Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 1436 – 1442
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3673

Ensuring Cybersecurity in the Modern World: Challenges from Artificial Intelligence-Based Fraud Posing a Threat to the Environment

Serhiy Marko[1], Yuriy Tsaruk[2], Halyna Skhidnytska[3], Myroslav Kryshtanovych[4], Uliana Nikonenko[5]

Abstract

Cybersecurity in the modern world is a critical field that involves protecting systems, networks, and programs from digital attacks. With advancements in technology, artificial intelligence (AI) has become a double-edged sword. While AI can enhance cybersecurity measures, it also introduces new vulnerabilities. Fraudulent activities facilitated by AI not only pose risks to financial and data security but increasingly threaten environmental sustainability as well. The purpose of the article is to identify ways to ensure cybersecurity. The object of the study is challenges from fraud using artificial intelligence technologies that threaten the environment. The research methodology involves the use of modern IDEF0 modeling methods. As a result of the study, a model for ensuring cybersecurity is presented.

Keywords: *Cybersecurity, Artificial Intelligence, Environment, Security, Threats, Modeling.*

Introduction

Artificial intelligence is rapidly evolving, extending its reach into various sectors including finance, healthcare, and the environment. AI systems can process and analyze data at unprecedented speeds and accuracy, making them invaluable tools for efficiency and innovation. However, this capability also allows for sophisticated fraudulent schemes that can manipulate data, leading to significant negative impacts on both economic and environmental fronts.

AI-based fraud involves the use of machine learning algorithms to mimic, replicate, or bypass security systems. For instance, AI can be used to create deepfake videos or generate synthetic identities, complicating the detection of frauds and scams. These technologies can be exploited to conduct large-scale fraudulent activities without immediate detection, affecting financial markets, consumer trust, and environmental regulations. The environmental impact of AI-based fraud is profound. Fraudulent activities can lead to erroneous data reporting in environmental monitoring, manipulation of emission reports, or unlawful exploitation of natural resources. These actions can result in misguided policies, inadequate resource allocation, and ultimately, significant harm to ecosystems and biodiversity. Detecting and preventing AI-based fraud poses significant challenges due to the complexity and adaptability of AI systems. Traditional cybersecurity measures often fall short against AI-driven attacks as they can evolve and learn from attempts to detect them. Ensuring the integrity of data and the authenticity of digital communications is becoming harder, necessitating advanced defensive strategies that can keep pace with AI-driven threats. As AI technologies advance, so too must the regulatory frameworks that govern their use. Current laws may not adequately address the novel ways in which AI can be used for fraud, particularly in terms of environmental regulations. Ethical considerations also come into play, as the deployment of AI must balance innovation with responsibilities toward protecting the environment and ensuring public trust.

[1] Department of Criminal Procedure and Criminalistics, Lviv State University of Internal Affairs, Lviv, Ukraine. https://orcid.org/0000-0002-9778-0570.
[2] Adjunct of the Department of Operative Search Activity, Lviv State University of Internal Affairs, Lviv, Ukraine https://orcid.org/0009-0008-4529-9567.
[3] Lviv National Environmental University, Lviv, Ukraine https://orcid.org/0000-0003-0333-1721.
[4] Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine https://orcid.org/0000-0003-1750-6385.
[5] Department of Management and Marketing in Publishing and Printing, Institute of Printing and Media Technologies, Lviv Polytechnic National University, Lviv, Ukraine, https://orcid.org/0000-0002-6015-6248

To combat AI-based fraud, new technologies and methodologies are being developed. Blockchain technology, for example, offers a way to secure data through decentralized and tamper-evident digital ledgers, making it more difficult for fraudulent data to be introduced. Similarly, advancements in AI and machine learning are being leveraged to predict and detect fraudulent patterns with greater accuracy. Addressing AI-based fraud requires collaborative efforts across multiple sectors. Governments, industries, and environmental organizations need to work together to share knowledge, strategies, and resources. By fostering a culture of transparency and cooperation, stakeholders can more effectively tackle the challenges posed by fraudulent activities and protect the environment.

