BUSINESS ETHICS AND IT PROJECT MANAGEMENT IN THE PROCESS OF UKRAINE'S POST-WAR RECOVERY

Sergey Rybak[1], Oleksandr Burkovskyi[2], Yevhenii Burkovskyi[3]

[1]Doctor of Science (Economics), Docent, senior researcher, Professor of the Department of Public Administration, Management and Inclusive Economy, Educational and Rehabilitation Institution of Higher Education "Kamyanets-Podil State Institute", Ukraine, ribaks@ukr.net ORCID: https://orcid.org/0009-0000-9251-1438

[2]PhD student, College of international business, Preshov, Slovakia, e-mail: alexburkov2017@gmail.com; ORCID: https://orcid.org/0009-0006-6057-7524

[3]PhD student, College of international business, Preshov, Slovakia, e-mail: yevheniiburkovskyi@gmail.com; ORCID: https://orcid.org/0000-0003-1867-9421

Citation:
Rybak, S., Burkovskyi, O., & Burkovskyi, Y. (2024). Business Ethics and IT Project Management in the Process of Ukraine's Post-War Recovery. *Economics, Finance and Management Review*, (4(20), 53–67.
https://doi.org/10.36690/2674-5208-2024-4-53-67

Received: December 01, 2024
Approved: December 28, 2024
Published: December 30, 2024

Abstract. *Considering Ukraine's course towards European integration and the rapid progress in digital technologies, there is a pressing need to modernize the financial, legal, and economic regulation of the digital economy, ensure the free flow and proper protection of data, and systematize ethical principles in business and effective IT project management to meet modern requirements and international standards. The purpose of the study is to analyze the significance of ethical principles in business and effective IT project management during the post-war recovery of Ukraine. To achieve this goal, various scientific analysis methods were employed, including systematization, systems analysis, logical analysis, synthesis, generalization, comparative analysis, modeling, structural, and functional analysis. The study highlights key aspects of applying ethical norms in the activities of companies implementing digital initiatives aimed at rebuilding critical infrastructure, strengthening cybersecurity, and advancing digital technologies. It examines the impact of ethical standards on managerial decision-making in the field of information technology. Additionally, the research addresses cybersecurity issues as one of the priority components of the post-war recovery and digital transformation of the country. The practical significance of the conducted research lies in the fact that the conclusions and recommendations developed by the author and proposed in the article can be utilized for: developing strategies to improve ethical standards in the management of IT projects; implementing effective mechanisms for managerial decisions in the field of digital initiatives aimed at restoring critical infrastructure and strengthening cybersecurity; enhancing the efficiency of management practices in the context of Ukraine's post-war recovery. Further research may focus on improving the methodology for assessing the impact of ethical standards on the efficiency of IT project management, particularly in the context of digital initiatives and innovations.*

Keywords: *IT projects, business ethics, post-war recovery, management technologies, cybersecurity.*

JEL Classification: H 55; H56; M 15

Formulas: 0, fig.: 1, tabl.: 2, bibl.: 33

Introduction. The post-war recovery of Ukraine presents a unique and critical opportunity to rebuild the nation's infrastructure, economy, and social fabric. Among the key drivers of this recovery is the effective management of IT projects, which play a pivotal role in fostering innovation, efficiency, and modernization across various sectors. However, the success of these initiatives hinges not only on technical expertise but also on adherence to strong business ethics.

In the context of Ukraine's recovery, business ethics and IT project management are deeply intertwined, as ethical considerations guide decision-making processes, ensure accountability, and promote equitable development. Ethical project management practices are essential for building trust among stakeholders, mitigating risks, and ensuring that resources are utilized transparently and responsibly. These factors are particularly critical in a post-war environment, where trust in institutions, equitable resource distribution, and sustainable development are paramount.

Literature Review. Digital technologies have become a fundamental driver of transformation in the modern world, ensuring the functionality of government institutions, the private sector, civil society, and individual lifestyles. The integration of digital infrastructure into all aspects of societal development necessitates its systematic protection to ensure societal resilience, economic stability, and the efficient functioning of critical infrastructure objects (E-Governance Academy, 2022; Petrukha et al., 2024b; Kotlyrevskiy et al., 2022).

The development and implementation of digital technologies in various fields introduce new challenges, particularly in cybersecurity and the ethical management of information resources. Responsibility for ensuring cybersecurity resilience is shared among the state, the corporate sector, the scientific community, and civil society. Consequently, special attention must be paid to forming an integrated approach to managing cyber threats, which includes international cooperation, intergovernmental interaction, and the use of innovative strategies to minimize risks associated with cybercrime (Kruhlov et al., 2020; Petrukha et al., 2024a).

The digitization of society has become a key driver of economic growth and social modernization. However, it simultaneously increases risks associated with attacks on critical infrastructure, targeting telecommunications, transportation, energy networks, and other systems whose disruption can lead to significant socio-economic losses. The essence of critical infrastructure lies in ensuring the functional continuity of societal processes, and its destruction creates global challenges for public safety and economic stability (Albahar, 2019; Petrukha et al., 2024c).

