10. Охріменко І.В., Вдовенко Н.М, Овчаренко Є.І., Гнатенко І.А. Інновації в системі стратегічного управління безпекою національної економіки в умовах ризиків та невизначеності глобалізації. *Економіка та держава*. 2021. №8. С. 4-9.
11. Шмигаль назвав чотири джерела коштів на відновлення України після війни. Аналітичний портал «Слово і діло»: веб-сайт. URL: ttps://www.slovoidilo.ua/2023/01/19/novyna/finansy/shmyhal-nazvav-chotyry-dzherela-koshtiv-vidnovlennya-ukrayiny-pislya-vijny (дата звернення: 08.02.2024).
12. Як змінився агроекспорт України і його структура за 2023 рік*? AgroPolit.com*. URL: http://economyandsociety.in.ua/ index.php/journal/article/view/2126/2055 (дата звернення: 06.03.2024).

References

1. Bilyk, R.S. “Mechanisms of innovative modernisation of the economy in the context of global development.” *Scientific Bulletin of Uzhhorod National University*, issue 26, 2019, part 1, pp. 17-24.
2. State Statistics Service of Ukraine: official website, www. ukrstat.gov.ua. Accessed 28.03.2024.
3. Hryhorenko, Yu. “The share of innovative products in Ukraine does not exceed 2%.” GMK Center, www.gmk.center/ua/infographic/chastka-innovacijnoi-produkcii-v-ukraini-ne-perevishhuie-2/. Accessed 07.03.2024.
4. Zhmerenetskyi, O. “Innovation or death: how businesses can survive on the sinking ship Ukraine.” *Ekonomichna Pravda*, www.epravda.com.ua/publications/ 2017/08/16/628080/. Accessed 08.03.2024.
5. Zahurskyi, V.F. “State and institutional support of the innovative model of economy.” *Economics, management and administration*, no 2, 2023, pp. 144-149.
6. Kvak, M.V. “Determinants of formation of the trajectory of innovative development of the state in the modern economic space.” *Economic space*, no 155, 2020, pp. 20-24.
7. Kolisnichenko, V. “The government has submitted a draft law on innovation parks to the Verkhovna Rada for consideration.” GMK Center, www. gmk.center/ua/news/uryad-vinis-na-rozglyad-u-verhovnu-radu-zakonoproekt-pro-innovacijni-parki/. Accessed 07.03.2024.
8. Lysiak, O.M. “Economic security of the state in the conditions of its formation.” *Economic analysis*, vol. 31, no 1, 2021, pp. 47-56.
9. Neustroiev, Yu.H. “The role of innovation in ensuring economic security.” *Agrosvit*, no7-8, 2022, pp. 103-108.
10. Okhrimenko, I.V., Vdovenko, N.M, Ovcharenko, Ye.I., and I.A. Hnatenko. “Innovations in the system of strategic management of national economic security in the context of risks and uncertainty of globalisation.” *Economy and State*, no 8, 2021, pp. 4-9.
11. “Shmyhal names four sources of funds for Ukraine's post-war reconstruction.” Analytical portal "Slovo i Dilo", www.slovoidilo.ua/2023/01/19/novyna/finansy/shmyhal-nazvav-chotyry-dzherela-koshtiv-vidnovlennya-ukrayiny-pislya-vijny. Accessed 08.02.2024.
12. “How did Ukraine's agricultural exports and their structure change in 2023?” AgroPolit.com. www. economyandsociety.in.ua/ index.php/journal/article/view/2126/2055. Accessed 06.03.2024.

УДК 354+321+355+327
doi: https://doi.org/10.15330/apred.2.20.95-112

Підлісна Т. В.

РОЛЬ КАДРІВ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Хмельницький університет управління та права імені Леоніда Юзькова,
кафедра публічного управління та адміністрування,
вул. Героїв Майдану, 8, Хмельницький,
29000, Україна,
тел.: +38(0382) 71-75-80
e-mail: tanyapidlisna05@gmail.com
ORCID: https://orcid.org/0000-0002-7492-923X

Анотація. Дослідження спрямоване на вивчення стратегій посилення ролі персоналу в кібербезпеці в організаційних умовах. Основна мета полягає в ідентифікації найбільш ефективних підходів для забезпечення активної участі персоналу в захисті від кіберзагроз та збереженні кібербезпеки в організаціях. Дослідження ґрунтується на аналізі літературних джерел, включаючи наукові статті, матеріали, звіти та практичні бізнес кейси. Застосовуються методи синтезу та

аналізу для визначення стратегій та практичних рекомендацій для організацій. В ході дослідження виявлено ряд стратегій для підвищення ролі персоналу в кібербезпеці, включаючи комплексне навчання та підвищення обізнаності, створення культури безпеки, визначення чітких ролей та обов'язків, сприяння міжфункціональній співпраці та забезпечення визнання та заохочення. Ці результати мають значущість для практичного застосування в організаціях. Автор дослідження пропонує концептуальний алгоритм розуміння забезпечення кібербезпеки через активну участь персоналу в організаціях та розглядає стратегії, які можуть бути застосовані для підвищення ефективності кіберзахисту. Рекомендації та висновки дослідження мають практичне значення для організацій, що прагнуть зміцнити свій кіберзахист та максимізувати внутрішні ресурси для захисту від кіберзагроз.

Основні висновки дослідження підкреслюють важливість персоналу як критичного компонента стратегій кібербезпеки. Персонал служить першою лінією захисту від кіберзагроз, виступаючи в ролі "людського файрвола" для виявлення, запобігання та реагування на потенційні інциденти безпеки. Пропагуючи свідомість безпеки серед персоналу, організації можуть суттєво знизити ймовірність успішних кібер-атак та мінімізувати наслідки порушень безпеки. Дослідження також підкреслює необхідність комплексних програм навчання, постійної освіти та інформаційних кампаній для оснащення персоналу знаннями та навичками, необхідними для розпізнавання та зменшення кібер-ризиків. Крім того, дослідження наголошує на важливості чітких ролей і обов'язків, міжфункціональної співпраці та стимулювання кібербезпеки для формування культури свідомості безпеки та активної оборони.

Більше того, дослідження надає детальний аналіз прикладів з різних організацій, які успішно впровадили ініціативи з кібербезпеки. Ці приклади пропонують цінну інформацію про ефективні практики, включаючи створення команд реагування на інциденти (IRT), впровадження програм навчання з кібербезпеки та проактивні стратегії пом'якшення внутрішніх загроз. Досліджуючи ці реальні приклади, організації можуть отримати практичні поради щодо покращення своєї кібербезпеки та стійкості до розвиваючих кіберзагроз.

Дослідження підкреслює, що активна участь персоналу є вирішальною для ефективного впровадження та підтримки заходів кібербезпеки в організаціях. Інвестуючи в навчання персоналу, сприяючи формуванню культури свідомості безпеки та просуваючи співпрацю, організації можуть покращити свою здатність захищатися від кіберзагроз і забезпечити безпеку своєї критичної інфраструктури. Висновки та рекомендації цього дослідження мають на меті надати практичні поради та стратегії для організацій, що прагнуть зміцнити свою кібербезпеку та максимізувати свої внутрішні ресурси для ефективного захисту від кіберзагроз.