The future of cybersecurity in relation to AI-based fraud is an ongoing battle of innovation. As AI technologies become more sophisticated, so too will the methods to exploit them. The cybersecurity community must remain vigilant and proactive, continuously advancing their strategies to outpace potential threats. This includes not only technological advancements but also training for cybersecurity professionals in AI-related risks and vulnerabilities.

Ensuring cybersecurity in the face of AI-based fraud is crucial for protecting not just financial and personal data, but also the environment. The intersection of AI, fraud, and environmental impact presents unique challenges that demand innovative solutions and global cooperation. As the digital landscape evolves, so must our approaches to maintaining security and integrity across all aspects of society.

Literature Review

Alazzam et al. (2023) discuss the formation of innovative models for e-commerce development to ensure economic security, highlighting the importance of integrating cybersecurity measures in these models to mitigate risks, including those posed by AI-based frauds . Following up, Alazzam et al. (2024) expand on the need for methodical approaches in business management strategies that adapt to changing commercial activities, suggesting that strategic decisions must consider the potential of AI to disrupt business operations through fraudulent activities .

The work by Alazzam et al. (2023) on rational environmental use in the context of commercial bioeconomy development points to the significant role that state management plays in regulating AI applications to ensure that these technologies do not harm the environment through unsustainable practices . This is particularly pertinent as AI's capability to manipulate data can lead to environmental mismanagement if not properly overseen.

Exploring the utilization of blockchain technology, Alazzam et al. (2023) focus on the nature of electronic contracts in the realm of cryptocurrencies, such as Bitcoin. They emphasize the blockchain's potential to secure transactions and prevent fraud, including in environmental applications where transparency in transactions is crucial for compliance and monitoring .

Further, Alazzam et al. (2023) present a study on developing information models for e-commerce platforms, emphasizing the need for legal compliance in the face of global digitalization . Al-Maagbeh et al. (2024) also discuss the use of AI in public administration, indicating that historical and modern legal frameworks must evolve to address the challenges posed by AI, including those related to cybersecurity and environmental law .

Addressing broader implications, Bani-Meqdad et al. (2024) articulate the challenges in the cyber-environment related to human rights and intellectual property law. They stress the importance of protecting these rights to ensure sustainable development, which is increasingly threatened by sophisticated AI-based frauds that can undermine both legal rights and environmental goals .

Blikhar et al. (2023) and Kopytko & Sylkin (2023) both highlight the legal aspects of combating corruption, including in the economic security management systems of states. They underscore the need for robust legal frameworks that can adapt to and address the complexities introduced by AI in economic and administrative systems .

Methodology

Integrated DEFinition for Function Modeling (IDEF0) is a method designed to model the decisions, actions, and activities of an organization or system. IDEF0 was derived from a well-established graphical language known as Structured Analysis and Design Technique (SADT). The primary purpose of using IDEF0 in this study is to comprehensively understand and articulate the processes involved in ensuring cybersecurity against the threats posed by artificial intelligence-based fraud, particularly those that impact environmental sustainability.

IDEF0 is utilized in this research to provide a clear, systematic, and visual representation of the complex processes that make up cybersecurity systems. The method helps in identifying and modeling the functions (what is done), the inputs (what drives the function), the controls (how the function is constrained), and the outputs (what the function produces) of these systems. In the context of cybersecurity, IDEF0 facilitates the exploration of various functions related to threat detection, response strategies, and prevention mechanisms against AI-enabled frauds.

Results Of Research

In the context of cybersecurity challenges posed by artificial intelligence (AI), Integrated DEFinition for Function Modeling (IDEF0) emerges as a critical methodological tool. IDEF0, originally developed from the Structured Analysis and Design Technique (SADT), is adept at modeling complex systems and processes. It is particularly suited to detailing the multifaceted nature of cybersecurity systems that must contend with the dual-threat of AI: its power to enhance security measures and its potential to enable sophisticated frauds, especially those impacting environmental sustainability.

