

CYBERSECURITY AS A COMPONENT OF NATIONAL AND ECONOMIC SECURITY

LEONID MAIDANEVYCH¹, VIKTOR GUDZ², VIKTORIIA REINSKA³, SVITLANA HURKOVSKA⁴, SERHII MOTORNIUK⁵

¹ PhD (Philosophical), Associate Professor, Department of Information Protection, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine

² Doctor of Historical Sciences, Professor, Department of History and Archaeology, Faculty of Social Sciences, Humanities and Law, Bohdan Khmelnytskyi Melitopol State Pedagogical University, Zaporizhzhia, Ukraine

³ PhD in Economics, Associate Professor, Educational and Scientific Institute of Cybernetics, Information Technologies and Engineering, National University of Water and Environmental Engineering, Rivne, Ukraine

⁴ PhD in Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technology and Data Analytics, Faculty of Production Automation, Information and Management Technologies, Metinvest Polytechnic Technical University, LLC, Zaporizhzhia, Ukraine

⁵ PhD Student, Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine.

E-mail: ¹ lmaidanevych@gmail.com, ² viktorvgudz@gmail.com, ³ vikrein@ukr.net, ⁴ n-s18@ukr.net,

⁵ tonnydexter@gmail.com

ABSTRACT

The article highlights the conceptual principles and practical aspects of ensuring cybersecurity as a key component of national and economic security in the context of the digitalization of society and the growth of hybrid threats. The study is aimed at generalizing modern approaches to the formation of a cyber defense system, analyzing the impact of cyber threats on the functioning of state institutions and economic processes, as well as determining the role of information influence as a tool for destabilizing society. Particular attention is paid to the importance of youth media literacy as an important factor in increasing cyber resilience and forming a safe information environment. The methodological basis of the study is the analysis of scientific publications, regulatory legal acts in the field of cybersecurity, analytical materials of international organizations, as well as the application of systemic and comparative approaches to assessing the effectiveness of cyber protection measures. Methods of generalization, systematization and structural-functional analysis were used to study the relationship between technical, organizational and social aspects of cybersecurity. It has been established that modern cyber threats are complex in nature and combine technical attacks with information and psychological influence, which significantly complicates the process of their detection and neutralization. It has been proven that effective cybersecurity requires an integrated approach, which includes the development of institutional capacity, improvement of regulatory and legal regulation, implementation of modern information protection technologies and activation of educational initiatives. It has been shown that increasing the level of media literacy of young people contributes to reducing vulnerability to disinformation, forming critical thinking and strengthening the information security of society. It is concluded that cybersecurity is a strategic prerequisite for ensuring the stability of the state, the sustainability of the economy and effective counteraction to modern information threats.

Keywords: *Cybersecurity, National Security, Economic Security, Information Influence, Youth Media Literacy*

1. INTRODUCTION

In today's global digitalization environment, cyberspace is becoming a key environment for the functioning of the state,

economy, and society. Information and communication technologies cover almost all spheres of life, – from public administration and financial systems to education, science, and the daily lives of citizens. At the same time, the rapid growth

of the level of digital integration is accompanied by increased vulnerability to cyber threats, which are becoming systemic and transnational.

The problem of cybersecurity becomes particularly relevant in the context of increasing hybrid conflicts, where cyberspace is used as a tool to influence political stability, economic sustainability and information sovereignty of the state. Cyberattacks on critical infrastructure facilities, financial institutions and state information resources can cause significant economic losses, disruption of management systems and loss of trust in government institutions.

An important component of modern cyber threats is information influence, which is implemented through the spread of disinformation, manipulation of public opinion and the formation of a distorted information environment. In this context, a special role is played by young people as the most active part of the digital society, which is both an object and a subject of information processes. An insufficient level of critical thinking and digital culture increases the risks of perceiving manipulative content, which necessitates the development of media literacy as a component of cyber resilience.

Ensuring cybersecurity today is considered not only as a technical task of protecting information systems, but also as a complex problem that encompasses legal, organizational, economic and social aspects. In this context, the formation of an effective cybersecurity system requires the integration of state policy, the development of institutional capacity, the introduction of innovative technologies and the activation of educational initiatives.

Thus, the relevance of the study is due to the need for a comprehensive understanding of cybersecurity as a component of national and economic security, as well as determining the role of information influence and media literacy of youth in the formation of a sustainable and safe information environment.

2. LITERATURE REVIEW

The issue of cybersecurity as a component of national and economic security is the subject of active research in the fields of information technology, economics, public administration, security studies and social communications. In modern scientific literature, cybersecurity is considered as a complex system that combines technical, organizational, economic and socio-humanitarian aspects aimed at ensuring the

resilience of the state and society to digital threats [1-3]. Researchers emphasize the transformation of cyberspace into a separate domain of confrontation, where, along with traditional threats, the role of information and psychological operations is growing.

A significant number of scientific works are devoted to the analysis of cyber threats in the context of national security. The studies of Khan et al. [4], Plazova et al. [5], Gallagher et al. [6] emphasize that cyber operations are becoming an important tool of geopolitical influence, capable of disrupting the functioning of critical infrastructure and public administration systems. At the same time, the literature focuses on the increasing complexity and hybridity of cyber threats, which combine technical attacks with elements of information influence.

A separate area of research focuses on the impact of cyber threats on the economic security of the state. Analysis of the works of Baranovska et al. [7], Juneja et al. [8], Krysovaty et al. [9] demonstrates that the digitalization of the economy creates new opportunities for development, but at the same time increases the risks of financial losses, disruption of business processes and reduced trust in digital platforms. Researchers emphasize the importance of forming effective cyber defense systems to ensure the stability of the financial sector, e-commerce and infrastructure systems.