The ethical dimension of IT project management plays a fundamental role in building transparent processes, reducing corruption risks, and strengthening trust in digital services. Companies adhering to high ethical standards demonstrate higher levels of social responsibility, enhancing their reputation among partners and clients, while reducing reputational risks and ensuring long-term investment appeal (Rass et al., 2020; Kamara, Zemlinsky, 2024; Shubalii et al. , 2023; Ryzhakov et al., 2022; Chernyshov et al al., 2021).

The state plays a key role in creating the regulatory framework for the effective functioning of cybersecurity systems. In the context of digitalizing social and economic life, a primary task is fostering public trust in the safety of digital platforms used in

daily activities, which involves implementing cybersecurity standards that account for both technical and ethical aspects (E-Governance Academy, 2022).

Thus, during Ukraine's post-war recovery, implementing a systematic approach to IT project management based on ethical principles, international cooperation, and comprehensive measures to enhance cybersecurity is critically important. Only through close collaboration between the public and corporate sectors and civil society can the long-term resilience of digital infrastructure be ensured as a foundation for restoring socio-economic stability during Ukraine's post-war recovery (Albahar, 2019; Rass et al., 2020).

An analysis of contemporary scientific research highlights an urgent need to unify international ethical standards in business, driven by the global trend of economic digitalization. Universalizing ethical principles is critical for developing theoretical foundations of corporate governance, shaping sustainable economic models, and fostering socially responsible entrepreneurship. This issue has been addressed by prominent scholars such as M. Sandel, O. Maslov, K. Eiker, and R. Tou, who laid the groundwork for further exploration of the interconnection between ethics, innovation, and economic growth (Sandel, 2018; Maslov, 2011; Eiker, 2017; Tou, 2013).

The full-scale war in Ukraine has posed unprecedented challenges for the IT sector, a vital driver of economic and innovative development. Key issues include the reduction in the number of companies and qualified professionals, leading to risks of diminished industry competitiveness. IT service exports have declined significantly, while difficulties in maintaining business process stability during wartime have necessitated the reorientation of markets. Additionally, a significant portion of highly qualified workers has emigrated, limiting the country's technical potential. The increase in the number of self-employed individuals has complicated state control over compliance with legislative and tax requirements (NISS, 2023).

The digital transformation of businesses, as noted by H. M. Dergachova and Y. O. Koleshnya, is a multidimensional process encompassing the reorganization of organizational structures, implementation of innovative business models, expansion of consumer audiences, and transition to digital platforms (Dergachova, Koleshnya, 2020). S. Chapco-Wade and J. Bloomberg emphasize the cultural-behavioral and social aspects of the digital economy, which define the key parameters of its functioning and integration into modern socio-economic systems (Chapco-Wade, 2018; Bloomberg, 2018).

Particular attention in research has been given to cybersecurity issues. A. Omelchenko notes that ensuring cybersecurity is a strategic priority of Ukraine’s national security. The author highlights the growing number of cyber threats driven by advancements in information technologies and artificial intelligence (Omelchenko, 2022). O. Neretin and V. Kharchenko have classified major attack types and stressed the importance of standardizing the lifecycle of artificial intelligence systems (Neretin, Kharchenko, 2022). K. Movchan proposed a multi-level approach to cybersecurity, which includes threat analysis, the development of countermeasures, and strengthening encryption, authentication, and physical protection procedures to prevent unauthorized access and data loss (Movchan, 2023).

Although existing literature outlines individual aspects of business ethics and IT project management, integrating ethical principles into project management within the context of Ukraine's post-war recovery remains underexplored. Current works are predominantly theoretical and do not address practical aspects related to adapting management approaches to crisis conditions. Consequently, further research is critically important to develop effective mechanisms for ethical management in the context of post-war economic recovery and ensuring the resilience of Ukraine's IT sector.

Aims. The aim of this article is to analyze the significance of ethical principles in business and the effective management of IT projects during Ukraine's post-war recovery and to identify theoretical and practical aspects of applying business ethics principles to IT project management in this context.

Methodology. Achieving the research objective involves employing the following methods:

- *Systematization:* Identifying the main theoretical and practical aspects of business ethics and IT project management during Ukraine's post-war recovery.
- *Systemic and logical analysis with synthesis:* Establishing interconnections among elements of the studied processes and integrating key ideas to formulate comprehensive conclusions.
- *Generalization:* Analyzing the latest scientific publications on IT project management, cybersecurity, and business ethics.
- *Comparative method:* Differentiating between concepts, approaches, and strategies in forming the national cybersecurity system.
- *Structural and functional analysis:* Evaluating the structural elements of the national cybersecurity system.
- *Modeling:* Developing a model for integrating business ethics into IT project management during Ukraine's post-war recovery.

