedure includes the collection and interpretation of data from statistical sources, scientific publications, government reports, analytical reports of leading research institutes [14].

The methodology made it possible to identify key areas of industry development, including the introduction of advanced technologies, the use of cryptographic tools and their impact on increasing the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

effectiveness of information protection strategies. In the process of analyzing cyber security strategies and investments, attention was focused on big data processing methods to identify funding trends, assess the effectiveness of existing information protection mechanisms, and determine promising directions for further investments. In the conditions of global competition and strengthening of international security, the cyber defense financing market and potential directions of its further development are investigated.

Applied statistical analysis methods to quantify trends and patterns in cybersecurity, including analysis of direct investments in cybersecurity of the global market. The US budget for ensuring the protection of the information space was analyzed and the relationship between the level of technological development and the effectiveness of cyber security measures was determined. The analysis of the literature made it possible to collect and systematize theoretical propositions, research conclusions and expert assessments regarding the best practices in the field of information protection.

The conclusions identify key challenges and promising directions for the enhancement of cyber security technologies. The combination of quantitative and qualitative analysis contributed to a deep understanding of the current state of cyber security and the identification of strategic directions for improving global digital security. An important stage of the methodology was the assessment of modern technologies in the development of the appropriate cyber security infrastructure through the implementation of data encryption systems and tools to ensure the integrity and availability of information. Thus, the research methodology includes the study of technical specifications, advantages and potential vulnerabilities, assessment of cyber security markets in order to create suggestions for enhancing the efficiency of strategies within the government sector. The definition of strategic directions for infrastructure modernization, considering the swift advancement of technological innovations and increasing cyber risks, is highlighted in the analysis presented in the study [24].

3. Research Results

The evolution of digital technologies has profoundly altered the contemporary world and the framework of the state and corporate sectors, where digitalization has become critical for the effectiveness of their functioning [25, 26]. The formation of digital infrastructure has turned out to be a key priority for large companies and government institutions that seek to optimize their internal processes and ensure access to their services via the Internet [27]. The cyber security approach encompasses the creation and deployment of sophisticated information systems, cloud solutions, integration of big data for real-time information analysis and processing. Big companies Google, Amazon and Microsoft play a leading role in the process of protecting information, investing billions of dollars in the improvement of infrastructure platforms that allow corporate and government customers to effectively scale their IT resources. State institutions are actively working on the digitization of their services, which includes electronic document management, e-government, digital healthcare and electronic educational platforms aimed at increasing the accessibility and transparency of public administration [28].

The issue of cyber security is becoming increasingly relevant in the light of society's increasing dependence on digital technologies, as the new digital space opens up wide opportunities for obtaining information and minimizing manipulation and unauthorized access. The digital era is forcing states to rethink their approaches to protecting critical information and infrastructure by developing and implementing comprehensive cyber security strategies [29]. This involves establishing national cyber security hubs and formulating a regulatory and legal framework governing cyber security issues, and the implementation of advanced data encryption technologies, firewalls, and intrusion detection and prevention systems. Given the ever-increasing threat of cyber-attacks from attackers and aggressor states, it is imperative to protect data, ensure the integrity and availability of information resources, as they play a crucial role in ensuring national security and economic prosperity.

The formation of the cyber security market is a response to the growing need to protect the digital space, integrating the corporate sector to serve government institutions around the world. The modern

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

market is characterized by rapid development and innovation, where leading corporations Cisco, Palo Alto Networks, Symantec and Kaspersky Lab develop complex solutions that include advanced cloud technologies and specialized services to counter cyber threats. They offer governments tools for threat analysis, data encryption, network infrastructure protection, and real-time security monitoring [25, 26].

The growth of the cybersecurity market fosters collaboration between government and private industries, as joint initiatives and partnerships allow for the exchange of knowledge, technology and leading practices in cybersecurity. Considering the ever-changing landscape of cyber threats, partnership is essential for adjusting to emerging challenges, safeguarding national security, and defending vital information resources. An evaluation of the cybersecurity industry is depicted in Figure 1, where private and public companies participate.