Within the framework of research on information influence, considerable attention is paid to the problem of disinformation and manipulation of public opinion. The works of Doskich [10], Pira [11], Chen et al. [12] highlight the mechanisms of the spread of fake news, the role of social networks in shaping information flows, and the influence of algorithms of digital platforms on user behavior. It has been established that information influence is an effective tool for destabilizing society, which is especially evident in conditions of hybrid conflicts.

A significant layer of scientific research is devoted to media literacy as a tool for countering information threats. The works of Kharchenko et al. [13], Voitovych et al. [14], Dame Adjin-Tettey [15] emphasize that the development of critical thinking, information analysis skills and digital culture are key factors in increasing the resilience of society to disinformation. Particular attention is paid to youth as the most active audience in the digital environment, which requires targeted educational programs in the field of media literacy.

Some studies focus on shaping public policy in the field of cybersecurity. The works of Siudak [16], Calcara and Marchetti [17], Mishra et al. [18] examine approaches to developing national

cybersecurity strategies, public-private partnership mechanisms, and international cooperation tools. Researchers emphasize the need to integrate the technical and social components of cybersecurity, including educational initiatives and raising public awareness.

Summarizing scientific developments, we can distinguish three key areas of research in the field of cybersecurity as a component of national and economic security:

1. Technological – research into cyber threats, methods for protecting information systems, and critical infrastructure security [19-21].
2. Economic – analysis of the impact of cyber risks on the functioning of the economy, financial systems, and digital markets [22-24].
3. Socio-humanitarian – research into information influence, disinformation, and the role of media literacy in ensuring information security [25-27].

At the same time, a critical analysis of the reviewed sources reveals several significant gaps that remain insufficiently addressed. First, most studies focus on one of the dimensions of cybersecurity – technological, economic, or socio-communication – without properly considering their interaction. In particular, works [4, 19–21] consider in detail the protection of critical infrastructure, but do not link technical threats to economic consequences and social resilience. Works [7–9, 22–24] analyze economic losses from cyberattacks, but do not offer models for integrating economic and social factors into a single cyber resilience system. Studies [10–12, 25–27] deeply study disinformation and media literacy, but consider them mainly in an educational or media context, without embedding these aspects into the architecture of national security as an integral component of cyber defense.

Second, despite the growing recognition of the role of youth in the digital space, there is a lack of work that quantitatively or qualitatively links the level of youth media literacy with indicators of the cyber resilience of the state. Existing publications [13–15] call for the development of critical thinking, but do not offer conceptual schemes where media literacy acts as a buffer between information influence and the stability of society. Third, there are no comprehensive models that simultaneously take into account technological protection, economic security and the human factor, which makes it impossible to form a holistic policy.

Thus, there is a clear scientific gap: the need for interdisciplinary research that not only describes the individual components of cybersecurity, but also integrates them into a systemic model where youth

media literacy is considered as a full-fledged element of national and economic security. It is this gap that this work aims to fill, proposing a conceptual unification of the technical, economic, and socio-humanitarian dimensions of cybersecurity with an emphasis on the role of youth.

3. MATERIALS AND METHODS

The study is based on the analysis of scientific, theoretical, regulatory and analytical materials devoted to the issue of cybersecurity as a component of national and economic security. The information base consisted of publications in professional scientific journals on information technology, cybersecurity, economics, public administration and social communications, materials of international scientific and practical conferences, analytical reports of international organizations, as well as strategic documents in the field of digital transformation and cyber defense. The key sources were reports of international organizations, in particular the European Union Agency for Cybersecurity [28], Pascoe et al. [29], Organisation for Economic Co-operation and Development [30], as well as national cybersecurity strategies and digital economy development programs. To ensure scientific reliability, open, peer-reviewed and officially published sources were used.

The methodological basis of the study is a systems approach, which is used to consider cybersecurity as a complex multi-level system that combines technical, economic, organizational and social components. This allowed us to analyze the relationships between the level of development of digital infrastructure, the nature of cyber threats, information influence and the resilience of society.

In order to study the structure and functioning of the cybersecurity system, structural and functional analysis methods were used, which made it possible to identify its key elements: information systems protection, critical infrastructure security, cyber risk management, mechanisms for countering information influence, and the development of media literacy. The comparative method was used to compare international experience in the field of cybersecurity and information security, which allowed identifying common trends and features of national approaches.

To summarize theoretical provisions and practical experience, the method of content analysis of scientific publications, analytical reports, and strategic documents in the field of cybersecurity was used. This provided the opportunity to systematize approaches to identifying and neutralizing cyber

threats, as well as to identify key factors in the formation of cyber resilience.

At the stage of conceptual understanding of the results, a modeling method was applied, aimed at forming a generalized model of cybersecurity, taking into account the interaction of technical, institutional and social components. Additionally, the analogy method was used to determine the possibilities of adapting international experience to national conditions, in particular in the field of developing media literacy of youth as a tool for countering information threats.

The study also applied a historical-logical method, which allowed us to trace the evolution of approaches to ensuring cybersecurity –from technically oriented models of information protection to modern complex concepts of cyber resilience, which take into account informational and psychological aspects. Methods of analysis, synthesis and generalization, as well as secondary analysis of scientific sources, were used to form conclusions.

Thus, the methodological structure of the study combines systemic, comparative, and conceptual-model approaches, which provides a comprehensive study of cybersecurity as a component of national and economic security in the context of growing information threats and the need to develop media literacy among young people.