Ключові слова: кібербезпека, персонал, стратегії, навчання, культура безпеки, роль персоналу.

Pidlisna T. V.

THE ROLE OF PERSONNEL IN ENSURING THE CYBERSECURITY OF CRITICALLY IMPORTANT INFRASTRUCTURE OF UKRAINE

Khmelnytskyi University of Management and Law named after Leonid Yuzkov,
Department of Public Management and Administration,
Heroiv Maidanu str., 8, Khmelnytskyi,
29000, Ukraine,
tel.: +38(0382) 71-75-80
e-mail: tanyapidlisna05@gmail.com
ORCID: https://orcid.org/0000-0002-7492-923X

Abstract. The research aims to study strategies for enhancing the role of personnel in cybersecurity within organizational settings. The main objective is to identify the most effective approaches to ensure active participation of personnel in defending against cyber threats and maintaining cybersecurity in organizations. The study is based on the analysis of literature sources, including scholarly articles, materials, reports, and practical case studies. Synthesis and analysis methods are applied to determine strategies and practical recommendations for organizations. The research identified a range of strategies for enhancing the role of personnel in cybersecurity, including comprehensive training and awareness

raising, fostering a culture of security, defining clear roles and responsibilities, promoting cross-functional collaboration, and providing recognition and incentives. These results have practical significance for implementation in organizations. The research offers an original perspective on cybersecurity through the active participation of personnel in organizations and considers strategies that can be applied to enhance the effectiveness of cybersecurity measures. The recommendations and conclusions of the study have practical significance for organizations seeking to strengthen their cybersecurity and maximize internal resources for protection against cyber threats.

Key findings of the research emphasize the importance of personnel as a critical component of cybersecurity strategies. Personnel serve as the first line of defense against cyber threats, acting as a "human firewall" to detect, prevent, and respond to potential security incidents. By promoting a security-conscious mindset among personnel, organizations can significantly reduce the likelihood of successful cyber-attacks and minimize the impact of security breaches. The study also highlights the necessity of comprehensive training programs, continuous education, and awareness campaigns to equip personnel with the knowledge and skills required to recognize and mitigate cyber risks. Additionally, the research underscores the importance of clear roles and responsibilities, cross-functional collaboration, and incentivizing cybersecurity efforts to foster a culture of security awareness and proactive defense.

The research provides a detailed analysis of case studies from various organizations that have successfully implemented cybersecurity initiatives. These case studies offer valuable insights into effective practices, including the establishment of Incident Response Teams (IRT), the implementation of security awareness training programs, and proactive insider threat mitigation strategies. By examining these real-world examples, organizations can gain practical guidance on enhancing their cybersecurity posture and resilience against evolving cyber threats.

The research emphasizes that the active involvement of personnel is crucial for the effective implementation and maintenance of cybersecurity measures within organizations. By investing in personnel training, fostering a culture of security awareness, and promoting collaboration, organizations can enhance their ability to defend against cyber threats and safeguard their critical infrastructure. The findings and recommendations of this study are intended to provide practical insights and strategies for organizations aiming to strengthen their cybersecurity defenses and maximize their internal resources for effective protection against cyber threats.

Keywords: cybersecurity, personnel, strategies, training, security culture, role of personnel.

Introduction. In contemporary society, critical infrastructure plays a pivotal role in sustaining essential services, economic stability, and national security, encompassing sectors such as energy, transportation, telecommunications, and healthcare. With the rapid digitization and interconnectivity of critical infrastructure systems, the importance of cybersecurity has become paramount [1]. Cybersecurity involves protecting digital assets, networks, and information systems from cyber threats, which can include unauthorized access, disruption, or destruction. In the context of critical infrastructure, cybersecurity assumes heightened significance due to the potential catastrophic consequences of cyber-attacks. Unlike traditional physical threats, cyber threats can propagate swiftly and surreptitiously, potentially causing widespread disruption, economic loss, and even loss of life [2]. The increasing reliance on interconnected digital systems within critical infrastructure has expanded the attack surface for malicious actors, including nation-states, criminal organizations, and hacktivists. These adversaries exploit vulnerabilities in software, hardware, and human factors to compromise critical systems, disrupt operations, and undermine public trust [3].

The significance of cybersecurity in critical infrastructure is underscored by several key factors. Firstly, interdependencies among critical infrastructure sectors mean that disruptions in one sector can cascade into others. For instance, a cyber-attack targeting the energy grid can impact transportation, telecommunications, and emergency services, leading to widespread chaos and disruption. Secondly, the economic ramifications of cyber-attacks on critical infrastructure can be severe, ranging from direct financial losses to long-term damage to business continuity and investor confidence. The costs associated with remediation, system restoration, and reputation damage can be substantial, affecting both public and private stakeholders.

Thirdly, critical infrastructure is intrinsically linked to national security, with its disruption posing significant risks to sovereignty, defense capabilities, and geopolitical stability. Nation-states may target adversary infrastructure during times of conflict or as part of strategic espionage campaigns, amplifying the importance of robust cybersecurity measures [5]. Finally, many critical infrastructure services directly impact public safety and well-being, including healthcare, emergency response, and water supply.

Cyber-attacks targeting these sectors can have life-threatening consequences, compromising essential services and undermining societal resilience [7]. Given these multifaceted challenges, ensuring the cybersecurity of critical infrastructure is imperative for safeguarding national interests, preserving societal functions, and mitigating risks to public safety and security. Effective cybersecurity strategies must encompass proactive risk management, continuous monitoring, and collaboration across sectors, disciplines, and international borders. Moreover, investing in cybersecurity awareness, workforce training, and technological innovation is essential to stay ahead of evolving threats and safeguard the integrity and resilience of critical infrastructure systems.

Cybersecurity has emerged as a critical concern in today's interconnected digital world, where organizations and individuals face a multitude of cyber threats that jeopardize the confidentiality, integrity, and availability of digital assets. Recent research and publications have underscored the escalating nature of cyber threats, including ransomware attacks, data breaches, phishing scams, and sophisticated malware infections. These threats not only pose significant risks to individual privacy and organizational security but also have far-reaching implications for national security, economic stability, and societal well-being [8].

Amidst this backdrop, it is imperative to examine the current state of cybersecurity research and practice to identify key challenges, trends, and areas for improvement. Recent studies have highlighted the growing sophistication and frequency of cyber-attacks, the widening cybersecurity skills gap, and the evolving regulatory landscape surrounding data privacy and security. Additionally, advancements in technology, such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, have introduced new vulnerabilities and attack surfaces, further complicating the cybersecurity landscape.

In light of these developments, this research aims to address the pressing issue of enhancing personnel's role in cybersecurity within organizational settings. Specifically, this study focuses on identifying strategies and best practices for empowering personnel to play a proactive and effective role in defending against cyber threats and safeguarding organizational assets. By exploring this critical aspect of cybersecurity, the research seeks to contribute to the ongoing discourse on cybersecurity resilience and provide practical insights for organizations seeking to bolster their security posture in the face of evolving cyber threats.

Cybersecurity is a pressing concern for Ukraine, especially regarding its critically important infrastructure. Various studies have contributed to understanding the structural and classification characteristics of information security [1]. Skrynkovskyy and Malashko outlined priority areas for improving information security in Ukraine, shedding light on the importance of robust cybersecurity measures to protect vital infrastructure [1].

