Machinery & Energetics
Vol. 15, No. 2. 2024

Journal homepage:
https://technicalscience.com.ua/en

UDC 004.056:355/359
DOI: 10.31548/machinery/2.2024.118

Oleh Semenenko*
Doctor of Military Sciences, Professor
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Air Force Ave., Kyiv, Ukraine
https://orcid.org/0000-0001-6477-3414

Serhii Kirsanov
Doctor of Technical Sciences, Senior Researcher
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Air Force Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-9696-0369

Artur Movchan
PhD in Technical Sciences
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Air Force Ave., Kyiv, Ukraine
https://orcid.org/0009-0006-0559-4962

Mykola Ihnatiev
PhD in Technical Sciences
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Air Force Ave., Kyiv, Ukraine
https://orcid.org/0009-0007-8797-3364

Uzef Dobrovolskyi
PhD in Technical Sciences, Associate Professor
National Aviation University
03058, 1 Liubomyr Huzar Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-1077-1402

Impact of computer-integrated technologies on cybersecurity in the defence sector

Abstract. The research relevance is determined by the ever-increasing threat of cyberattacks and the need to protect defence systems from these threats through the introduction of integrated computer technologies. The study aims to develop strategies for ensuring digital security in the defence sector, addressing the impact of information technology. The study analyses the impact of integrated computer technologies on information security in the military sphere, develops cybersecurity strategies and analyses examples of their application in the defence sector. The study determined that integrated computer technologies are substantial in improving cybersecurity in the defence sector. The analysis showed that they can effectively detect, analyse and respond to cyber threats, ensuring reliable protection of critical information resources. In addition, the digital security strategies developed addressed the specifics of the defence sector, helping to improve protection against cyberattacks and ensuring immediate action in the event of a threat. The resulting strategies for

Article's History: Received: 12.02.2024; Revised: 06.05.2024; Accepted: 29.05.2024.

Suggested Citation:
Semenenko, O., Kirsanov, S., Movchan, A., Ihnatiev, M., & Dobrovolskyi, U. (2024). Impact of computer-integrated technologies on cybersecurity in the defence sector. *Machinery & Energetics,* 15(2), 118-129. doi: 10.31548/machinery/2.2024.118.

*Corresponding author

improving the digital security of the defence sector consider the specifics of the industry, contributing to increased resilience against cyber threats and ensuring prompt action in the event of potential attacks. The most significant examples of the introduction of these technologies, namely data mining, big data, distributed blockchain technology, analytical methods of cyber-analysis and cyber-physical systems, have demonstrated their effectiveness in real-world conditions, contributing to the security and resilience of defence systems. The results show the importance of information technology in improving cybersecurity in the defence sector. This confirms the need for systematic implementation of such technologies to ensure effective protection against modern cyber threats

Keywords: information systems; digital defence; military complex; use of innovations; electronic threats

INTRODUCTION

Identification and elimination of digital security problems is an urgent task, as military information systems are subject to constant cyber threats. There is a gap in the development of digital security strategies in the defence sector, as well as in the understanding of the challenges associated with this area. The lack of proper digital security can have serious consequences for military systems and national security in general. To understand the study, it is important to get acquainted with the general theoretical aspects of digital security in the context of the defence sector. This includes an understanding of the basic principles of cyber security, covering a wide range of measures to prevent unauthorised access, destruction or modification of data, and to ensure the confidentiality and integrity of information. Analysing typical threats and vulnerabilities of information systems is key to identifying potential risks and developing effective protection measures. In addition, the study of modern approaches to the cybersecurity of military facilities allows to identify the most effective and innovative methods and technologies that can be used to ensure security in this area.

For a more detailed analysis of the current state of cybersecurity in the context of the defence sector, it is necessary to consider other studies in this area. For instance, the study of I.L. Humeniuk (2023) showed the positive impact of information technology on the Ukrainian economy, in particular, the growth of labour productivity, optimisation of business processes and improvement of the quality of services, and identified potential challenges related to employment, competitiveness of industries and cybersecurity. M. Rakushev *et al*. (2022) identified the main capabilities and shortcomings of the Terminal information and telecommunication system for the intelligence needs of the Kyiv Defence Forces and proposed recommendations for its further improvement. In turn, A. Munko (2023) determined the place of cybersecurity in the financial security policy of Ukraine, addressing the importance of a strategic approach and the development of a sectoral cybersecurity strategy, and proposed measures to counter cyber threats in this context.

S. Toliupa & L. Slipachuk (2023) revealed the composition and structure of measures and tools that are part of the system of protection of industrial integrated information management systems in the cybersecurity sector, as well as providing a detailed description of the various resources and tools included in this system. In addition, a study by J.H. Eom *et al*. (2023) determine that the key to creating an intelligent intelligence unit, which is being developed by advanced military countries, is to strengthen the security of the information system and real-time network using the latest technologies, such as artificial intelligence (AI) and big data (BD). Study results by F. Ahmed *et al*. (2023) highlight the interaction between cybersecurity and cyber defence with a focus on the development of the concept of cyber resilience.

D. Galinec (2023) demonstrated how cybersecurity and cyber defence contribute to cyber resilience using a new model developed by the author. Moreover, C.O. Qader & D.Z. Ablahd (2023) reflected on the current state of cybersecurity of computer systems, including the main threats and measures aimed at reducing these risks. According to S. Mishra (2023), the AI-based cybersecurity method improves the performance of cybersecurity systems by enhancing their defence capabilities, which is manifested in improved data protection, scalability, risk mitigation, information security and attack avoidance. Similarly, W.K. Too & M. Mutuku (2023) gained a deeper understanding of the state of cybersecurity implementation and identified problems and strategies to improve this process. The findings of the study can influence policy and decision-making, guiding future investments in cybersecurity and related technologies.

It is worth noting that the scientific contributions of these studies can help to form a more complete understanding of the current state of cybersecurity, especially in the context of the defence sector and other areas of life. The authors covered various aspects of cybersecurity, but some aspects remain insufficiently covered. For instance, these studies focus on describing information system security measures but do not consider their impact on military facilities. It is also worth analysing the possibilities of applying cybersecurity principles in the defence sector to ensure information security and protection against cyber threats. In general, this study focuses on the identification of optimal strategies for ensuring information security in the defence sector, including the impact of modern information technologies. The study aims to examine the current state of digital technologies in the military sphere, as well as to identify the main challenges and threats arising from digital security in the defence sector.