4. RESULTS

In the current conditions of digital transformation, cybersecurity acquires the status of a system-forming element of national and economic security, as it ensures the stability of the functioning of key state institutions, the continuity of economic processes, and the protection of information sovereignty. The results of the study indicate that cyberspace has transformed into an independent security domain that integrates technological, economic, and social components.

It has been established that cybersecurity has a multi-level structure, which includes both technical protection mechanisms and institutional and behavioral aspects. Its system-forming role is manifested in the ability to ensure the coordinated functioning of various sectors of the state, in particular energy, finance, transport and public administration. In this context, cybersecurity acts as an integrating factor that reduces the vulnerability of systems to internal and external threats.

In order to systematize the main components of cybersecurity as an element of national and economic security, their functional characteristics are summarized (Table 1).

Table 1: Structural components of cybersecurity and their impact on national and economic security

Cybersecurity component	Content	Impact on national security	Impact on economic security
Technological	Protection of information systems, networks and data using modern technologies	Ensuring the resilience of critical infrastructure	Reducing the risks of losses and disruptions in business processes
Institutional	Regulatory and legal regulation, public policy	Coordination of security actors, stability of management	Formation of a favorable investment environment
Economic	Cyber risk management, security investments	Increasing the resilience of the economic system	Reducing financial losses and increasing trust
Social	Media literacy level, digital culture	Counteracting information influence	Creating a secure information environment
Informative	Information space protection	Preserving information sovereignty	Stability of digital markets

Source: systematized by the author

As can be seen from Table 1, cybersecurity is complex and encompasses a wide range of interrelated elements, each of which has an impact on both national and economic security. Of particular importance is the integration of these components into a single management system that provides a synergistic effect.

An important element of a modern cybersecurity system is its technical and technological component, which provides direct protection of information resources, network infrastructure and digital services. Key cybersecurity technologies include intrusion detection and prevention systems (IDS/IPS), cryptographic data protection methods, multi-factor authentication, artificial intelligence technologies for analyzing cyber threats, and security information management systems (further – SIEM).

The use of proactive protection technologies is becoming particularly important, allowing not only to respond to incidents, but also to predict potential threats. The use of machine learning and big data helps to increase the efficiency of detecting anomalies in network traffic and user behavior.

In addition, the development of cloud technologies, the Internet of Things (further – IoT) and digital platforms leads to the emergence of new attack vectors, which requires the implementation of

comprehensive cyber defense solutions focused on the security of distributed systems. In this context, the integration of the principles of “security by design” and “zero trust architecture” is important, which involve building security at all levels of information systems.

Thus, the technical component of cybersecurity serves as the foundation for ensuring the stability of digital infrastructure and the effective functioning of national and economic systems.

To detail the technical architecture of a cyber defense system, it is advisable to visualize the

interaction of the main functional modules that provide monitoring, detection, analysis and neutralization of cyber threats. Such an engineering approach allows us to present cybersecurity not only as a conceptual category, but also as a structured technical system that operates in a mode of continuous control of the digital environment.



Figure 1: Engineering diagram of the technical architecture of the cyber defense system

As shown in Figure 1, the technical cyber defense system has a multi-level architecture, in which each functional module performs a separate task within a single process of ensuring cyber resilience. At the first level, data is collected from end devices, network equipment and industrial digital systems. Then, information flows pass through network protection tools and IDS/IPS modules, which provide initial detection of unauthorized access attempts. The central element of the system is the SIEM/SOC module, where event correlation, log analysis and response scenario generation take place. The use of artificial intelligence algorithms and threat intelligence databases allows to increase the accuracy of anomaly

detection and predict potential attack vectors. The final stage is automated response, data backup and system recovery after an incident.

In-depth analysis has shown that modern cyber threats are systemic in nature and can simultaneously affect several levels of security. For example, attacks on energy infrastructure can lead to economic losses, social instability, and loss of trust in state institutions. This confirms the need to consider cybersecurity as an integrated system that combines various functional components.

To visualize the relationships between key elements of cybersecurity and their impact on national and economic security, a generalized conceptual diagram is proposed (Figure 2).

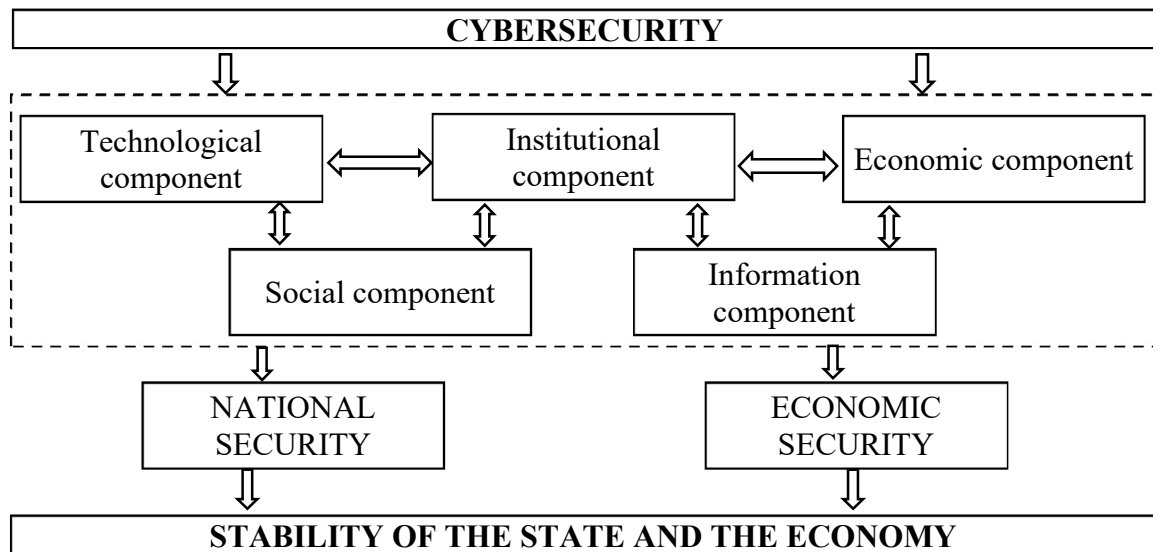


Figure 2: Conceptual diagram of cybersecurity as a system-forming element of security