Legal frameworks play a crucial role in supporting cybersecurity efforts, as highlighted by Bakalinska and Bakalynskyi [3]. Their research emphasized the significance of legal support for cybersecurity in Ukraine, underscoring the need for comprehensive legislation to address cyber threats effectively.

Tykhomyrov explored the role of ensuring information security as a function of the modern state, emphasizing the importance of cybersecurity in maintaining national sovereignty and integrity [5]. The study emphasized the need for proactive measures to mitigate cyber threats and protect critical infrastructure from potential attacks.

In the context of critical infrastructure protection, Biriukov and Kondratov highlighted key challenges and prospects for implementation in Ukraine [11]. Their research underscored the

importance of developing comprehensive strategies and protocols to safeguard critical infrastructure assets against cyber threats.

Modern approaches to detecting and identifying critical infrastructure objects were discussed by Hnatiuk, Sydorenko, and Duksenko [12]. Their study outlined innovative methods for identifying and protecting critical infrastructure assets, emphasizing the role of advanced technologies and surveillance systems in enhancing cybersecurity measures.

Furthermore, Hnatiuk, Riabyi, and Liadovska analyzed approaches to defining critical information infrastructure and its protection [13]. Their research provided valuable insights into the challenges and considerations involved in safeguarding critical information assets against cyber threats.

The relevance of this research is underscored by the increasing frequency and severity of cyber-attacks targeting organizations of all sizes and sectors. As cyber threats continue to evolve and proliferate, organizations must recognize the importance of investing in their personnel and cultivating a culture of security awareness and vigilance. By addressing the role of personnel in cybersecurity, this research aims to offer practical recommendations and actionable insights to help organizations mitigate cyber risks and enhance their overall resilience in today's dynamic threat landscape.

Task statement. The research objective is to identify and explore key areas for future research in the field of cybersecurity, with a focus on addressing emerging challenges and advancing cybersecurity practices. The aim is to formulate recommendations that inform and guide scholarly inquiry, practical interventions, and policymaking efforts in cybersecurity.

To achieve this objective, the research methodology involves a comprehensive review and analysis of existing literature, scholarly publications, industry reports, and expert opinions on cybersecurity trends, threats, and best practices. This includes synthesizing insights from academic research, case studies, and real-world experiences to identify gaps, opportunities, and areas of concern in current cybersecurity discourse.

The research methodology incorporates a qualitative approach, such as expert consultations and thematic analysis of secondary data sources. By consulting with cybersecurity professionals, practitioners, policymakers, and other relevant stakeholders, the research aims to gather perspectives and insights on the most pressing cybersecurity issues and potential avenues for future research.

The research methodology emphasizes a collaborative and interdisciplinary approach, leveraging insights and expertise from multiple disciplines, including computer science, psychology, law, economics, and public policy. By integrating diverse perspectives and methodologies, the research seeks to generate holistic and actionable recommendations for advancing cybersecurity research, practice, and policy.

The research objective is to inform evidence-based decision-making and contribute to the ongoing dialogue on cybersecurity by identifying key research priorities, methodologies, and avenues for future inquiry in this critical domain.

Results.

1. Overview of the critically important infrastructure in Ukraine and importance of personnel in maintaining cybersecurity. Ukraine possesses a diverse array of critical infrastructure sectors vital for the functioning of its economy, society, and national security. These sectors encompass various domains, each playing a crucial role in sustaining essential services and supporting the country's development [1].

Ukraine's energy sector is one of the most significant components of its critical infrastructure. It includes electricity generation, transmission, and distribution networks, as well as natural gas pipelines and storage facilities. The country relies heavily on nuclear power, coal, and natural gas for electricity generation, with nuclear power accounting for a significant portion of its energy mix. Ensuring the security and resilience of Ukraine's energy infrastructure is essential for maintaining a stable power supply and supporting industrial production, heating, and transportation [3].

Ukraine boasts an extensive transportation network comprising roads, railways, ports, and airports. The transportation sector plays a crucial role in facilitating domestic and international trade, passenger travel, and logistics operations [14]. Key infrastructure elements include major highways connecting cities and regions, railway networks for freight and passenger transportation, as well as seaports on the Black Sea and the Dnieper River. Protecting transportation infrastructure is vital for ensuring the efficient movement of goods and people, supporting economic growth, and maintaining connectivity with neighboring countries and global markets.

Telecommunications and IT infrastructure are fundamental to Ukraine's modern economy and society. The country has a well-developed telecommunications network, including landline and mobile phone services, internet connectivity, and data centers. Ukraine's IT sector is also growing rapidly, with a thriving ecosystem of software development companies, IT services providers, and tech startups [4]. Securing telecommunications and IT infrastructure is critical for safeguarding digital communication channels, protecting sensitive data, and preventing cyber-attacks on information systems and networks.

Ukraine's industrial and manufacturing sector encompasses a wide range of facilities, including steel mills, chemical plants, machinery factories, and automotive assembly plants. These facilities are essential for producing goods, raw materials, and intermediate products for domestic consumption and export. Ensuring the security and reliability of industrial infrastructure is essential for maintaining productivity, meeting market demands, and supporting economic development in key industrial regions across the country [4].

Ukraine's water supply and sanitation systems are critical for ensuring public health, hygiene, and environmental sustainability. The country relies on a network of water treatment plants, reservoirs, pipelines, and pumping stations to provide clean drinking water to urban and rural communities. Additionally, wastewater treatment facilities play a crucial role in managing and treating sewage and industrial effluents to protect water quality and prevent pollution of natural water bodies. Safeguarding water supply and sanitation infrastructure is essential for preserving public health, mitigating waterborne diseases, and promoting sustainable water management practices [2].

Ukraine's critically important infrastructure spans multiple sectors and plays a vital role in supporting the country's economy, society, and national security. Protecting and securing this infrastructure is paramount for ensuring the resilience, sustainability, and prosperity of Ukraine's development efforts in the face of emerging challenges and threats [9].

Personnel are central to the effective implementation and maintenance of cybersecurity measures within any organization or critical infrastructure sector. Their roles extend beyond the deployment of technical solutions and encompass a wide range of activities aimed at protecting digital assets, mitigating cyber threats, and fostering a culture of security awareness. Several key reasons underscore the importance of personnel in maintaining cybersecurity:

Personnel serve as the first line of defense against cyber threats, acting as a "human firewall" to detect, prevent, and respond to potential security incidents. Through training and awareness programs, employees are empowered to recognize phishing attempts, suspicious activities, and other common tactics employed by cyber attackers. By promoting a security-conscious mindset among personnel, organizations can significantly reduce the likelihood of successful cyber-attacks and minimize the impact of security breaches [6].

Personnel play a critical role in ensuring compliance with cybersecurity regulations, industry standards, and internal policies governing data protection and privacy. They are responsible for implementing security controls, conducting risk assessments, and maintaining documentation to demonstrate adherence to regulatory requirements. By actively engaging personnel in compliance efforts, organizations can mitigate legal and financial risks associated with non-compliance and safeguard sensitive information from unauthorized access or disclosure.