Results. Ethics, as a discipline studying the moral principles and norms of human behavior in society, forms the foundation for professional activities in the digital technology sector. It delineates morally right and wrong actions, as well as the behavioral standards to be adhered to in business, including IT project management. A code of ethics, a system of norms and principles, regulates professional behavior and contains rules that define the boundaries of acceptable and unacceptable conduct. It also provides recommendations for interactions with partners, clients, government authorities, and other stakeholders, ensuring transparency, integrity, and the protection of rights for all participants in the process (Sandel, 2018).

The relevance of applying ethical codes in the context of the digital economy's development stems from their role in regulating market relations and ensuring compliance with moral and legal requirements. Ethical codes help reduce the risk of conflicts and enhance trust in companies, which is particularly crucial for ensuring stability in the post-war period. They also contribute to protecting consumer rights, maintaining company competitiveness, and fostering long-term partnerships—essential elements for the effective implementation of recovery projects in Ukraine (Maslov, 2011).

Considering globalization and the necessity for international cooperation, it is important to create a unified foundation of ethical standards that regulate corporate behavior on a global level. Such integration of ethical norms promotes the development of international relations, ensuring transparency and efficiency in IT project implementation—critical for rebuilding infrastructure and advancing digital technologies in Ukraine (Eiker, 2017; Tou, 2013).

Ethical codes play a key role in ensuring the sustainability of organizations engaged in IT projects during Ukraine's post-war recovery. They serve as systems of norms and principles that facilitate sound and equitable decision-making. Specifically, according to G. Reynolds, ethical codes are strategic guidelines that ensure appropriate behavior in the professional realm, establishing clear boundaries between acceptable and unacceptable actions while emphasizing the significance of ethical responsibility as a foundation for decision-making, especially in situations where ethical standards may be at risk (Reynolds, 2003).

Adhering to ethical principles builds trust in organizations among all economic process participants, including state institutions, consumers, and international partners. This trust becomes the basis for stability in interactions at all stages of recovery, particularly in digital initiatives that promote the development of information and communication technologies and enhance national cybersecurity. Ethical codes also play an important role in self-assessment and monitoring the behavior of market participants, acting as mechanisms to uphold high standards of corporate social responsibility and operational transparency.

International experience demonstrates the effectiveness of ethical codes in regulating the activities of multinational corporations, which is significant for their adoption by national enterprises during digitalization. Organizations such as the World Trade Organization (WTO), the Organisation for Economic Co-operation and Development (OECD), and the European Union (EU) implement codes of conduct that regulate ethical standards at the international level. For instance, the OECD Guidelines for Multinational Enterprises define key principles related to human rights, labor protection, environmental conservation, and anti-corruption measures, all of which are critical for IT project management practices in Ukraine. According to research by consulting firm PwC, organizations with a strong ethical corporate culture are 12% less likely to face regulatory investigations and 24% less likely to encounter financial penalties compared to those that do not adhere to ethical standards (PwC, 2024).

The implementation of ethical codes in managing digital initiatives is a necessary component not only for ensuring the stable functioning of organizations in the IT sector but also for achieving long-term results in rebuilding the country's critical infrastructure after the war. Ethical codes not only enhance transparency and accountability but also lay the groundwork for forming strategic alliances with international partners, thereby ensuring sustainable development and global competitiveness for Ukrainian companies in the digital economy (Eiker, 2017).

Research on mitigating cyber threats is actively conducted in various countries worldwide. One significant area of such research involves defining the National Cyber Security Index (NCSI), which reflects a state's ability to counter cyber threats and effectively manage cyber incidents. The correlation between a country's level of digital

development and its capacity to combat cyber threats is presented in Table 1. In 2023, Ukraine ranked 24th with an index score of 75.32 among 176 countries, according to the relevant international ranking (EGA, 2023a; 2023b).

The analysis of cybersecurity indicators as of August 24, 2023, provides a comprehensive understanding of the country's capacity to effectively respond to cyber threats and its readiness to protect information infrastructure. According to the data in Table 1, Ukraine's national cybersecurity policy scored high in areas such as the presence of specialized units responsible for developing and implementing cybersecurity strategies. Overall, the cybersecurity policy development index, measured by the presence of relevant strategies and plans, reached 80%. However, the number of publications on cyber threats remains low, indicating the need to improve reporting and communication policies in this field.

Regarding basic cybersecurity indicators, Ukraine has made progress in protecting critical infrastructure, but the current stage reveals a limited number of regulatory acts and standards for ensuring national-level cybersecurity. The protection system for essential services like energy and transportation in Ukraine is still under development, necessitating stronger national cybersecurity standards and their integration into the public sector to enhance resilience against cyber threats.

Cyber incident response in Ukraine is managed by specialized units, but comprehensive national-level crisis management plans are lacking. Ukraine should improve its preparedness for crisis situations by developing more effective response mechanisms and participating in international cyber crisis training to enhance resilience against global cyber risks. The fight against cybercrime in Ukraine is advancing through legislative initiatives and the establishment of specialized digital forensic units, but the country still lacks a fully developed system to combat cybercrime. In the realm of military cyber operations, Ukraine has gaps in the development of specialized units to conduct cyber operations at the national defense level. Participation in international cyber operations and training is limited, underscoring the need to strengthen collaboration with international partners to improve military cyber operations (Table 1).