Source: developed by the author

As shown in Figure 2, cybersecurity acts as a central element that accumulates the impact of various components and transforms it into ensuring the stability of the state and the economy. The interaction between these components forms a comprehensive cyber resilience system capable of adapting to dynamic threats.

In addition, the study found that the effectiveness of cybersecurity depends largely on the level of integration between the public and private sectors. Companies that implement modern cyber protection systems demonstrate a higher level of risk resilience and the ability to recover faster from incidents. This highlights the importance of forming public-private partnerships in the field of cybersecurity.

Another important result is the identification of the relationship between cybersecurity and trust in digital systems. A high level of security of information resources contributes to the development of e-government, digital financial services and e-commerce, which has a positive impact on economic growth.

Thus, cybersecurity is a key integration element that ensures the coordinated functioning of national and economic systems, reduces the level of risks and forms the basis for sustainable development in the digital economy. The presence of clearly structured components (Table 1) and their interrelationships (Figure 2) confirms the need for a comprehensive approach to the formation of cybersecurity policy.

The study found that information influence is one of the key components of modern cyber threats, which significantly transforms approaches to ensuring national and economic security. Unlike traditional cyber threats, which are predominantly technical in nature, information influence combines technological tools with psychological mechanisms of influence on human consciousness, which significantly increases its effectiveness and complexity of counteraction.

It has been found that information influence is implemented through digital communication platforms, social networks and information resources, which ensure the rapid dissemination of content among wide audiences. The main tools of such influence are disinformation, manipulative messages, information injections, the use of botnets and algorithmic reinforcement of content. As a result, a distorted information environment is formed, which affects decision-making processes at both the individual and societal levels.

The study showed that information influence is multidimensional and can simultaneously affect political stability, social cohesion and economic processes. In particular, the spread of unreliable information can lead to panic, reduced trust in state institutions, destabilization of financial markets and increased social tension. In this context, information security becomes an integral component of cyber resilience.

The study pays special attention to youth as a key socio-demographic group that actively functions in the digital environment. It was found that young people are characterized by a high level

of digital activity, intensive consumption of information content and significant involvement in online communications. This, on the one hand, creates conditions for the rapid spread of information, and on the other hand, –increases vulnerability to manipulative influence.

At the same time, the results of the study indicate that young people have significant potential in shaping a cyber-resilient society, provided they

have the appropriate level of media literacy. Media literacy is considered an integral competence that includes critical thinking, the ability to analyze information flows, the skills of checking the reliability of sources, and awareness of the mechanisms of information influence.

In order to systematize the impact of information threats and the role of media literacy, their relationship is summarized in Figure 3.

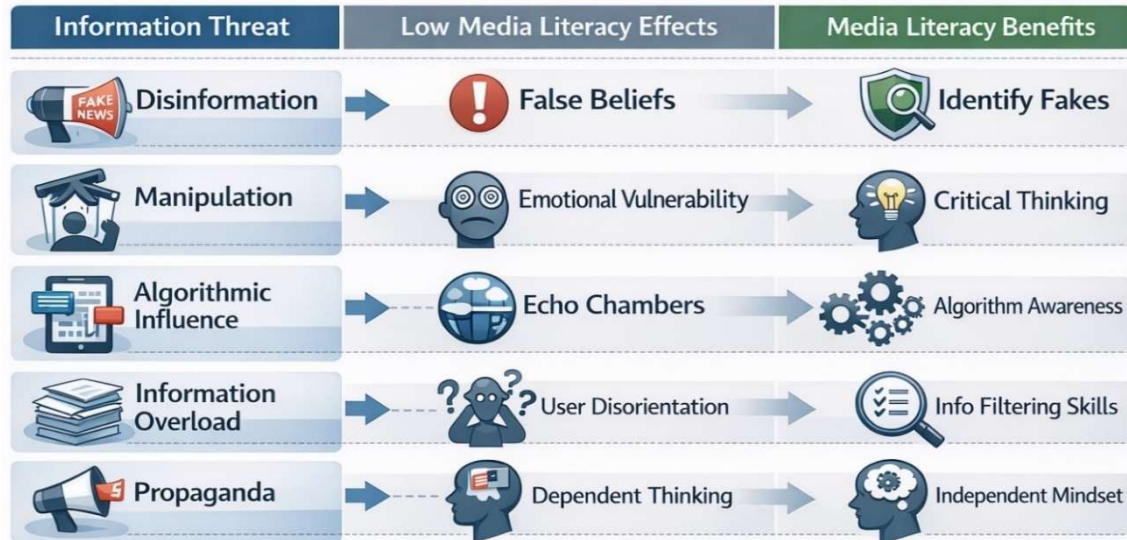


Figure 3: The relationship between information influence and media literacy in shaping cyber resilience

Source: systematized by the author

As can be seen from Figure 3, the level of media literacy directly affects the ability to counteract information threats. A high level of media literacy ensures the formation of sustainable information behavior, which is an important element of cyber resilience.