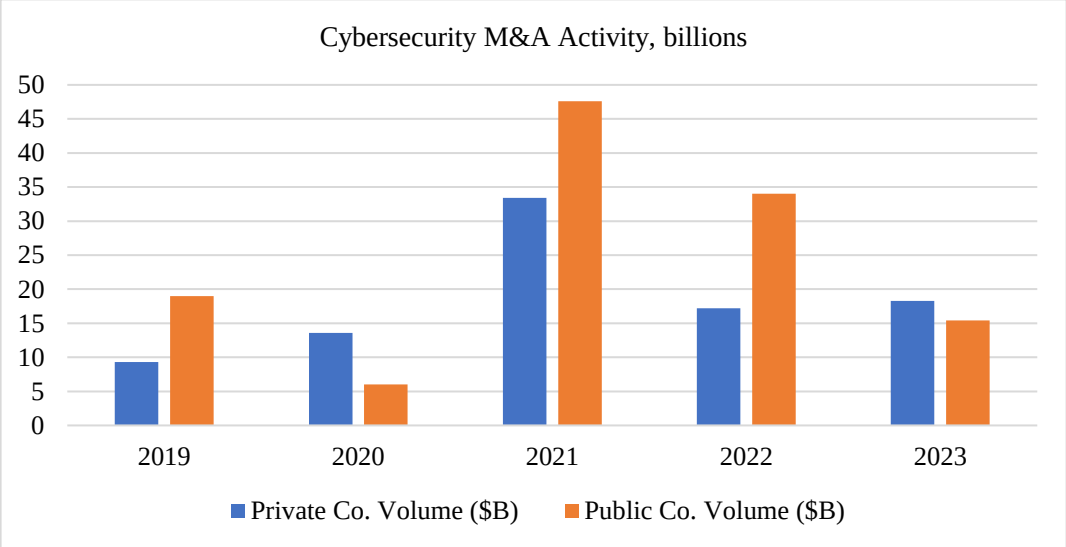

Figure 1.
Cybersecurity M&A Activity 2019–2023, billions.

Data encryption stands as a key technology within the realm of public sector cybersecurity, where protecting the confidentiality and integrity of information is critical. Encryption helps ensure that information remains inaccessible to unauthorized access by converting the original data into a coded format that can only be decoded using a special key. Within the diverse range of encryption techniques, both symmetric and asymmetric encryption methods are employed. Symmetric encryption uses one key for both encrypting and decrypting data, whereas asymmetric encryption relies on a key pair (public and private) to bolster security. In the public sector, these methods are used to protect important information, including personal data of citizens, military secrets and state secrets. Encryption standards such as Advanced Encryption Standard (AES) and RSA are widely used to protect data transmitted between various government agencies or to protect information stored on government servers. They are widely implemented in the countries of the European Union and function to ensure the integrity of the digital space.

Blockchain technology has become widespread due to its ability to provide a high level of security and transparency in the processing of information data. It is based on a distributed registry, where information is stored in the form of blocks connected to each other in such a way that it is impossible to change or delete information in one of the blocks without changing the entire sequence. For public institutions, the available technology opens up new opportunities for increasing efficiency, transparency and security in the provision of public services. Estonia is actively integrating blockchain technologies into government systems, using them to protect electronic voting, citizens' health and other public

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

services. Its approach ensures a high level of data security and contributes to increasing citizens' trust in e-government [3, 4].

The formation of cooperation between states in the field of cyber defense is becoming relevant in the conditions of globalization and the growth of cyber threats. Cooperation in the digital sphere allows for the exchange of information about threats, the establishment of unified standards and strategies for safeguarding critical infrastructure and coordinating responses to cyber incidents. The European Union is actively working to create a single digital economy, which includes initiatives to improve the cybersecurity of its member states through the European Cybersecurity Strategy and the Network and Information Security (NIS) Directive. Today, NATO is deploying joint efforts to defend against cyber threats, one of which is the creation of the NATO Center of Excellence for Cyber Defense.