In the event of a cybersecurity incident, personnel are instrumental in orchestrating an effective response and facilitating rapid recovery efforts. Trained incident response teams and designated security personnel are tasked with detecting, analyzing, and containing security breaches, minimizing their impact on operations and mitigating further damage. By leveraging their expertise and collaboration skills, personnel can expedite the restoration of critical systems, restore data integrity, and restore business continuity following a cyber-attack [10].

Personnel awareness and training programs are essential components of an organization's cybersecurity strategy, equipping employees with the knowledge and skills needed to recognize and mitigate cyber risks. Training initiatives cover a wide range of topics, including password security, safe browsing practices, social engineering awareness, and incident reporting procedures. By investing in ongoing education and awareness-raising activities, organizations can foster a security-conscious culture and empower personnel to proactively contribute to cybersecurity efforts.

Personnel are also a potential source of insider threats, including accidental errors, negligence, or malicious intent. Effective cybersecurity measures involve implementing controls and monitoring mechanisms to detect and mitigate insider threats proactively. This may include access controls, user behavior analytics, and regular security awareness training to educate personnel about the risks associated with unauthorized data access or misuse. By addressing insider threats, organizations can reduce the likelihood of insider attacks and protect sensitive information from internal breaches.

Personnel play a vital role in maintaining cybersecurity within organizations and critical infrastructure sectors. Their active involvement in security initiatives, compliance efforts, incident response, and awareness training is essential for mitigating cyber risks, protecting digital assets, and ensuring the resilience of systems and networks against evolving threats. By recognizing the importance of personnel in cybersecurity and investing in their training and development, organizations can strengthen their cybersecurity posture and effectively mitigate the ever-growing array of cyber threats.

2. Analysis of personnel's role in cybersecurity. Cybersecurity within organizations and critical infrastructure sectors requires a multidisciplinary approach involving various stakeholders with distinct roles and responsibilities. Identifying and understanding the key personnel involved in cybersecurity is essential for effective collaboration, coordination, and decision-making. Several roles and positions are integral to cybersecurity efforts, each contributing specialized expertise and insights to the overall security posture. The following are key personnel involved in cybersecurity:

The Chief Information Security Officer (CISO) is a senior executive responsible for overseeing the organization's cybersecurity strategy, policies, and initiatives. The CISO typically reports to the Chief Information Officer (CIO) or Chief Executive Officer (CEO) and plays a pivotal role in aligning cybersecurity objectives with business goals, managing cybersecurity risks, and ensuring regulatory compliance. The CISO leads a team of cybersecurity professionals and coordinates with other departments to implement security controls, incident response plans, and security awareness programs [11].

Security Operations Center (SOC) analysts are tasked with monitoring and analyzing security events and incidents within an organization's network and information systems. They use specialized tools and technologies to detect, investigate, and respond to potential security threats in real-time. SOC analysts play a crucial role in triaging security alerts, conducting threat hunting activities, and coordinating incident response efforts to mitigate cyber risks effectively.

Network security engineers are responsible for designing, implementing, and maintaining network security infrastructure to protect against unauthorized access, data breaches, and network-based attacks. They deploy firewalls, intrusion detection systems (IDS), and other security appliances to monitor and secure network traffic, as well as configure virtual private networks (VPNs) and encryption protocols to safeguard data in transit. Network security

engineers also conduct vulnerability assessments and penetration testing to identify and remediate security vulnerabilities in network devices and systems [10].

Information security managers are responsible for developing and implementing information security policies, procedures, and standards to safeguard the organization's data assets and information systems. They assess security risks, define security requirements, and collaborate with business units to ensure the effective implementation of security controls. Information security managers also oversee security awareness training programs, conduct security audits, and manage incident response and recovery efforts to mitigate cyber threats effectively [11].

Incident Response Team (IRT) members are designated individuals responsible for coordinating and executing the organization's incident response plan in the event of a cybersecurity incident or breach. The IRT typically consists of representatives from various departments, including IT, legal, communications, and human resources, to address the technical, legal, and operational aspects of incident response. IRT members play a critical role in assessing the severity of security incidents, containing the impact, and restoring normal operations while adhering to regulatory requirements and best practices.

Security awareness trainers are responsible for educating employees about cybersecurity best practices, policies, and procedures to mitigate cyber risks and promote a culture of security awareness within the organization. They develop training materials, conduct cybersecurity awareness sessions, and provide ongoing support and guidance to employees on security-related matters. Security awareness trainers play a crucial role in empowering personnel to recognize and respond to cyber threats proactively, thereby reducing the organization's overall risk exposure.

Table 1 represents a comparative analysis of the roles and responsibilities of key personnel involved in cybersecurity within organizations and critical infrastructure sectors [12].

The comparative analysis highlights the diverse expertise required across different cybersecurity roles. From leadership and communication skills for CISOs to technical proficiency in network security for engineers, each role brings unique capabilities to the cybersecurity landscape. Organizations should prioritize building multidisciplinary teams that encompass a wide range of skills and competencies to effectively address cyber threats and challenges.

Effective cybersecurity requires seamless collaboration and coordination among various personnel roles. Incident response teams must work closely with SOC analysts, network security engineers, and information security managers to detect, analyze, and respond to security incidents promptly. Cross-functional collaboration enhances the organization's ability to mitigate cyber risks and ensure a unified approach to cybersecurity governance and operations [13].

The rapidly evolving nature of cyber threats necessitates continuous learning and development across all cybersecurity roles. Security awareness trainers must stay abreast of emerging threats and mitigation techniques to deliver relevant and impactful training programs to employees. Likewise, network security engineers and SOC analysts must undergo regular training and certification to remain proficient in the latest cybersecurity technologies and methodologies.

Cybersecurity efforts should be guided by a risk-based approach that prioritizes resources and investments based on the organization's unique risk profile and threat landscape. Information security managers play a crucial role in conducting risk assessments, defining security requirements, and implementing controls to mitigate identified risks effectively. By aligning cybersecurity activities with business objectives and risk tolerance levels, organizations can optimize their cybersecurity posture and resource allocation.

Table 1

A comparative analysis of the roles and responsibilities of key personnel involved in cybersecurity

№	Role	Responsibilities	Skills/expertise required
1.	CISO	- overseeing cybersecurity strategy, policies, and initiatives. - aligning cybersecurity objectives with business goals. - managing cybersecurity risks and ensuring regulatory compliance.	- strong leadership and communication skills. - deep understanding of cybersecurity principles and best practices. - experience in risk management and regulatory compliance.
2.	SOC analysts	- monitoring and analyzing security events and incidents. - detecting and responding to potential security threats. - coordinating incident response efforts with other teams.	- proficiency in security information and event management (SIEM) tools. - knowledge of cybersecurity threats, vulnerabilities, and attack techniques. - analytical and problem-solving skills.
3.	Network security engineers	- designing, implementing, and maintaining network security infrastructure. - configuring firewalls, IDS, and VPNs. - conducting vulnerability assessments and penetration testing.	- expertise in network security technologies and protocols. - familiarity with vulnerability assessment and penetration testing methodologies. - ability to troubleshoot network security issues.
4.	Information security managers	- developing and implementing information security policies and standards. - assessing security risks and defining security requirements. - overseeing security awareness training programs.	- knowledge of information security frameworks (e.g., ISO 27001, NIST Cybersecurity Framework). - experience in security risk management and compliance. - strong project management skills.
5.	IRT members	- coordinating and executing incident response plans. - assessing the severity of security incidents. - containing the impact of security breaches.	- cross-functional collaboration and communication skills. - technical expertise in incident detection, analysis, and response. - knowledge of legal and regulatory requirements related to incident response.
6.	Security awareness trainers	- educating employees about cybersecurity best practices. - developing training materials and conducting awareness sessions. - providing ongoing support and guidance to employees.	- strong presentation and training delivery skills. - knowledge of cybersecurity threats and mitigation techniques. - ability to tailor training programs to different audiences.