MATERIALS AND METHODS

To achieve the objective of the study, an overview of the impact of integrated computing technologies on defence cybersecurity was conducted, focusing on their role and potential for strengthening digital security in the sector. The next phase of the study was to develop strategies to ensure digital security in the industry. Given the specifics of this area, the strategies developed were aimed at protecting against cyberattacks, ensuring data confidentiality and implementing other measures of great importance to the security of the state. In addition, a review of best practice examples in this area was conducted, which meant analysing successful initiatives and programmes that have already been implemented in the defence sector in different countries. As such, effective methods that could be used to develop new strategies to ensure digital security were identified.

The study analysed how these strategies can be applied, including their effectiveness and suitability for addressing specific challenges and threats in the defence context. Various technologies used in the defence sector to improve cybersecurity were studied. These technologies include intelligent threat monitoring and detection systems, data encryption systems, innovative approaches to protecting critical infrastructures from cyberattacks, as well as cyber-analytical and cyber-physical systems, blockchain technologies, BD and AI. This stage of the study included an analysis of the use of AI and machine learning in the defence sector cybersecurity. These advanced technologies are used to detect new threats, review large amounts of data and respond to cyberattacks in real-time. The effectiveness of blockchain technologies in the field of cybersecurity, which can be used to create reliable and unbreakable data storage systems was determined, which may be especially important for the defence sector, where confidential and critical information is stored.

Thus, the consideration of the introduction of technologies in the cybersecurity of the defence sector covered a wide range of innovative solutions aimed at improving digital security and protecting important information resources. Additionally, diagrams of complex data protection systems and cybersecurity strategies that reflected the structure and functionality of the various components of these systems were developed. Each scheme has been designed to meet the specific requirements and challenges faced by the defence sector. To develop the schemes, modelling methods were used that involved abstracting the essential aspects of data protection systems and using various cybersecurity components. The functions of each component, their interaction and their impact on the overall effectiveness of the system were addressed to better assess the level of protection and identify weaknesses.

The key problems and challenges faced by modern security systems were also identified, which allowed to identify priority areas for further research in this area. The results obtained were systematised and summarised, which were used to formulate the main conclusions based on the data obtained and provide the necessary recommendations.

RESULTS

In the digital environment, where information technology plays a crucial role in defence, digital security is becoming an extremely important task for ensuring national security and defence capability. Information technology, including computerised systems, communication networks, software and electronic databases, enables the exchange of information, the management of military operations and the storage of sensitive data. However, this environment also poses new challenges and threats to cybersecurity, including cyberattacks, espionage, sabotage and terrorist activities. Therefore, the development of effective strategies to ensure cybersecurity in the defence sector, considering the impact of information technology, is an extremely urgent and important task.

The first strategy is to develop and implement robust data protection systems (Fig. 1). This strategy envisages the creation of modern data protection systems in the defence sector. It includes the development of software that provides data encryption, network monitoring, intrusion detection and protection against cyberattacks. Implementing robust data protection systems protects confidential information from unauthorised access, preserves data integrity and ensures that information is available to the appropriate users. In addition, this strategy also provides for regular updates and audits of data protection systems to identify and eliminate vulnerabilities.

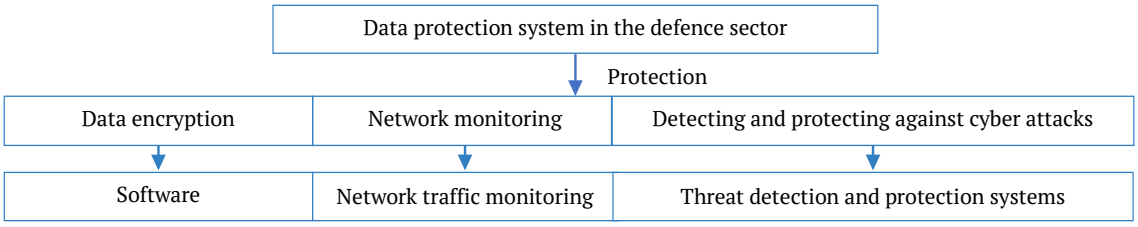

Figure 1. Developing and implementing robust data protection systems
Source: compiled by the authors

This diagram shows that the defence data protection system includes various components, such as data encryption, network monitoring, and detection and protection against cyberattacks. Each of these components

performs its function to ensure the security and integrity of important information. Moreover, it is worth giving an example of how to apply the strategy. For example, a government defence organisation may develop and deploy specialised software to encrypt sensitive information, control access to systems, and detect anomalous activity on the network. Such systems can prevent unauthorised access to sensitive military data and ensure the security and integrity of information.

The second strategy is to ensure cyber hygiene (Fig. 2). It involves the implementation and support of initiatives aimed at enhancing the cybersecurity culture among defence personnel and users. This strategy is aimed at training staff in the correct practices of using computer systems, implementing data security policies and raising awareness of potential cyber threats. It is possible to note that cyber hygiene includes not only technical security measures but also the awareness and responsibility of each user for the security of information. Enhanced cyber hygiene can avoid many threats, such as phishing, social engineering and other forms of attacks that use social engineering techniques to gain access to a system.

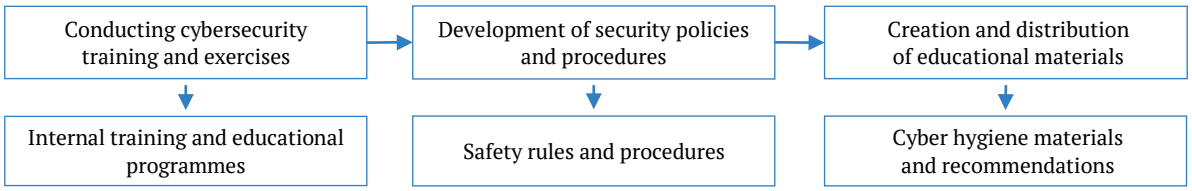

Figure 2. Ensuring cyber hygiene

Source: compiled by the authors

This flowchart presents the main steps of this strategy, including conducting cybersecurity training and exercises, developing security policies and procedures, and creating and distributing educational materials. For instance, a governmental organisation can provide regular cybersecurity training for its staff, make cyber hygiene materials and resources available, and implement policies and procedures to protect sensitive information. Such measures can help staff avoid situations where their actions could be vulnerable to cyberattacks.