International cooperation contributes to increasing the level of protection of each country involved and forms a united front against cybercrime and cyberterrorism, which is an important step towards creating a secure global cyberspace. Prospective information protection technologies in the public sector are depicted in Table 1.

Table 1.
Basic information protection technologies in the public sector.

Technology	Characteristic	Application in the public sector
Data encryption	Data encryption technology is used to convert information into an unreadable format that can be restored to its original state only with the help of a special key. It	The US uses encryption to protect state secrets and personal information of citizens. The European Union applies the GDPR, which requires data protection with encryption.
Firewalls	Firewalls serve as a protective boundary between secure internal networks and potentially unsafe external networks, like the Internet, by scrutinizing both inbound and outbound network traffic according to established security regulations.	Israel makes extensive use of firewalls to protect its critical information infrastructures. Singapore employs advanced firewall technologies to protect its national information infrastructure.
Intrusion detection tools	Intrusion detection tools (IDS) constantly track network activity to detect suspicious activity or known attack signatures.	China is implementing IDS to monitor government networks and protect against spyware.

The information technology market is characterized by rapid saturation with new products and software that is constantly being improved, offering solutions for a wide range of tasks from business analytics to cyber security. These dynamics hold special significance for the public sector, where the demand for effective and secure technological solutions is essential to maintaining national security, public administration efficiency and the provision of quality services to citizens [30].

Modern technological solutions of cloud services play a leading role in the transformation of public services, from the automation of administrative procedures to the protection of important data and ensuring the transparency of government operations. The constant updating of the software allows to increase the efficiency of government structures and to adapt to new challenges and threats in cyberspace, which is especially relevant in the conditions of the growth of cybercrime and cyberespionage.

The geopolitical conflicts of recent years, especially the war in Ukraine in 2022 and the military conflicts in Israel, have highlighted the critical need to strengthen information protection and cybersecurity at the national level. Modern warfare demonstrates that cyberspace is becoming an arena for geopolitical clashes, where cyberattacks are used as tools of warfare aimed at destabilizing state institutions, destroying critical infrastructure, and influencing public opinion. In response to existing threats, states have intensified their efforts to develop and implement advanced cyber defense strategies,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

expand cooperation with international partners and the private sector to share information on cyber threats and coordinate actions against cyber terrorism.

The increase in spending on cyber security in the United States of America from 2022 indicates the recognition of cyber security as a priority area in ensuring the national and economic security of the country. Given the increase in cyber threats and their complexity, governments around the world are increasing investments in protecting their information systems, developing national cyber security strategies, and training skilled professionals in this field. In the USA, a significant increase in budget allocations for cyber security was aimed at modernizing outdated information systems, enhancing the security of government data and broadening global collaboration in cybersecurity. The investment demonstrates the recognition of the seriousness of cyber threats and the readiness to respond to them with all the necessary determination and resources, using innovation and international cooperation as key elements of its strategy. The main dynamics of US budget expenditures on cyber security are systematized in Figure 2.