For a deeper understanding of the mechanisms of forming cyber resilience based on media literacy, a conceptual diagram of the interaction of key factors is proposed (Figure 4).

As shown in Figure 4, media literacy acts as a key buffer mechanism that determines the level of susceptibility to information influence. In the case of a low level of media literacy, the negative effects of information influence are amplified, which leads to social destabilization. In contrast, a high level of media literacy ensures the formation of critical thinking and the ability to independently analyze information, which contributes to strengthening cyber resilience.

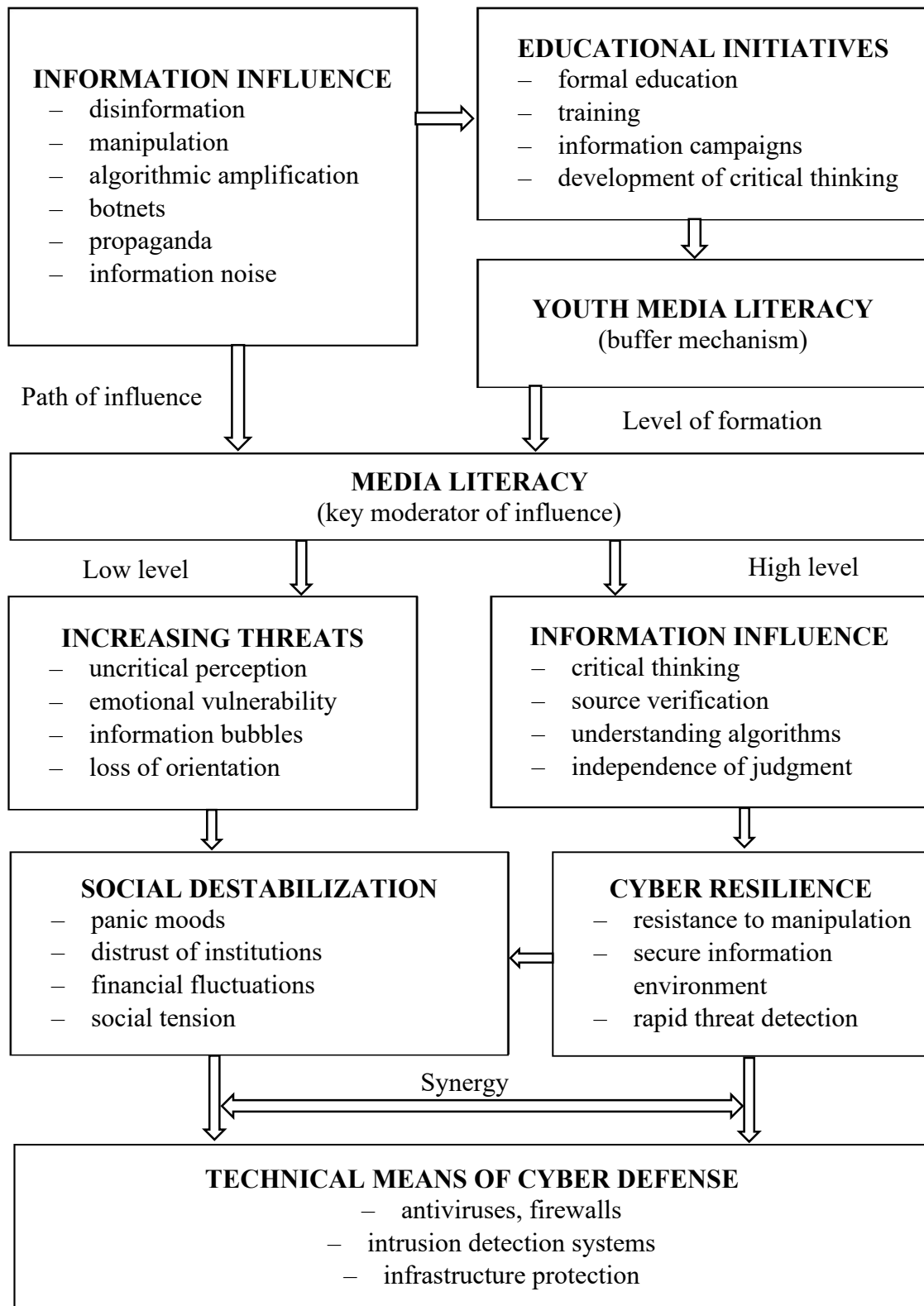


Figure 4: Model of the impact of youth media literacy on the level of cyber resilience

Source: developed by the author

Additionally, it has been established that the effectiveness of countering information threats largely depends on the integration of educational initiatives in the field of media literacy into the formal and informal education system. The implementation of specialized educational programs, trainings and information campaigns contributes to raising the level of awareness of young people about the risks of the digital environment.

The results of the study also confirm that the combination of technical cyber defense measures with the development of media literacy creates a synergistic effect. Technical solutions provide a basic level of protection for information systems, while media literacy increases users' resistance to information manipulation.

Thus, information influence is one of the key challenges of modern cybersecurity, and media literacy of youth is an effective tool for its neutralization. Their interaction determines the level of cyber resilience of society, which is confirmed by the generalized results presented in Figures 3, 4. This justifies the need to form a comprehensive state policy aimed at the development of media literacy as a component of the system of national and economic security.

5. DISCUSSION

The obtained research results are consistent with modern scientific approaches to understanding cybersecurity as a multidimensional and interdisciplinary phenomenon that goes beyond a purely technical interpretation. Unlike traditional concepts that focused mainly on the protection of information systems, this work substantiates the need for an integrated approach that combines technological, economic, and socio-humanitarian aspects. This approach correlates with the positions of modern researchers who emphasize the transformation of cyberspace into a full-fledged security domain.