The application of IDEF0 in cybersecurity revolves around its ability to visually represent functions, their interactions, and the overall workflow within an organization's security protocol. This method starts by defining the scope and context of the model, focusing specifically on areas susceptible to AI-related threats. These include systems involved in monitoring environmental data, which are particularly vulnerable to manipulation. The next step involves identifying major functions within the cybersecurity framework, such as threat detection, risk assessment, and incident response, which are depicted as distinct boxes in the IDEF0 diagrams.

Each function identified is further decomposed into sub-functions in the IDEF0 model. This decomposition is vital as it allows for a granular analysis of the cybersecurity operations, providing insights into specific actions within the broader process. This detailed breakdown helps in pinpointing where vulnerabilities might be exploited by AI to commit fraud that could lead to environmental damage, such as falsifying pollution data or manipulating emission reporting systems.

For each function and sub-function, IDEF0 requires the specification of inputs, outputs, controls, and mechanisms. Inputs are the resources needed to perform a function; outputs are the results; controls are the regulatory or policy constraints; and mechanisms are the tools or technologies employed. This systematic categorization helps in understanding the flow of information and the dependencies within the system, thereby highlighting potential points of failure where AI could be misused.

Creating the IDEF0 diagrams is a crucial step as these visual representations map out the interrelationships between different functions and their components. These diagrams serve as a tool for stakeholders to visualize complex workflows and dependencies clearly, making it easier to identify areas needing reinforcement against AI-based threats. Additionally, these diagrams facilitate communication among team members and across departments, helping to ensure that all parts of the organization understand the potential cybersecurity risks and their roles in mitigating them.

Lets build first IDEF model:

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3673

A1. Advanced Threat Intelligence Gathering. Develop a system that continuously gathers and analyzes data on emerging AI-driven threats. This involves integrating cutting-edge AI tools that can predict and simulate potential attack vectors, especially those that could manipulate environmental data or disrupt ecological monitoring systems.

A2. Real-Time Monitoring and Detection Systems. Deploy real-time monitoring systems that utilize AI to detect anomalies and potential threats as they occur. These systems should be capable of differentiating between typical network behavior and potentially malicious anomalies that indicate AI-driven fraud.

A3. Rapid Response and Mitigation. Once a threat is detected, a rapid response mechanism should be activated to contain and mitigate the impact. This involves automated systems capable of implementing immediate countermeasures to prevent data breaches or environmental harm.

A4. Post-Incident Analysis and System Update. After an incident, conduct thorough investigations to understand the breach, learn from the event, and strengthen the system against future attacks.. (Fig.1).