Table 1. Assessment of the 2023 National Cyber Security Index (NCSI) by Key Indicators (version August 24, 2023)

Indicator	Rating	Rating (%)
General cybersecurity indicators		
1. Cybersecurity policy development	7	100%
1.1. Presence of a cybersecurity policy unit	3	–
1.2. Cybersecurity policy coordination format	2	–
1.3. Cybersecurity strategy	1	–
1.4. Cybersecurity strategy implementation plan	1	–
2. Cyber threat analysis and information	4	80%
2.1. Cyber threat analysis unit	3	–
2.2. Publication of annual cyber threat reports	0	–
2.3. Presence of a cybersecurity and protection website	1	–
3. Education and professional development	8	89%
3.1. Cybersecurity competencies in general education institutions	0	–
3.2. Cybersecurity bachelor's program	2	–
3.3. Cybersecurity master's program	2	–
3.4. Cybersecurity doctoral program	2	–
3.5. Professional Cybersecurity Association	2	–

Indicator	Rating	Rating (%)
4. Contribution to Global Cybersecurity	2	63%
4.1. Convention on Cybercrime	1	–
4.2. Representation in International Cooperation Formats	1	–
4.3. International Cybersecurity Organization Located in the Country	0	–
4.4. Capacity Building in Cybersecurity for Other Countries	0	–
Cybersecurity Core Indicators		
5. Protection of Digital Services	1	20%
5.1. Cybersecurity Responsibilities of Digital Service Providers	1	–
5.2. Cybersecurity Standard for the Public Sector	0	–
5.3. Competent Supervisory Authority	0	–
6. Protection of Critical Services	6	100%
6.1. Identification of Critical Service Operators	1	–
6.2. Cybersecurity Requirements for Critical Service Operators	1	–
6.3. Competent Supervisory Authority	3	–
6.4. Regular Monitoring of Security Measures	1	–
7. Electronic Identification and Trust Services	9	100%
7.1. Unique persistent identifier	1	–
7.2. Requirements for cryptosystems	1	–
7.3. Electronic identification	1	–
7.4. Electronic signature	1	–
7.5. Time stamp	1	–
7.6. Electronic registered delivery service	1	–
7.7. Competent supervisory authority	3	–
8. Data protection	4	100%
8.1. Data protection legislation	1	–
8.2. Data protection authority	3	–
Indicators for incident response and crisis management		
9. Cyber incident response	4	67%
9.1. Cyber incident response unit	3	–
9.2. Responsibility for reporting	1	–
9.3. Single point of contact for international coordination	0	–
10. Cyber crisis management	3	60%
10.1. Cyber crisis management plan	0	–
10.2. National cyber crisis exercises	2	–
10.3. Participation in international cyber crisis exercises	1	–
10.4. Operational support of volunteers in cyber crises	0	–
11. Combating cybercrime	9	100%
11.1. Cybercrimes are criminalized	1	–
11.2. Cybercrime Unit	3	–
11.3. Digital Forensics Unit	3	–
11.4. 24/7 Contact Point for International Cybercrime	2	–
12. Military Cyber Operations	1	67%
12.1. Cyber Operations Unit	0	–
12.2. Cyber Operations Training	0	–
12.3. Participation in International Cyber Science Training	1	–

Source: Compiled by the authors based on the source (NCSI, 2023a).

Overall, the analysis of cybersecurity indicators in Ukraine demonstrates a high level of readiness in specific areas, such as the development of national cybersecurity strategies and the protection of critical infrastructure. However, it highlights the need for improvements in international cooperation, reporting, and the development of specialized structures to combat cybercrime and conduct cyber operations at the international level.

In the current conditions of rapid digitalization and evolving cyber threats, national cybersecurity assumes strategic importance for ensuring state stability, given

numerous challenges, including war and the globalization of information technologies. The country's overall cybersecurity index is 80.83% among 57 countries in 2023, reflecting progress in this direction. The most advanced area in ensuring cybersecurity is policy and legal regulation, demonstrating a high level of achievement—100%, indicating an effective national strategy focused on adapting international standards and ensuring regulatory compliance with the demands of the modern digital environment. However, an examination of Ukraine's participation indices in global initiatives, such as international cybersecurity platforms, shows that the country has a limited influence on shaping global standards, which may reduce the effectiveness of intergovernmental cooperation.

The indicator for cybersecurity education development stands at 60%, indicating a low level of integration of cybersecurity into general educational programs, particularly at the basic education level. Nevertheless, postgraduate education programs and specialized courses show significant progress. Research activities in the field of cybersecurity have achieved 100%, reflecting active participation by scientific institutions in developing innovative approaches to protecting digital infrastructure. Preventive cybersecurity measures demonstrate a relatively high level of implementation at 75%. However, the analysis reveals issues with meeting protection standards in critical infrastructure sectors, particularly in the public sector. The supply chain and cloud technology protection indicator, at 83%, indicates certain achievements, but this area requires further improvements due to growing risks from cyber threats in these domains.