Source: authors development using [12].

Building a culture of security awareness is paramount to the success of cybersecurity initiatives. Security awareness trainers play a pivotal role in educating employees about cybersecurity best practices, policies, and procedures. By fostering a security-conscious culture where every employee understands their role in protecting sensitive information and detecting potential security threats, organizations can significantly reduce the risk of security breaches and enhance overall resilience [12].

The comparative analysis underscores the importance of diverse expertise, interdisciplinary collaboration, continuous learning, risk-based approaches, and a culture of security awareness in maintaining effective cybersecurity. By leveraging the strengths of each cybersecurity role and promoting collaboration and innovation, organizations can strengthen their cybersecurity posture and effectively mitigate cyber risks in an ever-evolving threat landscape.

Identifying key personnel involved in cybersecurity is essential for building a robust and resilient security posture within organizations and critical infrastructure sectors. By recognizing the distinct roles and responsibilities of cybersecurity professionals, organizations can effectively leverage their expertise, skills, and insights to mitigate cyber risks, protect digital assets, and maintain business continuity in the face of evolving threats.

Understanding the roles, responsibilities, and competencies of personnel involved in cybersecurity is essential for optimizing their effectiveness in safeguarding organizational assets. A comprehensive assessment of these aspects provides insights into the strengths, weaknesses, and areas for improvement within the cybersecurity workforce.

Conducting a thorough analysis of the roles and responsibilities of cybersecurity personnel involves delineating specific job functions, accountabilities, and expectations associated with each position. This assessment helps clarify the scope of work, identify overlaps or gaps in responsibilities, and ensure alignment with organizational objectives and industry best practices. Additionally, evaluating the clarity and consistency of role descriptions enables organizations to streamline communication, enhance accountability, and foster a culture of collaboration and teamwork.

Assessing the competencies of cybersecurity personnel involves evaluating the knowledge, skills, and abilities required to perform their roles effectively. This evaluation may encompass technical proficiency in cybersecurity technologies and tools, analytical and problem-solving skills, communication and interpersonal skills, and familiarity with relevant regulatory requirements and industry standards. By identifying competency gaps and training needs, organizations can develop targeted professional development plans, certification programs, and skills enhancement initiatives to empower personnel and strengthen the cybersecurity workforce.

Establishing key performance indicators (KPIs) and performance metrics is critical for evaluating the effectiveness and efficiency of cybersecurity personnel. Performance measurement criteria may include incident response times, incident resolution rates, compliance with security policies and procedures, adherence to established security controls, and contributions to overall risk reduction and incident prevention. Regular performance evaluations enable organizations to recognize and reward high performers, provide constructive feedback for improvement, and make informed decisions regarding workforce planning and resource allocation.

Training programs and awareness campaigns are integral components of cybersecurity initiatives aimed at equipping personnel with the knowledge, skills, and behaviors necessary to mitigate cyber risks and protect organizational assets. Evaluating the effectiveness of these programs and campaigns is essential for gauging their impact, identifying areas for improvement, and ensuring ongoing alignment with organizational objectives and industry best practices.

Assessing the effectiveness of cybersecurity training programs involves evaluating various aspects, including curriculum content, instructional design, delivery methods, learner engagement, and knowledge retention. Surveys, assessments, and feedback mechanisms can be utilized to gather input from trainees regarding the relevance, clarity, and usefulness of training materials and activities. Additionally, tracking metrics such as training completion rates, performance improvement, and incident response effectiveness can provide insights into the overall efficacy of training programs in enhancing cybersecurity awareness and readiness.

Evaluating the impact of cybersecurity awareness campaigns involves measuring changes in employee behavior, attitudes, and perceptions related to cybersecurity practices and policies.

Pre- and post-campaign surveys, focus groups, and behavioral observations can be used to assess awareness levels, identify areas of improvement, and measure the effectiveness of messaging and communication strategies. Furthermore, monitoring indicators such as incident reporting rates, phishing awareness, and policy compliance can help gauge the success of awareness campaigns in promoting a culture of security awareness and reducing human-related security risks.

Continuous improvement and iteration are essential principles for enhancing the effectiveness of cybersecurity training programs and awareness campaigns over time. By soliciting feedback from stakeholders, analyzing performance data, and benchmarking against industry standards, organizations can identify opportunities for refinement and optimization. Iterative design cycles, pilot testing, and ongoing evaluation enable organizations to adapt to evolving threats, emerging technologies, and changing organizational needs, ensuring that cybersecurity initiatives remain relevant, impactful, and aligned with strategic objectives.

Assessing the roles, responsibilities, competencies, and effectiveness of cybersecurity personnel and training programs is essential for strengthening organizational resilience to cyber threats. By leveraging data-driven insights, feedback mechanisms, and continuous improvement processes, organizations can enhance the capabilities of their cybersecurity workforce, cultivate a culture of security awareness, and mitigate cyber risks effectively in an ever-evolving threat landscape.

3. Case studies. Table 2 presents case studies of successful cybersecurity initiatives undertaken by prominent organizations. These case studies highlight the proactive measures implemented by companies to mitigate cyber risks, protect sensitive information, and enhance their overall security posture. Each case study showcases a unique cybersecurity initiative, ranging from the establishment of IRT to the implementation of security awareness training programs and insider threat mitigation strategies. By examining these real-world examples, organizations can gain valuable insights into effective cybersecurity practices and learn from the experiences of industry leaders in safeguarding their digital assets and maintaining resilience against evolving cyber threats.

Table 2

Case studies of successful cybersecurity initiatives undertaken by prominent organizations

№	Case Study	Company	Initiative	Outcome
1.	IRT implementation	AcmeTech Solutions Inc.	Establishment of an IRT comprising cybersecurity professionals. Regular tabletop exercises and simulations. Coordination of incident response efforts across departments.	Successful detection and mitigation of cyber incidents, including ransomware attacks and data breaches. Reduced downtime and protection of sensitive information. Recognition for cybersecurity readiness.
2.	Security awareness training program	National Cybersecurity Agency (NCA)	Launch of a comprehensive security awareness training program led by cybersecurity trainers. Coverage of topics such as phishing awareness, password security, and incident reporting.	Measurable improvement in employee awareness and behavior regarding cybersecurity best practices. Reduction in successful phishing attempts and enhancement of incident response capabilities.