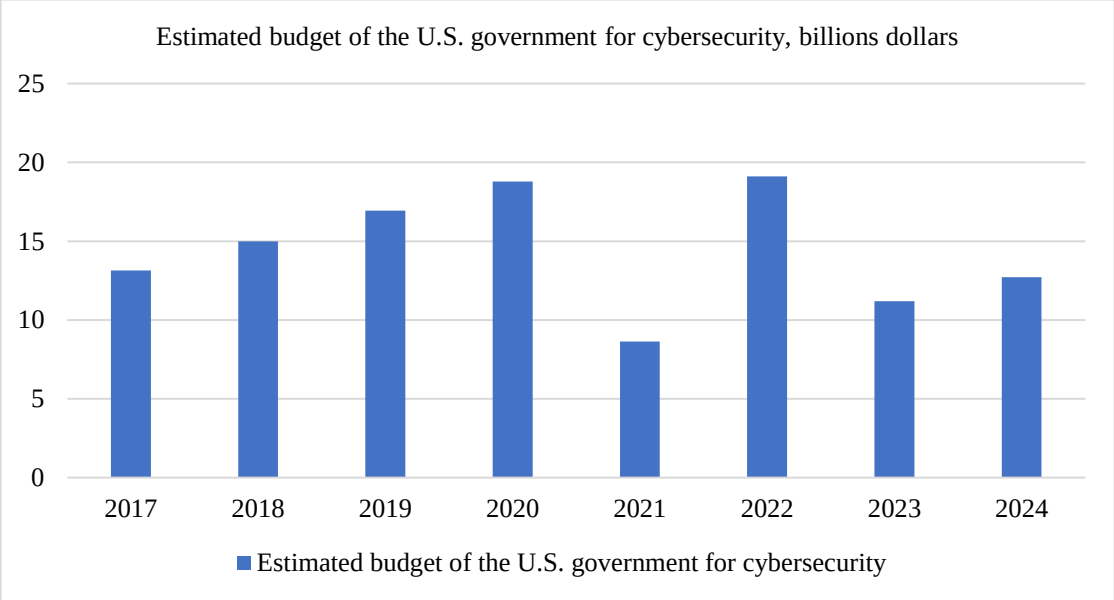

Figure 2.
Estimated budget of the US government for cybersecurity in FY 2017 to 2024 (in billion US dollars)

The increase in cooperation between the US and the European Union in the field of cyber security has become a response to the increase in cyber threats that do not know national borders and can affect the integrity and security of information networks of the entire region. In response, EU countries have stepped up cooperation, in particular through the creation of the European Union Agency for Cyber Security (ENISA), which facilitates the sharing of expertise and leading practices, the establishment of cybersecurity norms, and the synchronized response to cyber events. The role of the United States is significant, as the American government and private sector provide technological expertise, support international initiatives, and invest in the emergence of international cybersecurity. Collaboration between the EU and the US in information security spans numerous initiatives, including combined drills and educational programs, as well as crafting policy frameworks and quick-reaction procedures to cyber dangers. The cooperation demonstrates an understanding that effective defense against cyber threats requires a concerted effort at the national and international levels.

Establishing the necessary technological framework for safeguarding government information stands as a critical objective in cybersecurity, encompassing the incorporation of contemporary cloud computing technologies. They offer government agencies the flexibility, scalability and efficiency of data

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

management while providing a high level of protection through advanced encryption methods, resource isolation and automated security monitoring. The use of cloud services allows government agencies to optimize IT infrastructure spending by focusing on strategic cyber defense tasks instead of maintaining a large amount of physical equipment. Cloud platforms provide advanced capabilities for data backup and recovery, which is important to ensure the relevant level of information systems in the event of cyber attacks or other disruptions.

The transition to modern digital solutions requires government agencies to carefully select reliable service providers and develop a comprehensive cloud security management strategy to take into account the specific requirements for protecting government data and ensuring its confidentiality and integrity.

4. Discussion

Our research found that significant investment in cyber security and technology development is key to protecting information in the public sector. The obtained results are consistent with findings [31], which emphasize the importance of technological innovation for national security. The conducted analysis confirms theses [32] about the importance of innovations in the field of cyber security, while pointing to the need for careful study of potential risks associated with the latest technologies. In contrast to [33], highlighting the difficulties of incorporating cloud technologies, it has been discovered that creating international norms and standards can mitigate risks and enhance trust in adopting cloud solutions within the public sector. Unlike our study [18], pays more attention to the potential risks associated with the adoption of cloud technologies, which indicates the need for a deeper analysis of the balance between innovation and security.

The article confirms the conclusions [34] about the importance of international cooperation in the field of cyber security, finding that the joint efforts of countries can significantly increase the effectiveness of the protection of the information space. The results expand the understanding of the role of the United States in a study that demonstrates a number of US initiatives for global cybersecurity approaches. The research idea [35] is aimed at the rapid changes in cyberspace through the implementation of the latest technologies and the improvement of work with the digital corporate sector. According to [36], it was found that international norms can partially solve the problem of harmonization of cyber security efforts, as it will practically increase the level of global standards. Compared to the work of [37], the paper focuses on threats to national security and increased domestic funding, as there is a need to increase cyber literacy among government officials. According to [38], the importance of internal cybersecurity skills development and education in the public sector remains the most promising area for research in the coming years. Thus, further research should be coordinated on the technological, financial and educational levels of ensuring the quality of information protection.