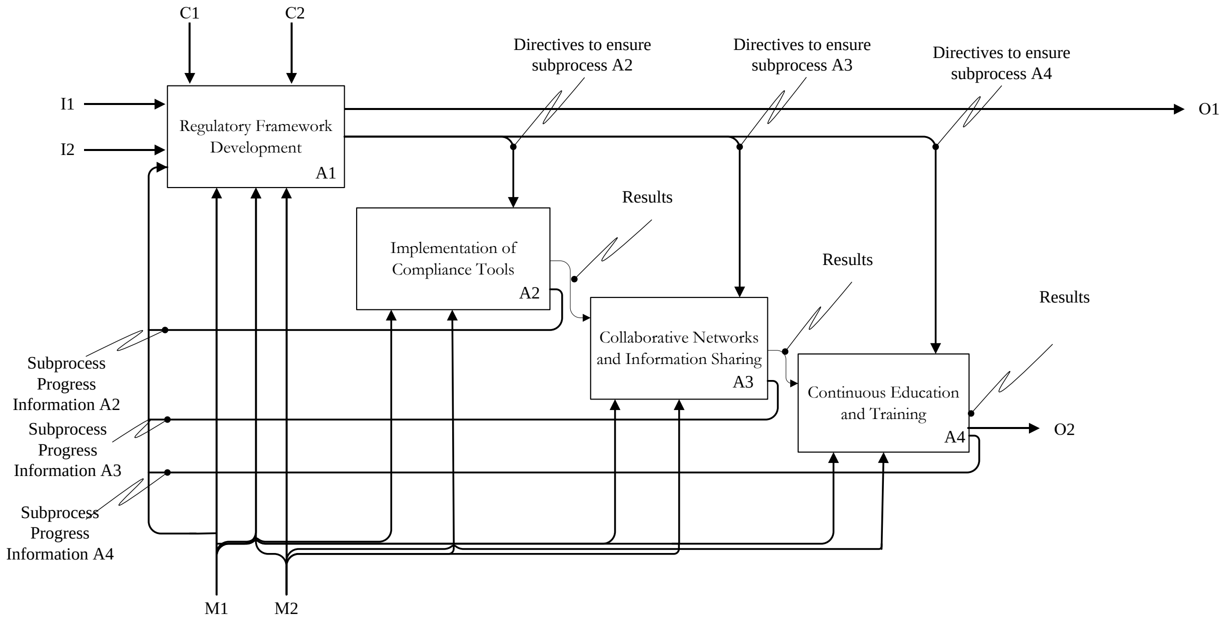
C1
C2
Directives to ensure subprocess A2
Directives to ensure subprocess A3
Directives to ensure subprocess A4
I1
I2
O1
Regulatory Framework Development
A1
Implementation of Compliance Tools
A2
Results
Collaborative Networks and Information Sharing
A3
Results
Results
Continuous Education and Training
A4
O2
Subprocess Progress Information A2
Subprocess Progress Information A3
Subprocess Progress Information A4
M1
M2

Figure 1. The first IDEF0 model

Source: own analysis

Lets build second IDEF model:

B1. Regulatory Framework Development. Establish a comprehensive set of regulations that mandate stringent cybersecurity measures for AI systems, particularly those handling environmental data.

B2. Implementation of Compliance Tools. Develop and implement tools that help organizations comply with these new regulations, ensuring that all AI systems are secure and their outputs are reliable.

B3. Collaborative Networks and Information Sharing. Foster a culture of collaboration and information sharing among organizations, governments, and cybersecurity experts to enhance collective defense against AI-based threats.

B4. Continuous Education and Training. Ensure that the workforce, from IT professionals to executive management, is well-educated about the risks associated with AI and the importance of compliance with cybersecurity practices. (Fig.2).