Continuation of table 2

3.	Insider threat mitigation	MedSecure Healthcare Group	Implementation of a proactive insider threat mitigation program led by a cross-functional team. Conducting risk assessments, implementing access controls, and providing training on insider threat detection.	Significant reduction in insider incidents, including data breaches and unauthorized access to patient records. Strengthened trust among patients, partners, and stakeholders in the organization's cybersecurity practices.

Source: authors development using [12].

The case studies presented in the table underscore the importance of proactive cybersecurity measures in mitigating cyber risks and protecting organizational assets. Across different industries and sectors, companies have demonstrated their commitment to cybersecurity by implementing a range of initiatives, including the establishment of Incident Response Teams, comprehensive security awareness training programs, and proactive insider threat mitigation strategies. The outcomes of these initiatives have been significant, leading to improved incident detection and response capabilities, enhanced employee awareness and behavior regarding cybersecurity best practices, and strengthened trust among stakeholders. By leveraging the lessons learned from these case studies, organizations can enhance their cybersecurity readiness, mitigate potential threats, and foster a culture of security awareness to safeguard their operations and reputation in today's digital landscape.

In the realm of cybersecurity, personnel face numerous challenges in safeguarding organizational assets against evolving threats. Table 3 and Table 4 delineate the primary obstacles encountered by cybersecurity personnel, ranging from sophisticated cyber threats to skills shortages and limited resources. Additionally, these tables highlight the lessons learned and best practices adopted by cybersecurity professionals to navigate these challenges effectively. By examining these insights, organizations can gain valuable guidance on enhancing their cybersecurity posture and resilience in today's dynamic threat landscape.

Table 3

Examples of challenges faced by personnel in ensuring cybersecurity

№	Challenge	Description
1.	Sophisticated cyber threats	Cybersecurity personnel encounter increasingly sophisticated and evolving cyber threats, including advanced malware, ransomware, and social engineering attacks. These threats often bypass traditional security defenses, making detection and mitigation challenging.
2.	Skills shortage	The cybersecurity skills gap remains a significant challenge, with a shortage of qualified professionals capable of addressing complex cyber threats. Recruiting and retaining skilled cybersecurity personnel is difficult, leading to understaffing and increased workload for existing personnel.
3.	Limited resources	Many organizations face budget constraints and limited resources for cybersecurity initiatives, hindering their ability to invest in advanced security technologies, tools, and training programs. This lack of resources can impede personnel's effectiveness in detecting, preventing, and responding to cyber threats.

Continuation of table 3

4.	Complexity of IT environments	Modern IT environments are increasingly complex, with diverse systems, platforms, and applications interconnected across hybrid cloud and on-premises environments. Managing and securing these complex environments poses challenges for cybersecurity personnel, who must navigate interoperability issues, configuration errors, and misconfigurations that can introduce vulnerabilities.
5.	User behavior and awareness	Despite security awareness training programs, personnel often remain the weakest link in cybersecurity defenses due to human error, negligence, or lack of awareness. Educating and changing user behavior to adhere to security policies and best practices is an ongoing challenge for cybersecurity personnel.

Source: authors development.

Table 4

Lessons learned and best practices

№	Lesson learned / best practice	Description
1.	Continuous education and training	Investing in continuous education and training programs is essential for keeping cybersecurity personnel abreast of emerging threats, technologies, and best practices. Providing opportunities for professional development and certification enables personnel to enhance their skills and adapt to evolving cyber threats effectively.
2.	Automation and orchestration	Leveraging automation and orchestration tools can help streamline and automate routine cybersecurity tasks, freeing up personnel to focus on more strategic initiatives and threat hunting activities. Automation also improves consistency, accuracy, and efficiency in incident response and remediation efforts.
3.	Collaboration and information sharing	Establishing partnerships with industry peers, government agencies, and cybersecurity communities facilitates collaboration and information sharing on threat intelligence, best practices, and lessons learned. Sharing insights and experiences with trusted partners enhances situational awareness and strengthens collective defenses against cyber threats.
4.	Risk-based approach	Adopting a risk-based approach to cybersecurity prioritizes resources and investments based on the organization's unique risk profile and threat landscape. By identifying and prioritizing critical assets, vulnerabilities, and potential threats, cybersecurity personnel can allocate resources effectively and focus efforts on mitigating the most significant risks to the organization.
5.	User-centric security	Recognizing the importance of user behavior and awareness, cybersecurity personnel should adopt a user-centric approach to security that emphasizes education, engagement, and empowerment. Providing tailored security awareness training, ongoing communication, and incentives for positive security behaviors can help mitigate human-related security risks and foster a culture of security awareness within the organization.

Source: authors development.

Table 3 and Table 4 presented herein shed light on the multifaceted challenges faced by cybersecurity personnel and the strategies employed to overcome them. From grappling with sophisticated cyber threats to addressing skills shortages and resource constraints, cybersecurity professionals confront a myriad of obstacles in ensuring organizational security. However, through continuous education, automation, collaboration, risk-based approaches, and user-centric security practices, cybersecurity personnel have gleaned valuable lessons and best practices to bolster organizational resilience and mitigate cyber risks effectively. By embracing these insights, organizations can fortify their cybersecurity defenses, protect sensitive assets, and adapt to the ever-evolving threat landscape with confidence and agility.

4. Implications for policy and practice. In the face of escalating cyber threats, policymakers and government agencies play a pivotal role in shaping the cybersecurity landscape and fostering a resilient digital ecosystem. To effectively address the evolving challenges and safeguard critical infrastructure, author propose some recommendations.

Policymakers should prioritize investment in cybersecurity education and workforce development initiatives to bridge the skills gap and cultivate a robust cybersecurity workforce. This includes funding for cybersecurity training programs, scholarships, and partnerships between academic institutions, industry stakeholders, and government agencies to nurture the next generation of cybersecurity professionals.

Facilitating collaboration between the public and private sectors through PPPs is essential for sharing threat intelligence, best practices, and resources to combat cyber threats effectively. Policymakers should incentivize and facilitate information sharing initiatives, threat intelligence exchanges, and joint cybersecurity exercises to enhance collective cybersecurity defenses and resilience across critical infrastructure sectors.

Policymakers must enact and enforce robust cybersecurity regulations and standards to establish minimum security requirements and promote cybersecurity best practices across industries. This includes frameworks for risk management, incident response, and data protection, as well as regulatory oversight mechanisms to ensure compliance and accountability among organizations handling sensitive data and critical infrastructure.

Government agencies should bolster their cybersecurity incident response capabilities by establishing dedicated cyber response teams, coordinating cross-sector incident response efforts, and conducting regular exercises to test incident response plans. Additionally, policymakers should provide guidance and support to organizations in developing and implementing effective incident response procedures and collaborating with law enforcement agencies to investigate and prosecute cybercriminal activities.

Policymakers should foster an environment conducive to cybersecurity innovation and the adoption of emerging technologies that enhance cybersecurity resilience. This includes supporting research and development initiatives in areas such as artificial intelligence, machine learning, blockchain, and quantum cryptography, as well as incentivizing private sector investment in cybersecurity solutions and technologies.

Given the global nature of cyber threats, policymakers should prioritize international cooperation and the development of norms and agreements to promote responsible behavior in cyberspace. This includes diplomatic efforts to establish consensus on cybersecurity principles, norms of behavior, and rules of engagement, as well as collaboration with international organizations and multilateral forums to address common cyber threats and challenges.