The national cyber incident response system, according to the indicators, shows an effectiveness level of 64%, reflecting insufficient integration with international information systems, which complicates prompt interaction with other states and international organizations. Additionally, the crisis management indicator, assessed at 56%, points to significant gaps in developing crisis plans and conducting practical training for operational services. Nonetheless, due to high efficiency in combating cybercrime, where the performance level is 100%, Ukraine has made significant progress in addressing cybercriminal activities and employing digital forensics to solve these problems (see Table 2).

Table 2. Cybersecurity Indicators of Ukraine by the NCSI Index (Version of November 29, 2023)

No	Cybersecurity indicator	Actual indicator	Maximum indicator	%
National Cybersecurity Index of Ukraine				80,83%
STRATEGIC CYBERSECURITY INDICATORS				–
1.	Cybersecurity policy	15	15	100%
1.1.	High-level leadership in cybersecurity	3	3	–
1.2.	Cybersecurity policy development	3	3	–
1.3.	Cybersecurity policy coordination	3	3	–
1.4.	National cybersecurity strategy	3	3	–
1.5.	Action plan for the implementation of the national strategy	3	3	–
2.	Global contribution to cybersecurity	4	6	67%
2.1.	Engagement in cyberdiplomacy	3	3	–
2.2.	Commitment to international law in cyberspace	1	1	–
2.3.	Contribution to international capacity building	0	2	–
3.	Education and professional development	6	10	60%

No	Cybersecurity indicator	Actual indicator	Maximum indicator	%
3.1.	Cyber competences in primary education	0	2	–
3.2.	Cyber competences in secondary education	0	2	–
3.3.	Basic cybersecurity education	2	2	–
3.4.	Postgraduate cybersecurity education	3	3	–
3.5.	Association of cybersecurity professionals	1	1	–
4.	Cybersecurity research and development	4	4	100%
4.1.	Research and development programs	2	2	–
4.2.	Doctoral studies in cybersecurity	2	2	–
PREVENTIVE CYBERSECURITY INDICATORS				–
5.	Cybersecurity of critical information infrastructure	9	12	75%
5.1.	Identification of critical information infrastructure	3	3	–
5.2.	Requirements for critical infrastructure operators	3	3	–
5.3.	Requirements for public sector organizations	0	3	–
5.4.	Competent supervisory authority	3	3	–
6.	Cybersecurity of digital enablers	10	12	83%
6.1.	Secure electronic identification	2	2	–
6.2.	Electronic signature	2	2	–
6.3.	Trust services	2	2	–
6.4.	Trust services supervisory authority	2	2	–
6.5.	Requirements for cloud services	2	2	–
6.6.	Cybersecurity of supply chains	0	2	–
7.	Cyber threat analysis and awareness raising	9	12	75%
7.1.	Cyber threat analysis	3	3	–
7.2.	Public cyber threat reports	3	3	–
7.3.	Awareness raising resources	3	3	–
7.4.	Coordination of awareness raising	0	3	–
8.	Personal data protection	4	4	100%
8.1.	Personal data protection legislation	2	2	–
8.2.	Personal data protection authority	2	2	–
RESPONSIVE CYBERSECURITY INDICATORS				–
9.	Cyber Incident Response	9	14	64%
9.1.	National Response Capability	3	3	–
9.2.	Incident Reporting Obligations	3	3	–
9.3.	Incident Reporting Tool	0	2	–
9.4.	Single Point of Contact for International Cooperation	0	3	–
9.5.	Participation in International Response Cooperation	3	3	–
10.	Cyber Crisis Management	5	9	56%
10.1.	Cyber Crisis Management Plan	0	2	–
10.2.	National Cyber Crisis Exercises	3	3	–
10.3.	Participation in International Exercises	2	2	–
10.4.	Operational Crisis Reserve	0	2	–
11.	Fighting Cybercrime	16	16	100%
11.1.	Criminalization of Cybercrime	3	3	–
11.2.	Procedural Law	3	3	–
11.3.	Cybercrime Convention	2	2	–
11.4.	Cybercrime Investigation Capability	3	3	–
11.5.	Digital Forensics Capability	2	2	–
11.6.	24/7 Contact Point	3	3	–
12.	Military Cyber Defense	6	6	100%
12.1.	Military Cyber Defense Capability	2	2	–
12.2.	Military Cyber Doctrine	2	2	–
12.3.	Military Cyber Defense Training	2	2	–

Source: Compiled by the authors based on the source (NCSI, 2023b).

The assessment of cybersecurity in Ukraine highlights positive progress in the development of policies, education, and research activities, as well as in combating cybercrime. However, there are certain imbalances in other areas, such as responding

to cyber threats, protecting critical infrastructure, and integrating international experience. To achieve higher cybersecurity standards, it is necessary to enhance cross-sectoral coordination, optimize educational initiatives, and integrate Ukraine into international cybersecurity platforms.