Another strategy is the development and implementation of cyber security strategies and policies, which involves the development and implementation of comprehensive defence sector practices and policies to ensure digital security (Fig. 3). This strategy aims to establish principles governing cybersecurity in the defence sector and identify specific measures for their implementation. The analysis of this strategy indicates that the creation of digital security methods and policies is a key element of effective cybersecurity management in the military sphere. They define strategic goals and priorities and are developed with the unique needs and challenges of the defence sector in mind. In addition, they unify approaches to cybersecurity, create standards and procedures, and promote coordination between different governance structures and agencies.

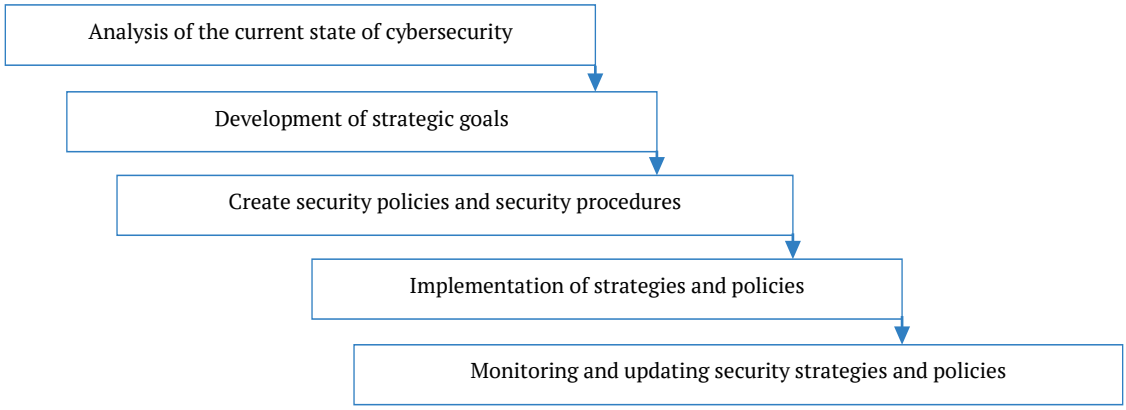

Figure 3. Developing and implementing cyber strategies and security policies

Source: compiled by the authors

The resulting scheme reflects the sequential process of implementing this strategy in the defence sector. An example of the application of this strategy could include the development of a national cyber strategy for the defence sector, which defines strategic goals and priorities in the field of cyber security and establishes a framework and standards for its implementation. Additionally, this strategy may include the creation of internal security policies and procedures to protect confidential information, critical systems and infrastructure from cyber threats. In addition,

it should include a strategy to improve the ability to detect and respond to cyberattacks (Fig. 4). It aims to improve the ability of defence institutions to detect and respond effectively to cyberattacks. This strategy envisages a comprehensive approach to cybersecurity management, including analysis of existing detection and response systems, their enhancement, testing and continuous improvement. The main steps in the implementation of this strategy are to analyse the current systems for detecting and responding to cyberattacks in the defence sector, improve existing systems and introduce new technologies to more effectively detect and respond to threats.

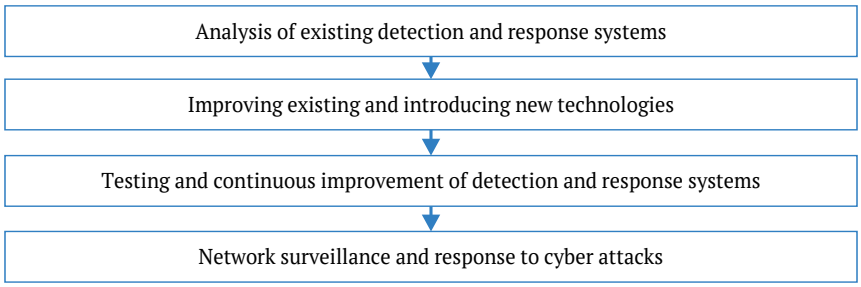

Figure 4. Improving the ability to detect and respond to cyber attacks
Source: compiled by the authors

This flowchart illustrates the sequence of actions that are included in a strategy to improve the ability to detect and respond to cyberattacks. In terms of the practical application of this strategy, a government defence organisation could develop and implement a new cyberattack detection system based on AI and BD analysis. This system automatically detects anomalous activity on the network and quickly alerts potential threats. When a cyberattack is detected, the system will automatically launch procedures to isolate and neutralise the threat, allowing the organisation to respond quickly and effectively to cyberattacks, ensuring the security and integrity of information.

Attention should also be devoted to the strategy of creating cyber defence teams and competence centres (Fig. 5). It envisages the creation of specialised groups and expert centres dealing with cyber defence. This strategy aims to increase the effectiveness of the response to cyber threats by analysing, identifying and eliminating potential threats to information security in depth. Establishing cyber defence teams and competence centres involves several steps. Firstly, it is necessary to identify the needs and staffing requirements for cyber defence. Then, specialised cybersecurity personnel are recruited and trained. After that, teams and centres are formed to ensure continuous monitoring and protection of defence information systems.

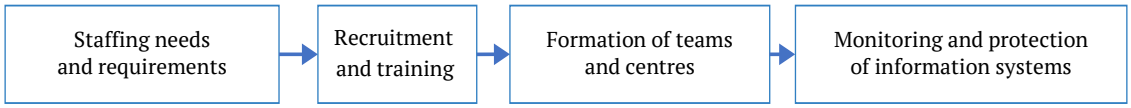

Figure 5. Establishment of cyber defence teams and competence centres
Source: compiled by the authors

This flowchart shows the sequence of steps to implement this defence strategy. It starts with identifying needs and staffing requirements, then includes recruiting and training specialised staff, forming teams and centres, and ends with monitoring and protecting information systems. An example of this strategy could include the creation of cyber defence centres that specialise in detecting and responding to cyberattacks in the military sphere. These centres may be responsible for network monitoring, analysing security incidents and developing data protection strategies. For instance, a government defence organisation may establish a cyber defence centre to protect critical military information resources and infrastructure from cyber threats.