The results presented in Table 1 and Figure 2 confirm the thesis about the system-forming role of cybersecurity in ensuring national and economic security. Unlike a number of studies, where cybersecurity is considered as an auxiliary element, this work proves its integrative nature. This allows us to consider cybersecurity as a platform that unites different areas of security into a single functional system. At the same time, it is worth noting that in practice the implementation of such an approach is complicated by the fragmentation of state policy and

the insufficient level of coordination between cyber defense entities.

The issue of the relationship between cybersecurity and economic stability deserves special attention. The results obtained confirm the conclusions of other authors regarding the significant impact of cyber threats on financial systems and business processes, but complement them with an emphasis on trust as a key economic factor. It has been established that trust in digital services is not only a consequence of effective cybersecurity, but also a prerequisite for the development of the digital economy. This opens a new direction for further research related to the quantitative assessment of the impact of cybersecurity on macroeconomic indicators.

In the context of information influence, the results of the study confirm the provisions of modern literature on its growing role in hybrid conflicts. However, unlike most scientific works, where information influence is considered separately from technical cyber threats, this study substantiates their synergistic nature. This is reflected in Figures 3, 4, which shows that the effectiveness of information influence largely depends on the level of media literacy of users.

A special contribution of the study is the emphasis on the role of youth media literacy as a key factor in shaping cyber resilience. The results extend existing approaches, which are mostly limited to general awareness-raising among the population, and emphasize the need for targeted work with youth as the most active digital group. At the same time, it should be noted that the effectiveness of such measures depends on the quality of educational programs, their adaptation to the modern digital environment and the level of user engagement.

The question of the ratio of technical and social measures in ensuring cybersecurity remains debatable. On the one hand, the results of the study confirm the need to develop modern cyber protection technologies. On the other hand, it has been proven that without the proper level of media literacy, even the most effective technical solutions do not provide complete protection against information threats. This indicates the feasibility of the transition from a technocentric to a human-oriented approach in the formation of cybersecurity policy.

In addition, the results of the study indicate the need to strengthen the institutional component of cybersecurity. Despite the presence of strategic documents and regulatory acts, their practical implementation often faces problems of resource provision, insufficient coordination and limited integration with international initiatives. In this

context, the development of public-private partnerships and international cooperation is important.

At the same time, certain limitations of the study should be taken into account. In particular, it is based mainly on secondary analysis of scientific sources and analytical materials, which limits the possibility of empirical verification of the results obtained. Further research should be directed at quantitative assessment of the level of cyber resilience, analysis of the effectiveness of specific policies, and studying the behavioral aspects of the perception of information influence by young people.

Thus, the results of the study confirm the need to rethink the role of cybersecurity in the system of national and economic security and justify the feasibility of a comprehensive approach that combines technological, economic and social tools. Of particular importance is the integration of media literacy into the system of ensuring cyber resilience, which opens up new prospects for the development of both scientific research and practical security policy.

Despite the results obtained, it is worth recognizing that the study has certain limitations. First, it is based mainly on secondary analysis of sources, which does not allow empirical verification of the proposed conceptual models. Second, the focus is only on young people, while other age groups also need to be studied. Third, although the work differs favorably from previous studies in that it does not isolate the technical, economic and informational components, but combines them into a holistic system, where media literacy acts as a buffer against informational influence, a number of unresolved issues remain. In particular, there is a lack of generally accepted quantitative metrics of cyber resilience, ethical dilemmas between security and privacy require attention, as well as the rapid development of generative artificial intelligence, which is able to outpace educational initiatives in media literacy. These are the areas that constitute the prospect of further research.

6. CONCLUSIONS

The study substantiates that cybersecurity is a key component of national and economic security in the context of the digital transformation of society and the growth of hybrid threats. It has been established that modern cyberspace functions as an independent security domain that integrates technological, economic, and socio-humanitarian

components, forming a comprehensive system for ensuring the stability of the state.

It has been proven that cybersecurity has a system-forming nature and ensures the coordinated functioning of critical infrastructure, state institutions and economic processes. The generalization of structural components (Table 1) and their interrelationships (Figure 2) allowed us to establish that the effectiveness of cybersecurity depends on the integration of technological, institutional, economic, social and information elements into a single management system.

It has been revealed that modern cyber threats are complex in nature and combine technical attacks with informational and psychological influence, which significantly complicates the process of their identification and neutralization. Of particular danger is informational influence, which is implemented through digital platforms and is aimed at manipulating public opinion, destabilizing socio-economic processes and reducing trust in state institutions.

It is substantiated that media literacy of youth is an important tool for countering information threats and a key factor in shaping the cyber resilience of society. The results presented in Figures 3, 4 confirm that increasing the level of media literacy contributes to the development of critical thinking, reducing vulnerability to disinformation, and forming responsible information behavior.

The feasibility of using a comprehensive approach to ensuring cybersecurity, which combines technical cyber protection measures with educational and institutional initiatives, has been proven. It has been established that the combination of technological solutions and the development of media literacy creates a synergistic effect that increases the effectiveness of countering modern cyber threats.

The practical significance of the results obtained lies in the possibility of their use in the formation of state policy in the field of cybersecurity, the development of educational programs on media literacy and the improvement of mechanisms for managing cyber risks. The proposed approaches can be adapted to increase the level of cyber resilience at both the national and organizational levels. Prospects for further research are related to the development of quantitative methods for assessing the level of cyber resilience, the analysis of the effectiveness of specific tools for countering information influence, as well as the study of behavioral aspects of user interaction with the digital environment.