Amid the Russian Federation's military aggression, Ukraine faces an urgent need to restore damaged infrastructure and territories. This task can only be realized through a systematic approach, which involves the development and implementation of strategic programs and projects aimed at national recovery. According to the Decree of the President of Ukraine dated April 21, 2022, No. 266/2022, the National Recovery Council of Ukraine has developed a comprehensive plan of measures that includes priority reforms and strategic initiatives for effective post-war recovery. Among the primary sources of funding for restoration efforts are confiscated Russian assets, which should serve as the basis for large-scale investments in rebuilding housing, transportation infrastructure, and other critically important facilities (National Council, 2024).

However, the high level of funding required for infrastructure restoration may pose additional risks to public administration, particularly in the form of the resurgence of corruption schemes that existed before the war. To prevent such negative consequences, it is essential to ensure effective control over resource utilization and to continuously monitor the rebuilding process through mechanisms that promote transparency. One of the primary tools for achieving this is the use of modern IT technologies. Implementing the Earned Value Method (EVM) in project management will enable clear tracking of progress and financial flows, which are crucial aspects for ensuring transparency and efficiency in restoration efforts (Molokanova, 2023).

For the post-war recovery process to succeed, adequate institutional support from the state is also required. In the context of active international cooperation, particularly in the realm of technical assistance, it is important to establish mechanisms that ensure effective resource allocation and focus on tangible investments rather than just consulting services and training. Furthermore, clear criteria for evaluating the effectiveness of projects and programs implemented within the framework of international technical assistance must be established. This will optimize resource utilization and ensure that the implemented initiatives align with Ukraine's socio-economic development priorities.

One significant achievement in the recovery process is the creation of the state electronic ecosystem DREAM (Digital Restoration Ecosystem for Accountable Management). This platform allows monitoring of all stages of recovery—from registering damaged objects to financing, procurement, and construction work execution. The system will promote transparency and enable public oversight of project implementation, access to reports, and monitoring of restoration progress. Additionally, the DREAM platform allows local authorities to initiate specific reconstruction projects in accordance with developed strategies and plans, ensuring the integration of strategic and tactical management in Ukraine's recovery process (DREAM, 2023).

We consider it necessary to develop and implement a model for integrating business ethics into IT project management, which serves as the foundation for creating

an effective strategy for managing digital initiatives during Ukraine's post-war recovery. This model includes the introduction of an ethical standards system at all stages of the IT project lifecycle, ensuring not only the successful implementation of projects but also adherence to high moral principles in the field of digital technologies, which are critical for the resilience of the country's economic and social infrastructure. Given the post-conflict recovery context, ethical IT project management is particularly significant as it fosters both innovation and public trust in new digital services.

The model involves the development and implementation of clear ethical norms that regulate the activities of all participants in IT projects. The main principles include transparency, accountability, honesty, data confidentiality, and respect for human rights. These principles should be reflected in all aspects of IT project management, from planning to completion, thereby promoting business ethics and corporate social responsibility during post-war recovery.

Developing a strategy for integrating ethics into IT project management requires a systematic approach throughout all stages of the project lifecycle. A key component of the model involves practical mechanisms for integrating ethics and monitoring the performance indicators of ethical management. The main indicators may include:

– the level of trust among stakeholders (citizens, businesses, partners) in the implemented IT projects;

– reduction in conflicts of interest and violations during project execution;

– improvement in project outcomes quality, driven by the integration of ethical standards into project management.

For effective implementation of the model, close cooperation among government bodies, the corporate sector, international partners, academic institutions, and civil society is necessary. Such collaboration facilitates the integration of ethical standards into national cybersecurity and digital transformation policies, which are essential for post-conflict recovery. The interaction between the state and businesses contributes to creating a favorable environment for developing ethical norms in the IT and digital services sectors (Fig. 1).

It is worth noting that the integration of business ethics into IT project management is a critical component of Ukraine's post-war recovery process. Implementing this model will enable the creation of effective, sustainable, and ethically sound management of digital initiatives, thereby contributing to the development of the national economy and society amidst global digital transformations.

Thus, Ukraine’s post-war recovery requires a comprehensive approach that includes not only funding but also effective organization of management processes, utilization of modern technologies, and ensuring transparency at all stages of reconstruction. A vital element of this process is business ethics and IT project management, which must become the foundation for the successful implementation of the post-war recovery and development strategy.

Discussion. The research results demonstrated that ethical norms and corporate culture are crucial for the successful management of IT projects, particularly in the context of restoring critical infrastructure and developing digital technologies in post-war Ukraine. The application of ethical standards helps mitigate risks related to corruption and fraud, which are critical for attracting investments and maintaining

economic stability.