Equally important is the strategy of conducting regular security audits and penetration testing, which is an important component of the defence cyber defence system (Fig. 6). This strategy involves periodic assessments of vulnerabilities in information systems and infrastructure to identify potential risks and security gaps. A security audit is a systematic review, testing and analysis of information systems and processes to identify weaknesses and potential security threats. This process includes reviewing security policies, applying access control measures, assessing network security, analysing system configurations and identifying potential vulnerabilities. Penetration testing is a method of systematically testing the security of information systems by attempting to penetrate or intrude into them. This process simulates the actions of a potential attacker and identifies weaknesses in security systems that can be used for unauthorised access or attack.

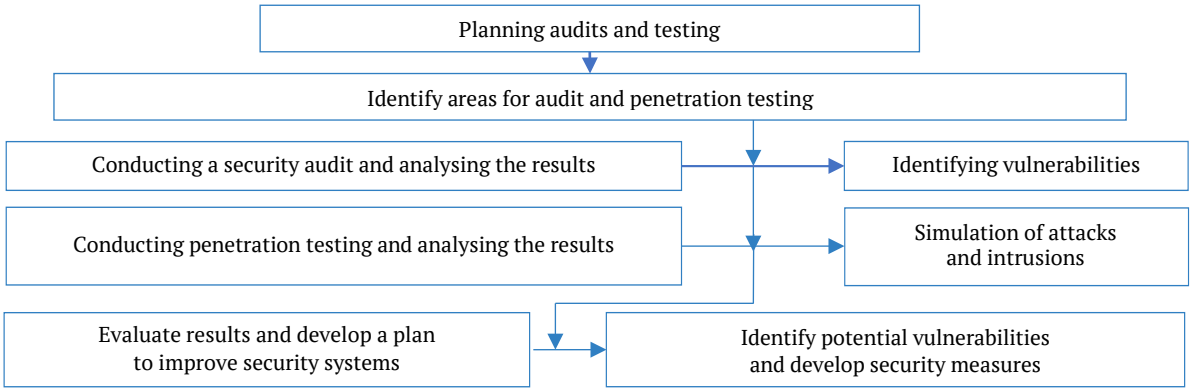

Figure 6. Conducting regular security audits and penetration testing
Source: compiled by the authors

This diagram shows the sequence of steps involved in conducting regular security audits and penetration testing. Each block represents a separate stage of the process, from planning to evaluating the results and developing protective measures. Thus, this strategy can be implemented, for example, in a government defence organisation that can regularly conduct security audits of its information systems and networks, as well as penetration testing using expert teams or external partners. This identifies potential security threats, risks, and takes timely measures to prevent or eliminate them.

The strategy of introducing strict access rules and restrictions at the user level involves the establishment of integrated access control systems and the development of security policies that regulate user access to information resources in the defence sector (Fig. 7). This strategy is aimed at reducing the risk of confidential information leakage and ensuring compliance with regulatory and legal requirements in the field of cybersecurity. Strict access rules imply that users' access rights to confidential information and critical infrastructure resources are limited to the minimum necessary, depending on their role and functional responsibilities. This may include restricting access rights through roles and privileges, two-factor authentication, access control lists, and system access auditing mechanisms.

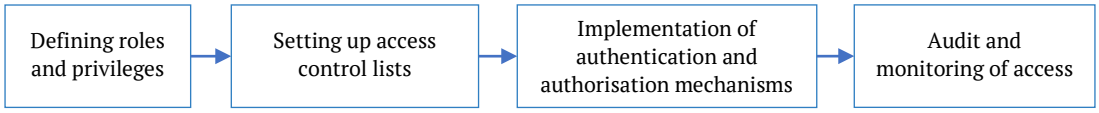

Figure 7. Introduce strict access rules and restrictions at the user level
Source: compiled by the authors

This flowchart shows the sequence of actions when implementing strict access rules and restrictions at the user level. As an example of the use of the strategy, a government defence organisation can implement this strategy by establishing a system of roles and privileges for users depending on their position and functional responsibilities. For example, high-level employees may be granted enhanced access rights to confidential information, while low-level employees may be granted limited access rights. This strategy reduces the possibility of internal threats and provides greater control over access to important information. Moreover, the strategy of cooperation with the private sector and international partners should be noted (Fig. 8). It involves partnerships with companies, organisations and other countries to share information, technologies and best practices in the field of cybersecurity. This strategy aims to increase the level of cyber defence capability by combining the efforts and resources of various actors. Cooperation with the private sector may include partnerships with information technology companies to create and implement new data protection systems, develop software to detect cyber threats, and other initiatives. It is also possible to jointly conduct training and training programmes to improve the skills of cybersecurity specialists.

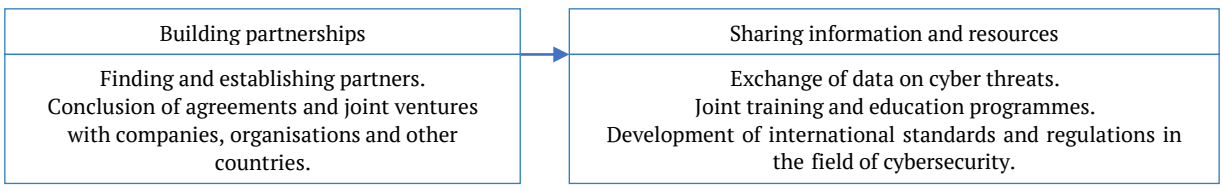

Figure 8. Cooperation with the private sector and international partners
Source: compiled by the authors

This diagram illustrates the main steps included in the strategy for cooperation with the private sector and international partners in the field of cybersecurity. Internationally, the strategy envisages information exchange and cooperation with other countries in the field of cybersecurity. This could include sharing data on cyber threats, joint exercises and training programmes, and the development of international standards and regulations in this area. For example, the government can cooperate with leading technology companies to create innovative data protection systems. In addition, cooperation agreements can be concluded with other countries to share information on cyber threats and respond to them jointly through joint operations centres. It is worth noting that these strategies complement each other and form a comprehensive approach to cyber defence. These include developing technological defences, promoting a culture of cybersecurity among staff, collaborating with the private sector and international partners, and conducting security audits and penetration testing (Piera *et al*., 2016). These strategies are aimed at preventing cyberattacks, identifying potential threats and responding effectively to them, thus ensuring the security and integrity of information in the defence sector. Implementation of strategies requires constant updating and adaptation to the rapidly changing cyber threat environment, but at the same time, it opens new opportunities to improve cybersecurity and protect critical information resources (Metelskyi & Kravchuk, 2023).