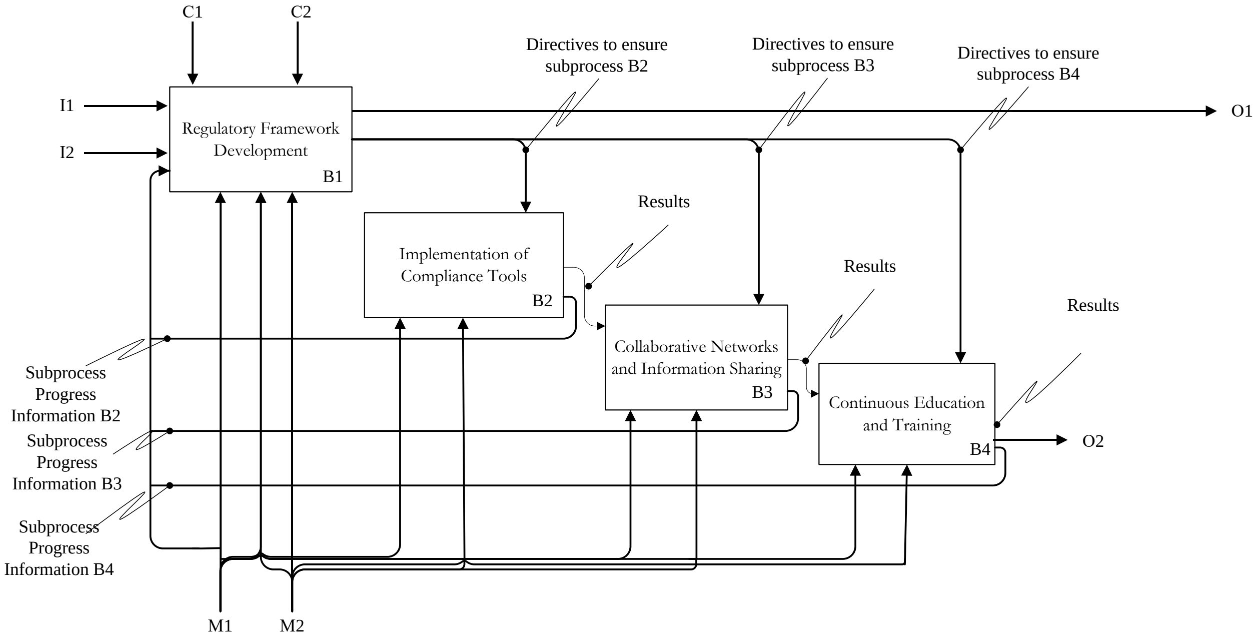
C1
C2
Directives to ensure subprocess B2
Directives to ensure subprocess B3
Directives to ensure subprocess B4
I1
I2
O1
Regulatory Framework Development
B1
Results
Implementation of Compliance Tools
B2
Results
Collaborative Networks and Information Sharing
B3
Results
Continuous Education and Training
B4
O2
Subprocess Progress Information B2
Subprocess Progress Information B3
Subprocess Progress Information B4
M1
M2

Figure 2. The second IDEF0 model

Source: own analysis

Ultimately, the utility of IDEF0 in enhancing cybersecurity lies in its structured approach to problem-solving. By methodically breaking down processes and identifying their key elements, IDEF0 enables organizations to develop targeted strategies to fortify their defenses against AI-driven fraud. This is particularly important for protecting environmental data, ensuring that decisions based on this data are accurate and truly reflective of real-world conditions, thus preserving the integrity of environmental policies and actions.

Discussions

Krupa et al. (2024) delve into the digital transformation of enterprise competitiveness through AI, emphasizing technical and technological support for personnel management . This study illustrates how AI integration into business processes can enhance operational efficiency but also introduces vulnerabilities that could be exploited for fraudulent activities, thereby impacting both economic security and environmental management.

Ravlinko et al. (2023) explore the formation, development, and use of human capital, specifically within the context of military conflicts . Their insights on personnel security underscore the broader implications of security management, where AI could either safeguard or compromise sensitive data, with significant repercussions for both human and environmental safety.

Saleh et al. (2020) focus on the legal aspects of managing cryptocurrency assets within national security frameworks . The intersection of AI, legal regulations, and cybersecurity as discussed provides a basis for understanding the potential environmental impacts, particularly if fraudulent activities lead to unregulated resource exploitation or violations of environmental laws.

Alkema et al. (2024) and Shtangret et al. (2021) present studies on managing weak signals in foreign economic activities and the practical aspects of anticipative management in economic security . These studies are pertinent as they highlight how AI can be utilized to detect early signs of economic distress, potentially caused by AI-based fraud, which indirectly affects environmental management through economic stability.

Shtangret et al. (2024) provide an extensive analysis of the impact of conflicts, like the war in Ukraine, on human and labor rights . This discussion is crucial in understanding how disruptions caused by conflicts—and potentially exacerbated by AI—can lead to severe environmental and human rights abuses.