5. Conclusions

Based on the analysis of the cyber security market, technologies and investment strategies in the field of information protection, it can be concluded that cyber security is a key priority for public institutions and the private sector against the background of growing cyber threats. Significant investments in the maturation of modern technologies, including cloud solutions, data encryption, emphasize the need to adapt to the dynamics of the strengthening of cyberspace. Cooperation between countries within the framework of international organizations and initiatives contributes to the exchange of knowledge and the development of joint strategies to combat cybercrime. Special attention to the role of the United States as a world leader in the field of information protection indicates the importance of international coordination and leadership in the formation of global cyber security norms.

Despite significant progress in the field of cyber security, there are serious challenges and issues that need attention. The globalization of cyberspace and the increase in the number and complexity of cyberattacks threaten the information security of countries and their global stability. Cyber threats are increasingly widespread and diverse, including phishing, malware distribution, attacks on critical infrastructure, and disinformation campaigns. Protecting the state in the field of cyber security requires

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819

governments to make a concerted effort to create effective mechanisms to counter cyber threats, which are constantly evolving in complexity and scope.

Information protection involves the implementation of advanced technologies, the development of complex strategies that include legal regulation, education and awareness raising of citizens, and the formation of specialized cyber security units. Special attention should be paid to ensuring the security of energy networks, healthcare systems and financial institutions, which are becoming prime targets for cyber-terrorists and aggressor states. Existing challenges are complicated by rapid technological changes, which require constant updating of knowledge and skills of specialists in the field of cyber security.

Given these challenges, a number of measures are recommended to improve the effectiveness of cyber security. It is necessary to increase investments in the development and implementation of innovative technologies that will allow to resist the latest cyber threats. The escalation of international cooperation and information exchange between countries is important for effective response to transnational cyber threats. Emphasis should be placed on the training of qualified personnel in the field of cyber security, ensuring constant training and development of professional skills. Therefore, the development and implementation of comprehensive national and international cyber security strategies, which would take into account the specifics of cyber threats and be able to adapt to rapid changes in the field of information technologies, become the most effective tool for ensuring the protection of the public sector.

References

[1]. T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk, and S. Podolyaka, "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine," *Journal of Information Technology Management*, vol. 13, pp. 75-90, 2021. https://doi.org/10.22059/jitm.2021.80738

[2]. M. Eidiani, "A rapid state estimation method for calculating transmission capacity despite cyber security concerns," *IET Generation, Transmission and Distribution*, vol. 17, no. 20, pp. 4480-4488, 2023. https://doi.org/10.1049/gtd2.12747

[3]. O. Piroh, O. Holovnia, and M. Koloshchuk, "Development and testing of a web-oriented electronic document management system using blockchain technologies elements," *Bulletin of the Khmelnytskyi National University*, vol. 5, no. 2, pp. 98-102, 2023.

[4]. O. V. Piroh, "Use of blockchain technology to protect web-based electronic document management systems," in *Abstracts of the First all-Ukrainian scientific and practical conference «Theoretical and applied cybersecurity»*, pp. 123-126, Kyiv: National Technical University of Ukraine «Kyiv Polytechnic Institute named after Ihor Sikorsky", 2023.