In general, integrated computer technologies are a complex combination of different information systems that interact with each other to achieve a common goal. In the defence sector, these technologies play a key role in ensuring the efficiency, reliability and security of military operations. Their role is to improve the armed forces, provide communications infrastructure, increase the accuracy and speed of response to threats, as well as to enhance defence capabilities and reduce the risk of cyberattacks. With the advent of the latest integrated computer technologies in the defence sector, new challenges for cybersecurity have emerged. Technological developments, such as the Internet of Things, cloud services and AI, provide the military with new opportunities but also increase their vulnerability to cyberattacks (Savytska *et al*., 2024). Analysing technological trends allows to understand which specific aspects of cybersecurity require the most attention and protection measures. A variety of innovative solutions are widely used to implement computer-integrated technologies in defence cybersecurity. For example, the use of AI to analyse data sets detects anomalous activity and potential cyber threats. Systems that use machine learning to analyse network traffic can detect and respond to malicious activity promptly (Pidpalyi, 2024). The large amounts of data generated in the defence sector can be used to identify patterns and predict cyber threats. BD analytics systems identify unusual connections and unusual events that may indicate cyberattacks. In addition, the use of blockchain in cybersecurity can help ensure that data is not available for unauthorised access and ensure the integrity of information. For example, using blockchain technology to create a distributed system for logging network activity can provide a reliable history of events, making it easier to detect attacks (Smutchak *et al*., 2023).

It is also important to use analytical methods and technologies to identify and analyse cyber threats. Various algorithms and software tools identify and classify threats based on their characteristics and properties. And the integration of computer systems with physical processes to detect and respond to cyber threats in real-time. For example, cyber-physical security systems can monitor the operation of physical facilities, such as power plants or heavy machinery, and automatically respond to attacks. These technologies can be successfully used in the defence sector to ensure cybersecurity and protect critical information resources. However, it is important to consider their advantages and disadvantages when choosing and implementing them (Table 1).

Table 1. Comparison of technologies in defence cyber security

Technology	Advantages	Limitations
Artificial Intellect	High speed of response to threats	Requires large amounts of data
BD	Ability to detect complex patterns	High demands on computing resources
Blockchain technologies	High reliability and data integrity	Limited scalability
Cyber analytics	Effective threat detection and classification	Requires constant updating of models
Cyber-physical systems	Real-time response to threats	Requires integration with physical systems

Source: compiled by the authors

A general analysis of the table shows that each technology has its unique advantages and disadvantages. AI and BD analysis enable fast and efficient detection of cyber threats but require significant computing resources. Blockchain technologies and cyber-physical systems provide reliability and real-time response but may be limited in scalability and integration. Cyber analytics provides an effective way of classifying threats but needs to be constantly updated. When choosing technologies to be implemented in the defence sector, their characteristics and the needs of a particular application should be addressed.

In the context of cybersecurity in the defence sector, there is a need to introduce computer-integrated technologies to protect critical information resources and effectively counter cyber threats. A variety of innovative solutions can be used to improve the level of protection and response to potential threats. Recommendations for ensuring digital security in the defence sector, considering the impact of information technology, are based on a comprehensive approach to cybersecurity. First, a detailed analysis of the impact of integrated computer technologies on defence cybersecurity should be conducted. This will identify

potential threats and determine the most effective ways to protect yourself. After that, it is necessary to develop strategies for digital security that meet the requirements and characteristics of the defence sector and address the impact of information technology. These strategies can include regular security audits, penetration testing, strict access rules and user-level restrictions, and collaboration with the private sector and international partners.

It is also important to consider the introduction of computer-integrated technologies in the cybersecurity of the defence sector. Technologies such as AI, BD, blockchain, cyber analytics and cyber-physical systems can be successfully used to ensure cybersecurity and protect critical information resources in the defence sector. For instance, the introduction of machine learning and AI systems to detect anomalous activity in networks helps to quickly identify and respond to potential threats. The use of blockchain technologies to create decentralised and non-destructive data storage systems can provide a high level of protection against cyberattacks and malicious interference. These examples demonstrate how information technology can be effectively used to strengthen cybersecurity in the defence sector.

DISCUSSION

This study analysed the impact of computer technology on cybersecurity, by examining integrated monitoring systems, data encryption systems and innovative approaches. The findings confirmed the importance of a comprehensive approach to cyberspace protection and the need to develop cyber analytics systems for effective network defence. These findings are also noted by J.M. Couretas (2022). Moreover, the results of the study pointed to the growth of security problems due to the introduction of new technologies and the need for new defence measures, which also coincides with the findings of Y. Zheng *et al*. (2021). The results of the study of R.M. Rajendran & B. Vyas (2023) emphasised the complexity of cyber threats and stressed the need to further improve security systems to effectively counter cybercriminals. Thus, this study has revealed that integrated monitoring systems and data encryption systems play a key role in improving cybersecurity in the defence sector. The results confirmed that the development of innovative approaches is necessary for the effective protection of the network and information resources.

Additionally, this paper confirmed the importance of using AI in cybersecurity and noted that it contributes to the effectiveness of computer system protection, as noted by B.S. Guru Prasad *et al*. (2023). What makes this study different is the detailed analysis of various strategies and technologies, including both passive and active defences, that can be used to ensure cybersecurity. This work focused on developing strategies and considering technologies for defence in the digital environment, in the context of the defence sector, rather than reviewing aspects of cyber-physical systems, as was done by T. Liu *et al*. (2019). Compared to the above study, this work has identified additional advantages in the use of AI in ensuring high resistance to complex cyberattacks and reducing vulnerability to smart threats. Thus, this paper has highlighted the importance of using AI in cybersecurity, confirming that it contributes to the efficiency of computer system protection.