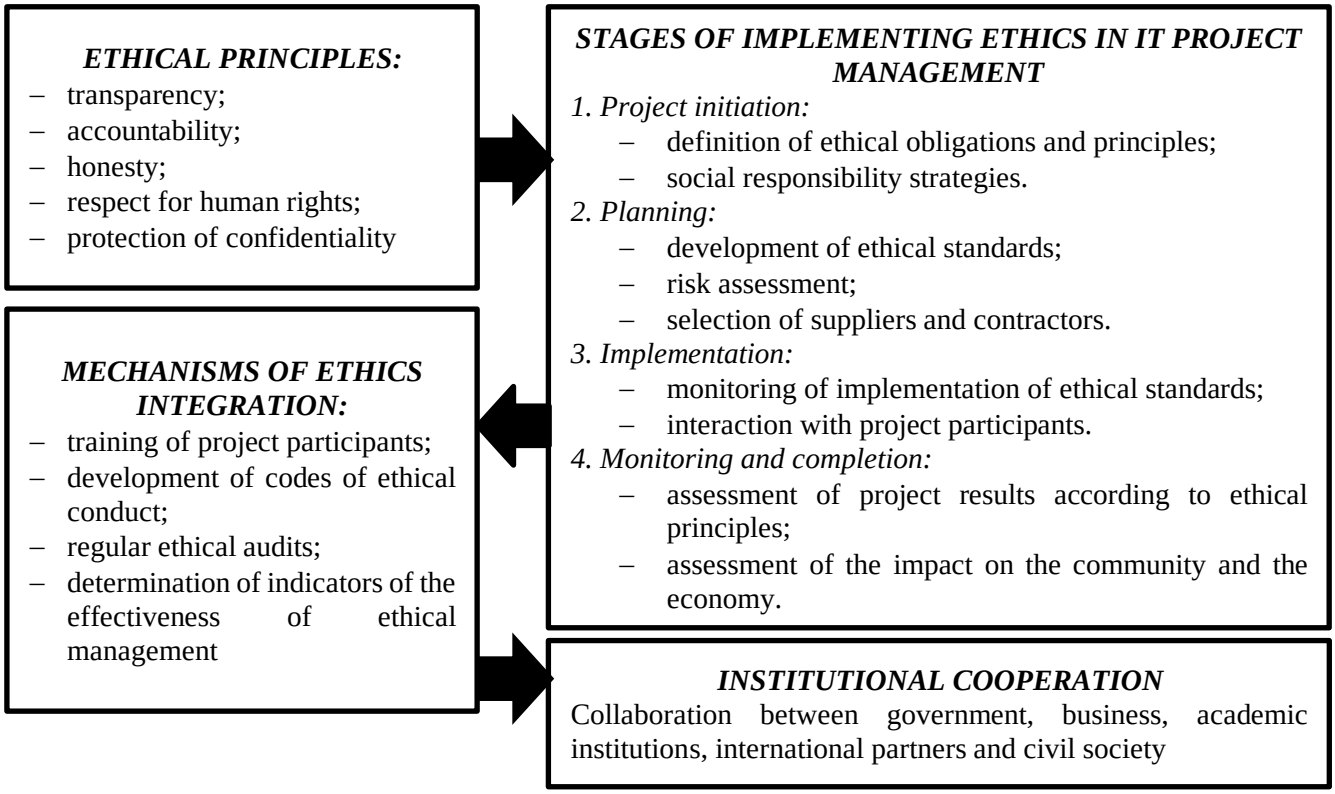

Figure 1. Model of Integrating Business Ethics into IT Project Management

Source: Compiled by the authors

Post-war recovery in Ukraine necessitates the integration of advanced technologies and digital innovations to rebuild critical infrastructure and enhance cybersecurity. Simultaneously, effective IT project management requires the adherence to high ethical standards by organizations involved in these initiatives. Ethics is an integral part of corporate culture, setting guidelines for decision-making and establishing behavioral norms that uphold organizational integrity and transparency. It helps reduce corruption and fraud, which is essential for creating a stable investment climate. The application of ethical norms in managerial decision-making within IT ensures transparency and process efficiency. Therefore, during post-war recovery, it is crucial to ensure that digital initiatives comply with ethical standards, particularly in aspects of data protection, information confidentiality, and cybersecurity.

Ethical principles also help prevent manipulations that could lead to negative consequences for companies and the state as a whole. Ethical leadership, characterized not only by personal examples set by management but also by the implementation of systematic corporate initiatives, is a significant factor in fostering an ethical culture. Company leaders who actively promote ethical principles create a favorable environment for professional development and mutual trust, with corporate social responsibility programs being a key component of this process.

One of the primary tools for ensuring ethical behavior is the development and implementation of ethical codes. These codes define the key principles that employees and leaders of an organization must follow, serving as a benchmark for self-monitoring

and evaluating compliance with ethical standards. On a global scale, many international organizations, such as the OECD, EU, and WTO, have developed ethical codes for their members, requiring adherence to principles related to human rights, environmental issues, and anti-corruption efforts. In this regard, it is worth emphasizing the importance of this aspect for companies seeking to enter international markets and attract investments.