It has been established that the combination of technological solutions and the development of media literacy creates a synergistic effect that increases the effectiveness of countering modern cyber threats, in particular through the implementation of modern cyber defense technologies and intelligent threat detection systems.

Thus, cybersecurity is a strategic prerequisite for ensuring the stability of the state, the sustainability of the economy, and the effective functioning of society in the face of modern digital challenges, and the development of media literacy among youth is one of the key areas for strengthening cyber resilience.

According to the authors, the presented study not only systematizes modern approaches to understanding cybersecurity, but also demonstrates the urgent need for a paradigm shift – from purely technical protection of information systems to a human-centric model of cyber resilience. We are convinced that the integration of youth media literacy into the national security strategy is not a secondary educational option, but a critically important element that can significantly reduce society's vulnerability to hybrid threats. The proposed conceptual schemes, despite their theoretical nature, reflect our vision of how the interaction between the state, business and citizen should be built in the digital environment. Aware of the limitations associated with the lack of empirical verification, we consider this work as an invitation to interdisciplinary dialogue and hope that the ideas presented will stimulate both further scientific research and practical steps to form a holistic cybersecurity policy.

In summary, this study aimed to summarize modern approaches to cybersecurity, analyze the impact of cyber threats on state institutions and the economy, and determine the role of information influence and media literacy of youth as factors of cyber resilience. A critical analysis of the results obtained shows that these tasks were accomplished mainly at the conceptual level.

On the one hand, the work achieved a number of significant results: the structural components of cybersecurity were systematized (Table 1) and their impact on national and economic security was shown; an engineering scheme of the cyber defense architecture was built (Figure 1) and a conceptual scheme of cybersecurity as a system-forming element was built (Figure 2); the hybrid nature of modern threats, combining technical attacks with information and psychological influence, was proven; a model was developed in which youth media literacy acts as a buffer between

disinformation and social stability (Figure 4). Thus, the work fills the gap identified in the literature - the lack of integrated models that simultaneously take into account the technological, economic and socio-humanitarian dimensions.

On the other hand, it is worth critically recognizing significant limitations. First, all the proposed conceptual constructs remain theoretical hypotheses that have not undergone empirical verification; therefore, the strength of the relationship between media literacy and real cyber resilience has not been quantitatively confirmed. Second, the study is limited to a youth audience, ignoring other demographic groups that are also objects of information influences. Third, the work does not offer specific metrics or indicators for measuring cyber resilience, which complicates the practical application of the conclusions. Furthermore, the ethical conflicts between enhancing security and protecting privacy have been overlooked, as well as the new challenges posed by generative artificial intelligence, which can scale disinformation faster than educational initiatives.

Thus, the work presented is more an invitation to interdisciplinary dialogue than a complete practical tool. It lays a conceptual foundation on which future research can build empirical models, develop validated metrics, and formulate concrete policy recommendations. Only by combining quantitative methods, reaching a wider audience, and taking into account ethical aspects can the outlined ideas be transformed into an effective system for ensuring national and economic security in the digital age.

REFERENCES:

- [1] A. Diegtiar and M. Bilokon, "Institutional resilience of public administration under hybrid threats: Economic and socio-humanitarian countermeasures," *Global Scientific Trends: Economics and Public Administration*, vol. 4, no. 4, pp. 26–44, 2025. <https://gst-journal.net.ua/index.php/gst/article/view/61>
- [2] O. Vivchar, V. Gevko, and L. Kvasnyi, "Security of economic agents under conditions of digitalization: Methodological basis and applied contexts," *Herald of Khmelnytskyi National University. Economic Sciences*, vol. 308, no. 4, pp. 247–251, 2022. <https://doi.org/10.31891/2307-5740-2022-308-4-38>
- [3] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards – a review and comprehensive overview,"