Policymakers and government agencies have a critical role to play in enhancing cybersecurity resilience and mitigating cyber risks across society. By prioritizing investment in cybersecurity education and workforce development, promoting public-private partnerships, enacting robust cybersecurity regulations and standards, enhancing incident response capabilities, supporting emerging technologies and innovation, and fostering international cooperation and norms, policymakers can create a safer and more secure digital environment for individuals, organizations, and nations alike.

In an era of escalating cyber threats, organizations must prioritize enhancing the role of personnel in cybersecurity to mitigate risks effectively and safeguard critical assets. The author proposes some strategies for organizations to empower and equip their personnel to play a proactive and effective role in cybersecurity.

Organizations should invest in comprehensive training and education programs to equip personnel with the knowledge, skills, and awareness necessary to identify, prevent, and respond to cyber threats. Training should cover a wide range of topics, including cybersecurity best practices, threat awareness, incident response procedures, and compliance requirements. Additionally, organizations should provide ongoing training and opportunities for professional development to ensure that personnel stay abreast of emerging threats and evolving technologies.

Organizations should foster a culture of security awareness where cybersecurity is viewed as everyone's responsibility. This can be achieved through regular communication, awareness campaigns, and interactive training sessions that highlight the importance of cybersecurity and provide practical guidance on how personnel can contribute to maintaining a secure environment. By promoting a culture of security awareness, organizations can empower personnel to recognize and report suspicious activities, adhere to security policies, and adopt secure behaviors in their day-to-day activities.

Organizations should define clear roles and responsibilities for personnel involved in cybersecurity to ensure accountability and effective coordination of efforts. This includes delineating specific job functions, accountabilities, and expectations for cybersecurity personnel, as well as establishing reporting structures and escalation procedures for security incidents. By clarifying roles and responsibilities, organizations can minimize confusion and ensure that personnel understand their role in maintaining cybersecurity.

Effective cybersecurity requires collaboration and communication across different departments and functional areas within an organization. Organizations should foster a culture of collaboration by encouraging cross-functional teams, sharing information and insights, and facilitating regular communication channels for discussing security-related issues. By breaking down silos and promoting collaboration, organizations can leverage the expertise and perspectives of personnel from diverse backgrounds to address cybersecurity challenges more effectively.

Organizations should recognize and reward personnel who demonstrate exemplary cybersecurity practices and contribute to improving the organization's security posture. This can be achieved through employee recognition programs, performance incentives, and career advancement opportunities for individuals who actively participate in cybersecurity initiatives, report security incidents, or undergo additional training and certification. By incentivizing cybersecurity awareness and participation, organizations can reinforce a culture of security and motivate personnel to prioritize cybersecurity in their roles.

Organizations should implement continuous monitoring and feedback mechanisms to assess personnel's adherence to security policies and identify areas for improvement. This includes conducting regular security assessments, monitoring compliance with security controls, and soliciting feedback from personnel on their experiences and challenges related to cybersecurity. By monitoring personnel's cybersecurity behaviors and providing constructive feedback, organizations can identify gaps in knowledge or practices and tailor training programs accordingly to address specific needs.

Organizations play a critical role in enhancing personnel's role in cybersecurity by investing in training and education, promoting a culture of security awareness, defining clear roles and responsibilities, fostering cross-functional collaboration, recognizing and incentivizing cybersecurity efforts, and implementing continuous monitoring and feedback mechanisms. By empowering personnel to take an active role in cybersecurity and providing the necessary support and resources, organizations can strengthen their security posture and mitigate cyber risks effectively in today's dynamic threat landscape.

5. Suggestions for future research. Future research could delve deeper into understanding human behavior and its impact on cybersecurity outcomes. This could involve studying factors such as cognitive biases, decision-making processes, and social dynamics within organizations to identify strategies for promoting more secure behaviors among personnel. Additionally, exploring the effectiveness of different approaches to security awareness training and interventions in changing user behavior could provide valuable insights for enhancing cybersecurity practices.

With the increasing adoption of AI and ML in cybersecurity, there is a need for research on developing more advanced AI-driven security solutions. Future research could focus on improving the accuracy and effectiveness of AI-based threat detection and response systems, as well as exploring the potential risks and ethical considerations associated with autonomous cybersecurity decision-making.

As supply chains become more interconnected and globally distributed, there is a growing need to research and develop effective strategies for securing supply chain ecosystems against cyber threats. Future research could explore approaches for assessing and managing cybersecurity risks across supply chains, as well as developing mechanisms for enhancing transparency, accountability, and resilience in supply chain operations.

The proliferation of IoT devices presents new cybersecurity challenges due to their inherent vulnerabilities and diverse deployment scenarios. Future research could focus on developing robust security architectures, protocols, and standards for IoT devices, as well as exploring novel approaches for detecting and mitigating IoT-specific threats such as device tampering, data breaches, and botnet attacks.

With growing concerns about data privacy and regulatory requirements such as GDPR and CCPA, there is a need for research on privacy-preserving technologies and techniques. Future research could explore methods for anonymizing and encrypting sensitive data, enhancing user privacy controls, and ensuring compliance with privacy regulations while maintaining usability and functionality in digital systems.

Research in cyber threat intelligence (CTI) and attribution is essential for understanding the motives, tactics, and origins of cyber-attacks. Future research could focus on developing advanced CTI frameworks, methodologies, and tools for collecting, analyzing, and sharing threat intelligence data across organizations and sectors. Additionally, research on attribution techniques and forensic methodologies could help improve the accuracy and reliability of identifying cyber attackers and attributing cyber incidents to specific threat actors.

As cybersecurity practices and technologies evolve, there is a need to consider the ethical and legal implications of cybersecurity decisions and actions. Future research could explore topics such as cybersecurity ethics, digital rights, liability frameworks, and international legal norms in cyberspace. Additionally, research on the socio-political impacts of cybersecurity policies and regulations could help inform more balanced and equitable approaches to cybersecurity governance.

The field of cybersecurity offers numerous opportunities for future research to address emerging challenges, develop innovative solutions, and advance our understanding of cyber threats and defenses. By focusing on areas such as behavioral analysis, AI and ML, supply chain security, IoT security, privacy-preserving technologies, CTI and attribution, and ethical and legal implications, researchers can contribute to building a safer and more secure digital ecosystem for individuals, organizations, and societies.

Conclusions. The recommendations provided for future research in cybersecurity offer valuable insights into the evolving landscape of cyber threats and defenses. By addressing these research areas, scholars and practitioners can contribute to advancing the field of cybersecurity and enhancing our collective ability to mitigate cyber risks effectively.

Scientific novelty. The suggested research directions highlight novel approaches and methodologies for addressing pressing cybersecurity challenges. From exploring human factors and behavioral analysis to developing AI-driven security solutions and advancing supply chain

security, these research areas offer new avenues for understanding and combating cyber threats in a rapidly evolving digital environment.

Theoretical and practical significance. The proposed research directions have both theoretical and practical significance. By delving into the complexities of human behavior, AI-driven security, and IoT security, researchers can enhance our theoretical understanding of cybersecurity phenomena and develop theoretical frameworks and models that inform practical cybersecurity strategies and interventions. Additionally, research on privacy-preserving technologies, CTI, and attribution addresses practical concerns such as data privacy, threat intelligence sharing, and cyber incident response, which have tangible implications for cybersecurity practitioners and policymakers.