[5]. K. Dixit, U. K. Singh, and B. K. Pandya, "Comparative study of information security risk assessment model," *International Journal of Computer Applications*, vol. 185, no. 7, pp. 18-22, 2023. https://doi.org/10.5120/ijca2023922722

[6]. E. Ceko, "Cyber security issues in Albanian higher education institutions curricula," *CRJ*, vol. 1, pp. 56-65, 2023. https://doi.org/10.59380/crj.v1i1.2728

[7]. A. Panda, A. Baird, S. Pinisetty, and P. Roop, "Incremental Security Enforcement for Cyber-Physical Systems," *IEEE Access*, vol. 11, pp. 18475-18498, 2023. https://doi.org/10.1109/ACCESS.2023.3246121

[8]. G. Li et al., "A critical review of cyber-physical security for building automation systems," *Annual Reviews in Control*, Elsevier Ltd, 2023. https://doi.org/10.1016/j.arcontrol.2023.02.004

[9]. M. Ibrahim and R. Elhafiz, "Security analysis of cyber-physical systems using reinforcement learning," *Sensors*, vol. 23, no. 3, 2023. https://doi.org/10.3390/s23031634

[10]. D. I. Sukmawan and D. P. Setyawan, "Hacker, Fear, and Harm: Data Breaches and National Security," *Jurnal Global & Strategis*, vol. 17, no. 1, pp. 153-182, 2023. https://doi.org/10.20473/jgs.17.1.2023.153-182

[11]. S. Kalogiannidis, M. Paschalidou, D. Kalfas, and F. Chatzitheodoridis, "Relationship between cyber security and civil protection in the Greek reality," *Applied Sciences (Switzerland)*, vol. 13, no. 4, 2023. https://doi.org/10.3390/app13042607

[12]. V. Ananin and O. Uvarkina, "Political visions of cyber education," *National Technical University of Ukraine Journal. Political Science. Sociology. Law*, vol. 1, no. 57, pp. 35-39, 2023. https://doi.org/10.20535/2308-5053.2023.1(57).280780

[13]. V. Demertzi, S. Demertzis, and K. Demertzis, "An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities," *Applied Sciences (Switzerland)*, MDPI, 2023. https://doi.org/10.3390/app13020790

[14]. M. Jomon Jose and P. S. Aithal, "An Analytical Study of Applications of Artificial Intelligence on Banking Practices," *International Journal of Management, Technology, and Social Sciences*, pp. 133-144, 2023. https://doi.org/10.47992/ijmts.2581.6012.0275

[15]. J. Knott, H. Yuan, M. Boakes, and S. Li, "Cyber security and online safety education for schools in the UK: looking through the lens of Twitter data," in *Proceedings of the ACM Symposium on Applied Computing*, pp. 1603-1606, Association for Computing Machinery, 2023. https://doi.org/10.1145/3555776.3577805

[16]. A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors," *Progress in Nuclear Energy*, Elsevier Ltd., 2023. https://doi.org/10.1016/j.pnucene.2023.104738

[17]. L. Gjesvik and K. Szulecki, "Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout," *European Security*, vol. 32, no. 1, pp. 104–124, 2023. https://doi.org/10.1080/09662839.2022.2082838

[18]. S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, pp. 1294-1335, 2023. https://doi.org/10.1109/COMST.2023.3251899

[19]. T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship and Sustainability Issues*, vol. 4, no. 4, pp. 559-573, 2017. https://doi.org/10.9770/jesi.2017.4.4(12)

[20]. M. L. Ngoma, M. Keevy, and P. Rama, "Cyber-security awareness of South African state-mandated public sector organizations," *Southern African Journal of Accountability and Auditing Research*, vol. 23, no. 1, pp. 53-64, 2021. https://doi.org/10.54483/sajaar.2021.23.1.4

[21]. R. Wilson and A. Fitz, "Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues," *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 440–448, 2023. https://doi.org/10.34190/iccws.18.1.1050

[22]. S. Y. Diaba, et al., "SCADA securing system using deep learning to prevent cyber infiltration," *Neural Networks*, vol. 165, pp. 321–332, 2023. https://doi.org/10.1016/j.neunet.2023.05.047

[23]. S. Dutchak, N. Opolska, R. Shchokin, O. Durman, and M. Shevtsiv, "International aspects of legal regulation of information relations in the global internet network," *Journal of Legal, Ethical and Regulatory Issues*, vol. 23, no. 3, pp. 1-7, 2020.