This study has expanded the understanding of comprehensive cybersecurity in the defence sector, focusing on the implementation of robust data protection systems. It is possible to state that this study complemented the results of S.B. Rahayu *et al*. (2023), which emphasised the importance of comprehensive cybersecurity education among employees in the defence and security sectors, as it discussed in detail strategies for ensuring cybersecurity. This work focused on general cybersecurity technologies, not limited to aspects related to quantum computing or cyber-physical protection methods developed by M. Barbeau & J. Garcia-Alfaro (2022). Compared to the aforementioned study, this paper focuses on the development and implementation of general cybersecurity strategies, including improving methods of detecting and responding to cyberattacks, protecting against real-time threats, and ensuring data integrity. Additionally, this study complemented the work of M. Kaur (2022), which focused on the importance of cybersecurity and data protection in the information environment, as both works focused on improving security measures in the digital space. Moreover, the results obtained highlighted the importance of using comprehensive strategies in ensuring the information security of systems, as also noted in the study by U.K. Singh *et al*. (2022). However, this work has expanded this understanding by presenting concrete ways to protect computer systems and networks from cyber threats. This study identified common approaches to cybersecurity, including both passive and active defence strategies, which was also done by B. Latha *et al*. (2024), where an intrusion detection system was developed. In other words, the results of this study pointed to the importance of improving intrusion detection systems for computer systems and networks. To this end, effective methods have been developed to integrate these systems into existing infrastructures, which helps to increase the level of security and protection against cyber threats.

While this study pointed to the importance of a comprehensive approach to cybersecurity in the defence sector, J. Kallberg (2022) highlighted the strategic inefficiency of redistributing military capabilities to combat civilian cyber threats. Additionally, the study questioned the effectiveness of the integrated intelligence approach in the defence sector and suggested alternative strategies, while the study by K. Veni *et al*. (2024) emphasised the use of this approach to improve intrusion detection and classification capabilities for digital-double industrial cyber-physical systems. Finally, this study examined the specific challenges and opportunities associated with the impact of computer-integrated technologies on cybersecurity in the defence sector, which is an important aspect of global security and defence, and H. Singh *et al*. (2023) focused on the relevance of cybersecurity in the data technology industry. Thus, they demonstrated that a comprehensive approach

to cybersecurity in defence is extremely important, especially given the risks associated with civilian cyber threats.

The study determined that the introduction of computer-integrated technologies in the cybersecurity of the defence sector involves not only the use of the latest methods but also requires active improvement of existing protection systems. The development of cyber defence requires not only technological solutions but also consideration of the human factor and organisational aspects (Smailov *et al*., 2023). This study highlighted cybersecurity issues and the need to improve critical infrastructure protection measures, as in the study by I. Cesarec (2020). However, the aforementioned paper focused on analysing the general state of cybersecurity and identifying threats in general, while this paper addresses the protection of critical infrastructure, which plays an important role in the defence and security sector. The use of machine learning to ensure the security of computers and information in the digital environment was also emphasised, as noted by B.B. Gupta & Q.Z. Sheng (2018). Overall, the study found that computer-integrated technologies have a significant impact on cybersecurity in the defence sector. However, in comparison to the above-mentioned studies, this work focused on the impact of technology on cybersecurity in the military structure and considered a wider range of cybersecurity aspects.

It is worth noting that the study provided some defence-specific protection strategies, while C.F. Azubuike (2023) demonstrated the results of the motivation of state cyberattacks and the need to develop international norms and standards for cybersecurity. This study did not identify the role of cyberspace in special operations, unlike D. Trifunovic & Z. Bjelica (2018), as this study concluded on the technical aspects of cyber defence and the impact of technology on the defence sector. The study also provided a broad overview of cybersecurity technologies specific to the sector under consideration, and the study by S. Lee & S. Kim (2021) demonstrated the introduction of blockchain technologies into national cybersecurity systems. Thus, the study results included the use of specific protection measures aimed at ensuring cybersecurity in the defence sector. Emphasising the importance of a comprehensive approach, specific recommendations were made on the use of technologies and strategies for the effective protection of information resources.

Finally, this study has identified certain challenges in creating and implementing modern cyber defence strategies. While O.A. Guidetti *et al*. (2023) identified general cyber defence strategies, this study focused on adapting these strategies to the specific needs of the defence sector, considering its unique challenges and requirements. In addition, as the study by C. Shi *et al*. (2024), this paper presents strategies and technologies for active and passive network protection. However, the technologies and strategies themselves differ across studies. This paper added important details to the understanding of current cyber defence strategies, focusing on specific challenges and recommendations for the defence sector. Certain aspects of digital defence have been identified that can be used to develop effective network defence methods in the context of military structures.

Based on a comparative analysis with other studies in the field of cybersecurity in the defence sector, several conclusions can be drawn. The study analysed the impact of computer-integrated technologies on cybersecurity in the defence sector, focusing on specific aspects of technology application in this area. Addressing the results of other studies, it is possible to emphasise the importance of a comprehensive approach to cybersecurity, covering current challenges and opportunities of technology. This confirms the need to develop new strategies and technologies to protect against cyber threats in the military sector.

CONCLUSIONS

The study analysed the impact of integrated computer technologies on information security in the military sphere, created cybersecurity strategies and analysed examples of the use of these strategies in the defence sector. The study determined that integrated computer technologies are substantial in improving cybersecurity in the defence sector. The analysis showed that they can effectively detect, analyse and respond to cyber threats, ensuring reliable protection of critical information resources. In addition, the digital security strategies developed addressed the specifics of the defence sector, helping to improve protection against cyberattacks and ensuring immediate action in the event of a threat. The resulting strategies for improving the digital security of the defence sector consider the specifics of the industry, contributing to increased resilience against cyber threats and ensuring prompt action in the event of potential attacks.