Prospects for future research. The recommendations outlined for future research lay the groundwork for ongoing scientific inquiry and innovation in cybersecurity. Scholars and practitioners have the opportunity to explore these research areas further, develop novel methodologies and technologies, and contribute to the advancement of cybersecurity knowledge and practices. By embracing interdisciplinary collaboration, leveraging emerging technologies, and addressing ethical and legal considerations, future research endeavors in cybersecurity hold the promise of enhancing our collective resilience to cyber threats and safeguarding the integrity and security of digital ecosystems.

The recommendations for future research in cybersecurity underscore the importance of ongoing scientific inquiry and innovation in addressing evolving cyber threats and challenges. By pursuing these research directions, scholars and practitioners can contribute to the advancement of cybersecurity theory and practice, develop innovative solutions to emerging threats, and ultimately, foster a safer and more secure digital world for individuals, organizations, and societies.

1. Скриньковський Р. М., Малашко О. Є. Структурно-класифікаційна характеристика забезпечення інформаційної безпеки. *Інтернаука. Серія: Юридичні науки.* 2020. №7(29). С. 25–32.
2. Малашко О. Є., Скриньковський Р. М. Пріоритетні напрями удосконалення інформаційної безпеки України. *Інтернаука. Серія: Юридичні науки*. 2020. №6(28). С. 13–19.
3. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. №9. С. 100–108. doi: 10.32849/2663-5313/2019.9.17.
4. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, 19.06.2019, № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#n8 (дата звернення 12.04.2024).
5. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави. Київ, Ліра, 2014.
6. Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона», 25.03.2021, № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n2 (дата звернення 12.04.2024).
7. Порядок формування переліку об’єктів критичної інформаційної інфраструктури (Україна), 09.10.2020, № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (дата звернення 12.04.2024).
8. Про інформацію (Україна), 02.10.1992, № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 12.04.2024).
9. Про Національну програму інформатизації, 04.02.1998, № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (дата звернення 12.04.2024).
10. Стратегія розвитку інформаційного суспільства в Україні, 15.03.2013, № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (дата звернення 12.04.2024).
11. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ, НІСД, 2012
12. Гнатюк С. О., Сидоренко В. М., Дуксенко О. П. Сучасні підходи до виявлення та ідентифікації найбільш важливих об’єктів критичної інфраструктури. *Безпека інформації*. 2015. №21(3). С. 269–275. doi: 10.18372/2225-5036.21.9690.
13. Гнатюк С. О., Рябий М. О., Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв’язок.* 2014. №4. С. 3–7.
14. Про основні засади кібербезпеки України, 05.10.2017, № 2163-VIII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 12.04.2024).

References

1. Skrynkovskyy, R. M.,, & O. Ye. Malashko. “Structural and classification characteristics of information security.” *Internauka. Seriia: Yurydychni nauky*, no.7(29), 2020, pp. 25–32..

2. Malashko, O. Ye., Skrynkovskyy R. M. “Priority areas for improving information security in Ukraine.” *Internauka. Seriia: Yurydychni nauky*, no.6(28), 2020, pp. 13–19.
3. Bakalinska, O., and O. Bakalynskyi. “Legal support of cybersecurity in Ukraine.” *Pidpryiemnytstvo, hospodarstvo i pravo*, no.9, 2019, pp. 100–108, doi: 10.32849/2663-5313/2019.9.17.
4. General requirements for cyber security of critical infrastructure, 19.06.2019, No 518. Verkhovna Rada of Ukraine,/zakon.rada.gov.ua/laws/show/518-2019-п#n8. Accessed 12 April. 2024.
5. Tykhomyrov, O. O. *Ensuring information security as a function of the modern state*. Kyiv, Lira , 2014.
6. Military Security Strategy of Ukraine "Military Security - Comprehensive Defense", 25.03.2021, No 121/2021. Verkhovna Rada of Ukraine, zakon.rada.gov.ua/laws/show/121/2021#n2. Accessed 12 April. 2024.
7. The order of formation of the list of objects of critical information infrastructure, 09.10.2020, No 943. Verkhovna Rada of Ukraine, zakon.rada.gov.ua/laws/show/943-2020-п#Text. Accessed 12 April. 2024.
8. About information, 02.10.1992, No 2657- XII. Verkhovna Rada of Ukraine, zakon.rada.gov.ua/laws/show/2657-12#Text. Accessed 12 April. 2024.
9. About the National Informatization Program, 04.02.1998, No 74/98-ВР. Verkhovna Rada of Ukraine,zakon.rada.gov.ua/laws/show/74/98-вр#Text. Accessed 12 April. 2024.
10. Information society development strategy in Ukraine, 15.03.2013, No 386-р. Verkhovna Rada of Ukraine, zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text. Accessed 12 April. 2024.
11. Biriukov, D. S., and S. I. Kondratov. *Critical infrastructure protection: problems and prospects of implementation in Ukraine*. *Kyiv, NISD*, 2012.
12. Hnatiuk, S. O., Sydorenko, V. M., and O. P. Duksenko. “Modern approaches to critical infrastructure objects detection and identification.” *Bezpeka informatsii*, no.21(3), 2015, pp. 269–275, doi: 10.18372/2225-5036.21.9690.
13. Hnatiuk, S. O., Riabyi, M. O., and V. M. Liadovska. “Critical Information Infrastructure Definition and Protection - Approach Analysis.” *Zv’iazok*, no.4, 2014, pp. 3–7.
14. On the basic principles of cybersecurity of Ukraine, 05.10.2017, No 2163-VIII. Verkhovna Rada of Ukraine, zakon.rada.gov.ua/laws/show/2163-19#Text. Accessed 12 April. 2024.

УДК 351:338.4
doi: https://doi.org/10.15330/apred.2.20.112-119

Щур Р. І.[1], Ткачук Д. Ю.[2]

ПУБЛІЧНЕ УПРАВЛІННЯ РОЗВИТКОМ МАШИНОБУДІВНОГО КОМПЛЕКСУ УКРАЇНИ В УМОВАХ ЕКОНОМІЧНОЇ НЕСТАБІЛЬНОСТІ

[1]Прикарпатський національний університет імені Василя Стефаника,
Міністерство освіти і науки України,
кафедра фінансів,
вул. Шевченка, 57, м. Івано-Франківськ,
76018, Україна,
тел.: 0342752351,
e-mail: roman.shchur@pnu.edu.ua,
ORCID: https://orcid.org/0000-0001-9945-3939

[2]Прикарпатський національний університет імені Василя Стефаника,
Міністерство освіти і науки України,
кафедра публічного управління та адміністрування,
вул. Шевченка, 57, м. Івано-Франківськ,
76018, Україна,
тел.: 0342752351,
e-mail: denys.tkachuk.19@pnu.edu.ua,
ORCID: https://orcid.org/0000-0001-8803-3218

Анотація. В статті доведено, що машинобудівний комплекс є, був і залишається базовим сегментом національної економіки та промисловості, зокрема тому, що він має достатній