Shakhatreh et al. (2023) discuss financial and economic security in the context of public-private partnerships aimed at ensuring commercial and legal development in regions . The integration of AI within these partnerships could enhance transparency and efficiency but also poses risks of fraud that could undermine environmental policies and regulations. Lastly, Sylkin et al. (2019) and Sylkin et al. (2018) explore the application of anti-crisis management in ensuring financial security of enterprises, highlighting the role of assessing financial security as a precondition for effective crisis management . These perspectives are essential, as financial instability caused by AI-based fraud could divert resources away from environmental protection efforts.

Conclusions

Ensuring cybersecurity in the modern world, especially with the rise of artificial intelligence (AI)-based fraud, involves addressing a range of complex challenges that span economic, social, and environmental issues. The potential for AI-based fraud to impact the environment is significant, manifesting through various mechanisms such as manipulation of environmental data, fraudulent activities in carbon credit markets, and cyber-attacks on critical infrastructure.

AI's ability to analyze and manipulate large datasets can be exploited to alter environmental monitoring data. Companies could use sophisticated AI algorithms to falsify pollution levels or emission reports, misleading regulatory bodies and leading to incorrect environmental policy decisions and significant ecological harm.

Carbon trading schemes, essential for combating climate change, are vulnerable to AI-based fraud. Unscrupulous entities might use AI to create false reports of carbon emissions reductions from non-existent or underperforming projects. This undermines the integrity of carbon markets and allows for higher emissions than ecosystems can sustain.

AI-based fraud could also affect the financial models of renewable energy projects by manipulating energy production data or falsifying the efficiency of renewable technologies. Such activities could attract investments under false pretenses, leading to misallocated resources and potentially stalling the transition to clean energy.

Critical infrastructure such as water treatment facilities, nuclear plants, and energy grids can be targets of AI-enhanced cyber-attacks. Compromises in safety and operational data could lead to environmental disasters, including oil spills, nuclear accidents, or widespread pollution.

AI can facilitate illegal resource extraction, such as unauthorized logging or mining, by being used to forge permits, alter land records, or disguise illegal activities as legitimate operations. This can cause significant environmental degradation.

References

Alazzam, F. A. F., Tubishat, B. M. A.-R., Savchenko, O., Pitel, N., & Diuk, O. (2023). Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. Business: Theory and Practice, 24(2), 594–603. https://doi.org/10.3846/btp.2023.19781

Alazzam, F. A. F., Tubishat, B. M. A.-R., Storozhuk, O., Poplavska, O., & Zhyvko, Z. (2024). Methodical approach to the choice of a business management strategy within the framework of a change in commercial activities. Business: Theory and Practice, 25(1), 1–10. https://doi.org/10.3846/btp.2024.19676

Alazzam, F.A.F., Aldrou, K.K.A.R., Berezivskyy, Z., Zaverbnyj, A., Borutska, Y. (2023). State management of the system of rational environmental use in the context of commercial development of the bioeconomy: Ecological aspect. International Journal of Environmental Impacts, Vol. 6, No. 4, pp. 155-163. https://doi.org/10.18280/ijei.060401

Alazzam, F.A.F., Salih, A.J., Amoush, M.A.M., Khasawneh, F.S.A. (2023). The nature of electronic contracts using blockchain technology - Currency bitcoin as an example. Revista De Gestão Social E Ambiental, 17(5): e03330. https://doi.org/10.24857/rgsa.v17n5-014

Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. Ingénierie des Systèmes d'Information, Vol. 28, No. 4, pp. 969-974. https://doi.org/10.18280/isi.280417

Alkema, V., Hryhoruk, P., Skhidnytska, H., Senyk, S. Mykytyn O. Managing Weak Signals In The Foreign Economic Activity of a Modern Enterprise: Preventing a Decrease in the Financial and Economic Security with a Strategic Approach to Solving the Problem. International Journal of Economics and Finance. Vol. 5. № 9. 2024. S. 1062-1071. https://ijor.co.uk/ijor/article/view/5067/2621