The most significant examples of the introduction of these technologies, namely data mining, BD, distributed blockchain technology, cyber analytics and cyber-physical systems, have demonstrated their effectiveness in improving the security and resilience of defence systems. The results show the importance of information technology in improving cybersecurity in the defence sector. This confirms the need for systematic implementation of such technologies to ensure effective protection against modern cyber threats. It should be noted that the study was limited by the availability of certain data and resources, which may affect the completeness of the analysis. The rapid pace of technology development in the cybersecurity industry may make some results outdated within a short time after the study is completed. In addition, disadvantages may include the limited scope of the models or algorithms used, which may affect the accuracy of the results obtained.

Given the results of the study, it is worth recommending further improvement of integrated computer technologies in the field of cybersecurity in the defence sector. To do this, it is necessary to actively introduce new methods of data analysis, and the use of AI and machine learning technologies to detect and counter cyber

threats. One area for further research could be the development of other cybersecurity methods specifically tailored to the needs of the defence sector. In addition, it is recommended to improve cooperation between the military and civilian sectors in the field of cybersecurity. To this end, joint research centres should be established where specialists from both sectors can work together to solve problems and develop innovative methods of protecting against cyber threats. It is also necessary to establish mechanisms for information exchange between military and civilian scientists so that they can interact and learn from each other's best practices and experiences. The development of joint research projects and funding programmes can help bring these sectors closer together and jointly address cybersecurity issues. Thus, further research in this area can help improve cybersecurity in the defence sector and ensure effective protection against modern cyber threats.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Ahmed, F., Hasan Molla, A., Uddin, R., & Chowdhury, R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. *International Journal for Multidisciplinary Research*, 5(6), article number 230610726.

[2] Azubuike, C.F. (2023). Cyber security and international conflicts: An analysis of state-sponsored cyber attacks. *Computer Security*, 9(1), 101-114.

[3] Barbeau, M., & Garcia-Alfaro, J. (2022). Cyber-physical defense in the quantum era. *International Security and Arms Control*, 12, article number 1905. doi: 10.1038/s41598-022-05690-1.

[4] Cesarec, I. (2020). Beyond physical threats: Cyber-attacks on critical infrastructure as a challenge of changing security environment – Overview of cyber-security legislation and implementation in SEE countries. *Annals of Disaster Risk Sciences*, 3(1). doi: 10.51381/adrs.v3i1.45.

[5] Couretas, J.M. (2022). Cyber security and defense for analysis and targeting. In *An Introduction to Cyber Analysis and Targeting* (pp. 119-150). Cham: Springer. doi: 10.1007/978-3-030-88559-5_6.

[6] Eom, J.H., Yoon, D.W., & Choo, J.H. (2023). Design of an integrated cyber defense platform for communication network security of intelligent smart units. In *Computational Science and Its Applications* (pp. 218-230). Cham: Springer. doi: 10.1007/978-3-031-37111-0_16.

[7] Galinec, D. (2023). Cyber security and cyber defense: Challenges and building of cyber resilience conceptual model. *International Journal of Applied Sciences & Development*, 1, 83-88. doi: 10.37394/232029.2022.1.10.

[8] Guidetti, O.A., Speelman, C., & Bouhlas, P. (2023). A review of cyber vigilance tasks for network defense. *Frontiers in Neuroergonomics*, 4, article number 1104873. doi: 10.3389/fnrgo.2023.1104873.

[9] Gupta, B.B., & Sheng, Q.Z. (2018). *Machine learning for computer and cyber security: Principle, algorithms, and practices*. London: CRC Press.

[10] Guru Prasad, B.S., Kiran, G.M., & Dinesha, H.A. (2023). AI-driven cyber security: Security intelligence modelling. *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(6), 961-965. doi: 10.54660/.IJMRGE.2023.4.6.961-965.

[11] Humeniuk, I.L. (2023). The impact of information technology on the economy. *Inclusion and Society*, 2, 5-9. doi: 10.32782/2787-5137-2023-2-1.

[12] Kallberg, J. (2022). *Demilitarize civilian cyber defense, and you'll gain deterrence*. Retrieved from https://www.defensenews.com/opinion/commentary/2022/02/09/demilitarize-civilian-cyber-defense-and-youll-gain-deterrence/.

[13] Kaur, M. (2022). Cyber security challenges in the latest technology. In *Proceedings of Third International Conference on Communication, Computing and Electronics Systems* (pp. 655-671). Singapore: Springer. doi: 10.1007/978-981-16-8862-1_43.

[14] Latha, B., Kalyan, Y.M., Kancheti, D., Siddi, P.K., Prabhunadh Kancheti, D., & Vellela, S.S. (2024). A proactive defense mechanism against cyber threats using next-generation intrusion detection system. *Intrusion Detection System*, 10(2), 110-116. doi: 10.46501/IJMTST1002015.

[15] Lee, S., & Kim, S. (2021). Blockchain as a cyber defense: Opportunities, applications, and challenges. *IEEE Access*, 10, 2602-2618. doi: 10.1109/ACCESS.2021.3136328.

[16] Liu, T., Tian, J., Wang, J.Z., Wu, H., Sun, L.M., Zhou, Y.D., Shen, C., & Guan, X.H. (2019). Integrated security threats and defense of cyber-physical systems. *Acta Automatica Sinica*. doi: 10.16383/j.aas.2018.c180461.

[17] Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.

[18] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, 13(10), article number 5875. doi: 10.3390/app13105875.