- Electronics*, vol. 11, no. 14, p. 2181, 2022. <https://doi.org/10.3390/electronics11142181>
- [4] A. W. Khan, S. Saeed, and M. S. Kakar, "Cybersecurity as a geopolitical tool: The growing influence of digital warfare in statecraft," *International Research Journal of Social Sciences and Humanities*, vol. 3, no. 2, pp. 345–357, 2024. <https://irjssh.com/index.php/irjssh/article/view/209>
- [5] T. Plazova, O. Kuz, N. Konnova, D. Korotkov, and O. Galushchenko, "Information warfare as an instrument of geopolitical influence on Ukraine: Main aspects and the state's response," *International Journal of Religion*, vol. 5, no. 2, pp. 121–130, 2024. <https://doi.org/10.61707/0g2yt516>
- [6] L. Gallagher, M. Lang, and J. Morrissey, "Cyber warfare during the Russian invasion of Ukraine—the impact of geopolitical dynamics on global cybersecurity," in *2025 Cyber Research Conference-Ireland (Cyber-RCI)*, 2025, pp. 1–6. <https://doi.org/10.1109/Cyber-RCI68134.2025.11384990>
- [7] T. Baranovska, V. Savitskyi, M. Serbov, Y. Stoliar, and Y. Krutik, "The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures," *Economic Affairs*, vol. 69, pp. 33–42, 2024. <https://doi.org/10.46852/0424-2513.1.2024.5>
- [8] A. Juneja, S. S. Goswami, and S. Mondal, "Cyber security and digital economy: Opportunities, growth and challenges," *Journal of Technology Innovations and Energy*, vol. 3, no. 2, pp. 1–22, 2024. <https://doi.org/10.56556/jtie.v3i2.907>
- [9] A. Krysovaty, O. Desyatnyuk, and O. Ptashchenko, "Digital innovations and their ramifications for financial and state security," *African Journal of Applied Research*, vol. 10, no. 1, pp. 431–441, 2024. <https://doi.org/10.26437/ajar.v10i1.713>
- [10] L. Doskich, "Fake news as the newest tool of manipulation and disinformation," *Library Science. Record Studies. Informology*, no. 4, pp. 72–77, 2022. <https://doi.org/10.32461/2409-9805.4.2022.269809>
- [11] F. Pira, "Disinformation a problem for democracy: Profiling and risks of consensus manipulation," *Frontiers in Sociology*, vol. 8, p. 1150753, 2023. <https://doi.org/10.3389/fsoc.2023.1150753>
- [12] L. Chen, J. Chen, and C. Xia, "Social network behavior and public opinion manipulation," *Journal of Information Security and Applications*, vol. 64, p. 103060, 2022. <https://doi.org/10.1016/j.jisa.2021.103060>
- [13] S. Kharchenko, A. Savchuk, H. Dehtiarova, A. Pomaza-Ponomarenko, and O. Siemilietov, "Media literacy of citizens as a factor in counteracting manipulative influence on the state," *European Journal of Sustainable Development*, vol. 15, no. 1, pp. 563–563, 2026. <https://doi.org/10.14207/ejsd.2026.v15n1p563>
- [14] N. Voitovych, M. Kitsa, and I. Mudra, "Media education and media literacy as a factor in combating disinformation," *Journalism and Media*, vol. 6, no. 4, p. 188, 2025. <https://doi.org/10.3390/journalmedia6040188>
- [15] T. Dame Adjin-Tettey, "Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education," *Cogent Arts & Humanities*, vol. 9, no. 1, p. 2037229, 2022. <https://doi.org/10.1080/23311983.2022.2037229>
- [16] R. Siudak, "Cybersecurity discourses and their policy implications," *Journal of Cyber Policy*, vol. 7, no. 3, pp. 318–335, 2022. <https://doi.org/10.1080/23738871.2023.2167607>
- [17] A. Calcara and R. Marchetti, "State-industry relations and cybersecurity governance in Europe," *Review of International Political Economy*, vol. 29, no. 4, pp. 1237–1262, 2022. <https://doi.org/10.1080/09692290.2021.1913438>
- [18] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, 2022. <https://doi.org/10.3390/s22020538>
- [19] A. Akinyemi, "Securing critical infrastructure against cyber attacks," *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, vol. 14, no. 4, pp. 201–209, 2022. <https://doi.org/10.18090/samriddhi.v14i04.43>
- [20] V. Khaustova, M. R. Țirlea, L. Dandara, N. Trushkina, and I. Birca, "Development of critical infrastructure from the point of view of information security," *Univers Strategic*, vol. 53, no. 1, pp. 170–188, 2023. <https://www.cceol.com/search/article-detail?id=1107664>
- [21] R. H. Chowdhury and B. Mostafa, "Cyber-physical systems for critical infrastructure protection: Developing advanced systems to

- secure energy grids, transportation networks, and water systems from cyber threats,” *Journal of Computer Science and Electrical Engineering*, vol. 7, no. 1, pp. 16–26, 2025. <https://doi.org/10.61784/jcsee3027>
- [22] O. Gulyas and G. Kiss, “Impact of cyber-attacks on the financial institutions,” *Procedia Computer Science*, vol. 219, pp. 84–90, 2023. <https://doi.org/10.1016/j.procs.2023.01.267>
- [23] A. Kuzior, T. Vasylieva, O. Kuzmenko, V. Koibichuk, and P. Brožek, “Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 4, p. 195, 2022. <https://doi.org/10.3390/joitmc8040195>
- [24] J. Yang, Y. Zhao, C. Han, Y. Liu, and M. Yang, “Big data, big challenges: Risk management of financial market in the digital economy,” *Journal of Enterprise Information Management*, vol. 35, no. 4–5, pp. 1288–1304, 2022. <https://doi.org/10.1108/JEIM-01-2021-0057>
- [25] Y. Chmyr, A. Nekryach, L. Kochybei, A. Dakal, and L. Strelbytska, “Postindustrial society and global informational space as infrastructure medium and factor for actualization of the state informational security,” in *National Security Drivers of Ukraine*, O. Radchenko, V. Kovach, I. Semenets-Orlova, and A. Zaporozhets, Eds. Cham, Switzerland: Springer, 2023, pp. 61–73. https://doi.org/10.1007/978-3-031-33724-6_4
- [26] S. Tayie, “Media and information literacy to counter disinformation,” *Insights into Language, Culture and Communication*, vol. 2, no. 2, pp. 83–83, 2022. <https://dx.doi.org/10.21622/ilcc.2022.02.2.083>
- [27] S. Diepeveen and M. Pinet, “User perspectives on digital literacy as a response to misinformation,” *Development Policy Review*, vol. 40, p. e12671, 2022. <https://doi.org/10.1111/dpr.12671>
- [28] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2023*. Luxembourg: Publications Office of the European Union, 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [29] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper CSWP 29. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024. <https://doi.org/10.6028/NIST.CSWP.29>
- [30] Organisation for Economic Co-operation and Development, *Fast-Track on Digital Security in Health (OECD Health Working Papers)*. Paris, France: OECD Publishing, 2023. https://www.oecd.org/en/publications/fast-track-on-digital-security-in-health_c3357f9f-en.html