Al-Maagbeh, M. M., Rabbo Aldrou, K. K. A., Al-Naimat, O., & Sylkin, O. (2024). Historical approaches to the development of administrative law in Jordan in the period 1970-2024: From the modernization of public administration to the use of artificial intelligence. Clio. Journal of History, Human Sciences and Critical Thought., (8), 52-72. https://doi.org/10.5281/zenodo.12597931

Bani-Meqdad, M.A.M., Senyk, P., Udod, M., Pylypenko, T., Sylkin, O. (2024). Cyber-environment in the human rights system: Modern challenges to protect intellectual property law and ensure sustainable development of the region. International Journal of Sustainable Development and Planning, Vol. 19, No. 4, pp. 1389-1396. https://doi.org/10.18280/ijsdp.190416

Blikhar, M., Vinichuk, M., Kashchuk, M., Gapchich, V., Babii , S. (2023). Economic and legal aspects of ensuring the effectiveness of counteracting corruption in the system of anti-corruption measures of state authorities. Financial and Credit Activity Problems of Theory and Practice, 4(51): 398-407. https://doi.org/10.55643/fcaptp.4.51.2023.4138

Hisham Jadallah Mansour Shakhatreh, Farouq Ahmad Faleh Alazzam, Kalyayev, A., Kohut, P., Skhidnytska, H., Krymchak L., Financial and Economic Security in the Context of Public-Private Partnership to Ensure the Commercial and Legal Development in the Region. Review of Economics and Finance. Vol. 21. 2023. S. 2706-2712

Kopytko, M., & Sylkin, O. (2023). Modelling information support for combating corruption in the economic security management system of the state. Social and Legal Studios, 6(3), 60-66. https://doi.org/10.32518/sals3.2023.60

Krupa, V., Oliinyk, I., Bazaka, R., Shtangret, A., Sylkin, O. Technical And Technological Support for Personnel Management: Digital Transformation of Enterprise Competitiveness Through Artificial Intelligence. (2024). International Journal of Religion, 5(11), 260-270. https://doi.org/10.61707/d400cc80

Ravlinko Z. Shliakhetko V., Motorniuk U., Petrukha N., Pawera R. (2023) Formation, development and use of human capital: aspects of personnel security in a military conflict. International Journal of Services, Economics and Management, 2023 Vol.14 No.4, pp.452 - 466. https://dx.doi.org/10.1504/IJSEM.2023.134125

Saleh, A.J., Alazzam, F.A.F., Aldrou, K.K.A.R., Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. Journal of Security and Sustainability Issues, 10(1): 235-247. https://doi.org/10.9770/jssi.2020.10.1(17)

Shtangret, A., Topalova, E., Polovcev, O., Chornenka, O., & Musiyovskyi, A. (2021). Practical aspects of the use of antisipative management in the process of ensuring the economic security of an enterprise. Business: Theory and Practice, 22(1), 202-210. https://doi.org/10.3846/btp.2021.13556

Shtangret, A., Volodymyr, B., Berest, I., & Baran, I. (2024). Beyond the Battlefield: The War in Ukraine and its Protracted Impact on Human and Labor Rights. Detailed Analysis of Crimes Against Humanity in the Context of Human Capital Management (2014-2023). Clio. Journal of History, Human Sciences and Critical Thought., (8), 369-386. https://doi.org/10.5281/zenodo.12600819

Skhidnytska H., Digital Technologies Planning of Commercial Activity and Optimization of Processes for Open Socio-Economic Systems: Financial and Legal Aspect. (2024). International Journal of Religion, 5(11), 2160 – 2166. https://doi.org/10.61707/9y1vy754

Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., & Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. Business: Theory and Practice, 20, 446-455. https://doi.org/10.3846/btp.2019.41

Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: Practical aspect. Business and Economic Horizons, 14(4): 926-940. https://doi.org/10.15208/beh.2018.63