[19] Munko, A. (2023). Cyber security as a component of the state's financial security policy. *Problems of Modern Transformations*, 7. doi: 10.54929/2786-5746-2023-7-02-09.
[20] Pidpalyi, O. (2024). Future prospects: AI and machine learning in cloud-based SIP trunking. *Bulletin of Cherkasy State Technological University*, 29(1), 24-35. doi: 10.62660/bcstu/1.2024.24.
[21] Piera, M.A., Buil, R., & Ginters, E. (2016). State space analysis for model plausibility validation in multi-agent system simulation of urban policies. *Journal of Simulation*, 10(3), 216-226. doi: 10.1057/JOS.2014.42.
[22] Qader, C.O., & Ablahd, D.Z. (2023). Survey on computer cyber security. *World of Science: Journal on Modern Research Methodologies*, 2(9), 15-27.
[23] Rahayu, S.B., Jusoh, N., & Wardhana, A.A. (2023). Assessment of cybersecurity awareness in supply chain system for defense and security sector. *AIP Conference Proceedings*, 2617, article number 050001. doi: 10.1063/5.0119724.
[24] Rajendran, R.M., & Vyas, B. (2023). Cyber security threat and its prevention through artificial intelligence technology. *International Journal for Multidisciplinary Research*, 5(6). doi: 10.36948/ijfmr.2023.v05i06.10956.
[25] Rakushev, M., Zuiko, V., & Pantiushenko, R. (2022). Analysis of the use of the "Terminal" information and telecommunications system in the interests of the defense forces of Kyiv. *Modern Information Technologies in the Sphere of Security and Defence*, 44(2), 54-59. doi: 10.33099/2311-7249/2022-44-2-54-59.
[26] Savytska, L., Korobeinikova, T., Kostiuk, O., Kolesnyk, I., & Dudnyk, O. (2024). Internet of Things protection means in the corporate computer network. *Information Technologies and Computer Engineering*, 59(1), 83-93. doi: 10.31649/1999-9941-2024-59-1-83-93.
[27] Shi, C., Peng, J., Zhu, S., & Ren, X. (2024). From passive defense to proactive defence: Strategies and technologies. In *Artificial Intelligence Security and Privacy* (pp. 190-205). Singapore: Springer. doi: 10.1007/978-981-99-9785-5_14.
[28] Singh, H., Khatri, A., & Kaur, A. (2023). A study of cyber security challenges and its emerging trends on the latest technologies. *International Research Journal of Modernization in Engineering Technology and Science*, 5(12), 1085-1090. doi: 10.56726/IRJMETS47270.
[29] Singh, U.K., Sharma, A., Singh, S.K., Tomar, P.S., Dixit, K., & Upreti, K. (2022). Security and privacy aspect of cyber physical systems. In *Cyber Physical Systems* (pp. 141-164). New York: Chapman and Hall. doi: 10.1201/9781003220664.
[30] Smailov, N., Dosbayev, Z., Omarov, N., Sadykova, B., Zhekambayeva, M., Zhamangarin, D., & Ayapbergenova, A. (2023). A novel deep CNN-RNN approach for real-time impulsive sound detection to detect dangerous events. *International Journal of Advanced Computer Science and Applications*, 14(4), 271-280. doi: 10.14569/IJACSA.2023.0140431.
[31] Smutchak, Z., Fedun, I., Chorna, N., Chornyi, R., Kulikov, O., & Tyshchenko, O. (2023). Blockchain technologies in the conditions of digitalization of international business. In B. Alareeni, A. Hamdan, R. Khamis, R.E. Khoury (Eds.), *Digitalisation: Opportunities and challenges for business* (vol. 621, 796-804). Cham: Springer. doi: 10.1007/978-3-031-26956-1_74.
[32] Toliupa, S., & Slipachuk, L. (2023). Formation of the cyber protection system for the integrated industry information system of Ukraine of the national cyber security sector. *Information Systems and Technologies Security*, 71(13), 1183-1191. doi: 10.1615/TelecomRadEng.v71.i13.30.
[33] Too, W.K., & Mutuku, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions. *Reviewed Journal International of Business Management*, 4(1), 471-477. doi: 10.61426/business.v4i1.141.
[34] Trifunovic, D., & Bjelica, Z. (2018). Cyber war – trends and technologies. *National Security and the Future*, 3(21), 65-94. doi: 10.37458/nstf.21.3.2.
[35] Zheng, Y., Li, Z., Xu, X., & Qingzhan, Z. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, 8(4), 422-435. doi: 10.1016/j.dcan.2021.07.006.

Олег Семененко
Доктор військових наук, професор
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0000-0001-6477-3414

Сергій Кірсанов
Доктор технічних наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0000-0002-9696-0369

Артур Мовчан
Кандидат технічних наук
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0009-0006-0559-4962

Микола Ігнатьєв
Кандидат технічних наук
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0009-0007-8797-3364

Юзеф Добровольський
Кандидат технічних наук, доцент
Національний авіаційний університет
03058, просп. Любомира Гузара, 1, м. Київ, Україна
https://orcid.org/0000-0002-1077-1402

Вплив комп'ютерно-інтегрованих технологій на кібербезпеку в оборонному секторі

Анотація. Актуальність дослідження визначається постійно зростаючою загрозою кібератак та необхідністю захисту оборонних систем від цих загроз шляхом впровадження інтегрованих комп'ютерних технологій. Метою дослідження є розробка стратегій забезпечення цифрової безпеки в оборонному секторі з урахуванням впливу інформаційних технологій. У дослідженні проаналізовано вплив інтегрованих комп'ютерних технологій на інформаційну безпеку у військовій сфері, розроблено стратегії кібербезпеки та проаналізовано приклади їх застосування в оборонному секторі. Дослідження визначило, що інтегровані комп'ютерні технології відіграють важливу роль у покращенні кібербезпеки в оборонному секторі. Аналіз показав, що вони можуть ефективно виявляти, аналізувати та реагувати на кіберзагрози, забезпечуючи надійний захист критично важливих інформаційних ресурсів. Крім того, розроблені стратегії цифрової безпеки враховують специфіку оборонного сектору, допомагаючи покращити захист від кібератак та забезпечуючи негайні дії у разі виникнення загрози. Розроблені стратегії підвищення цифрової безпеки оборонного сектору враховують специфіку галузі, сприяючи підвищенню стійкості до кіберзагроз і забезпечуючи негайні дії у разі потенційних атак. Найбільш значущі приклади впровадження цих технологій, а саме: інтелектуальний аналіз даних, великі дані, розподілена технологія блокчейн, аналітичні методи кібер-аналізу та кібер-фізичні системи, продемонстрували свою ефективність в реальних умовах, сприяючи підвищенню безпеки та стійкості оборонних систем. Результати показують важливість інформаційних технологій для покращення кібербезпеки в оборонному секторі. Це підтверджує необхідність системного впровадження таких технологій для забезпечення ефективного захисту від сучасних кіберзагроз

Ключові слова: інформаційні системи; цифровий захист; оборонний комплекс; використання інновацій; електронні загрози