[24]. D. Koshkin, "Cyber risks: prospective control instruments (using the example of Cyber Insurance)," *Artificial Societies*, vol. 18, no. 1, 2023. https://doi.org/10.18254/s207751800024767-2

[25]. S. Bondarenko, O. Halachenko, L. Shmorgun, I. Volokhova, A. Khomutenko, and V. Krainov, "The effectiveness of network systems in providing project maturity of public management," *TEM Journal*, vol. 10, no. 1, pp. 272-282, 2021. https://doi.org/10.18421/TEM101-34

[26]. S. Bondarenko, O. Makeieva, O. Usachenko, V. Veklych, T. Arifkhodzhaieva, and S. Lernyk, "The legal mechanisms for information security in the context of digitalization," *Journal of Information Technology Management*, vol. 14, pp. 25-58, 2022. https://doi.org/10.22059/jitm.2022.88868

[27]. V. Klochan, I. Piliaiev, T. Sydorenko, V. Khomutenko, A. Solomko, and A. Tkachuk, "Digital platforms as a tool for the transformation of strategic consulting in public administration," *Journal of Information Technology Management*, vol. 13, pp. 42-61, 2021. https://doi.org/10.22059/jitm.2021.80736

[28]. N. Vyhovska, I. Voronenko, A. Konovalenko, V. Dovgaliuk, and I. Lytvynchuk, "Cyber Security of the System of Electronic Payment of the National Bank of Ukraine," *Economic Affairs (New Delhi)*, vol. 68, Special Issue, pp. 881-886, 2023. https://doi.org/10.46852/0424-2513.2s.2023.34

[29]. V. Greiman, "Nuclear cyber attacks: a study of sabotage and regulation of critical infrastructure," *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 103–110, 2023. https://doi.org/10.34190/iccws.18.1.1042

[30]. I. Semenets-Orlova, R. Shevchuk, B. Plish, I. Grydiushko, and K. Maistrenko, "Innovative approaches to development of human potential in modern public administration," *Economic Affairs (New Delhi)*, vol. 67, no. 4, pp. 915-926, 2022. http://doi.org/10.46852/0424-2513.4s.2022.25

[31]. A. Fitz and R. Wilson, "Just warfare: is a nuclear attack an appropriate response to a cyber attack?" *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 534-541, 2023. https://doi.org/10.34190/iccws.18.1.1059

[32]. T. Johansmeyer, "How reversibility differentiates cyber from kinetic warfare: a case study in the energy sector," *International Journal of Security, Privacy and Trust Management*, vol. 12, no. 1, pp. 1–14, 2023. https://doi.org/10.5121/ijsptm.2023.12101

[33]. Y. Li and R. Mamon, "The Price Tag of Cyber Risk: A Signal-Processing Approach," *IEEE Access*, vol. 11, pp. 44294-44318, 2023. https://doi.org/10.1109/ACCESS.2023.3272572

[34]. G. Czeczot, I. Rojek, and D. Mikołajewski, "Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors," *Electronics (Switzerland)*, MDPI, 2023. https://doi.org/10.3390/electronics12112503

[35]. E. U. Haque, W. Abbasi, S. Murugesan, M. S. Anwar, F. Khan, and Y. Lee, "Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of Cyber Threat Landscape and Readiness," *IEEE Access*, 2023. https://doi.org/10.1109/ACCESS.2023.3268529

[36]. E. O. Paul et al., "Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors," *International Journal on Soft Computing*, vol. 14, no. 3, pp. 1-16, 2023. https://doi.org/10.5121/ijsc.2023.14301

[37]. S. Zdilar, "Security challenges," *National Security and the Future*, vol. 24, no. 1, pp. 47–52, 2023. https://doi.org/10.37458/nstf.24.1.5

[38]. A. Bobbio, L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "A cyber warfare perspective on risks related to health IoT devices and contact tracing," *Neural Computing and Applications*, vol. 35, no. 19, pp. 13823-13837, 2023. https://doi.org/10.1007/s00521-021-06720-1

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5: 1164-1174, 2024
DOI: 10.55214/25768484.v8i5.1819