Hence, the application of ethical principles in Ukraine's recovery process is vital for achieving sustainable development and strengthening trust among international partners and investors. The adoption of ethical codes, the promotion of ethical leadership, and the development of corporate social responsibility programs create favorable conditions for post-war reconstruction, reduce risks of corruption and fraud, and foster innovation in digital technologies. Thus, business ethics and IT project management are prerequisites for ensuring success in Ukraine's post-war recovery process (Kamara, Zemlinsky, 2024).

Based on the conducted research, it can be concluded that ethical standards must be integrated into IT project management strategies at all stages of implementation. This will not only ensure transparency and accountability in project management but also contribute to the sustainable development of digital initiatives, which is essential for Ukraine's recovery and modernization in the post-war period.

Conclusion. The study revealed several important aspects that confirm the need to integrate ethical standards into the process of information technology management in the post-war reconstruction. First, ethics is the basis for creating trusting relationships between all participants in IT projects, where the introduction of ethical codes into the process of IT project management helps ensure transparency, reduce corruption risks, and improve the corporate culture of enterprises engaged in the restoration of critical infrastructure.

Secondly, ethical leadership plays a special role in the process of IT project management. Company leaders who actively implement ethical principles become a driving force for creating an atmosphere of trust among employees and partners.

Third, the application of ethical standards in IT project management is important for the restoration of critical infrastructure and strengthening the country's cybersecurity. In the context of digitalization and globalization, ethics is becoming a key factor in ensuring the effective and sustainable development of infrastructure systems. Therefore, given the rapid development of technologies and changes in the socio-economic situation after the war, it is important to adapt ethical norms to new challenges, which will ensure effective management of IT projects and maintain high standards of corporate ethics.

Thus, it has been established that the integration of ethical norms into the processes of IT project management is a necessary condition for the successful recovery of Ukraine after the war. The application of ethics in IT project management allows not only to ensure stability in business processes, but also contributes to building trust from the public and international partners.

The practical significance of the study is that the conclusions and recommendations developed by the author and proposed in the article can be used for: developing strategies for improving ethical standards in the process of IT project

management; implementation of effective management decision-making mechanisms in the field of digital initiatives aimed at restoring critical infrastructure and strengthening cyber defense; increasing the effectiveness of management practices in the context of post-war reconstruction of Ukraine.

Further research may be aimed at improving the methodology for assessing the impact of ethical norms on the effectiveness of IT project management, in particular in the context of digital initiatives and innovations. Given current trends in digitalization, it is important to develop new approaches to integrating ethical principles into corporate governance strategies, which will ensure sustainable development in post-war reconstruction processes and reduce the risks of ethical violations in conditions of unpredictable changes. In addition, significant attention needs to be paid to studying the effectiveness of cyber defense mechanisms and digital security tools within the framework of ethical standards, which should contribute to reducing risks and increasing trust in digital platforms. In the context of globalization and rapid adaptation of new technologies, issues of data protection and transparency of processes are becoming particularly relevant for business and government agencies.

Author contributions. The authors contributed equally.

Disclosure statement. The authors do not have any conflict of interest.

References:

1. E-Governance Academy. (2022). *Upgrading National Cyber Resilience*. Tallinn: E-Governance Academy. Retrieved from https://ega.ee/wp-content/uploads/2021/05/NCSI-Cyber-Resilience-Digi_F.pdf
2. Kruhlov, V., Latynin, M., Horban, A., & Petrov, A. (2020). Public-private partnership in cybersecurity. *CEUR Workshop Proceedings*, (2654), 619–628.
3. Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Science and Engineering Ethics*, 25(4), 993–1006.
4. Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures*. Springer International Publishing.
5. Sandel, M. (2018). *Shcho take spravedlyvist? Spir pro moralni mezhi rynku* [What is justice? The debate on the moral limits of the market]. Kyiv: Dukh i Litera.
6. Maslov, O. V. (2011). Etyka v upravlinni biznesom: praktyka rozrobky etychnykh kodeksiv [Ethics in business management: Practice of ethical code development]. *Ekonomichnyi Chasopys-XXI*, 9-10(2), 52–56.
7. Eiker, K. (2017). *Kodeks povedinky dilovoi elity: Yak staty etychnym liderom v biznesi ta v zhytti* [Code of conduct for the business elite: How to become an ethical leader in business and life]. Kyiv: Vydavnycha Hrupa "Osnovy".
8. Tou, R. (2013). Korporatyvna sotsialna vidpovidalnist: kontseptualni pidkhody ta praktychna realizatsiia [Corporate social responsibility: Conceptual approaches and practical implementation]. *Visnyk Kyivskoho Natsionalnoho Universytetu Imeni Tarasa Shevchenka*, (147), 29–34.
9. NISD**.** (2023). Rynok pratsi IT-sektoru v umovakh viiny: realii ta perspektyvy [Labor market of the IT sector in wartime: Realities and prospects]. Retrieved from https://niss.gov.ua/news/komentari-ekspertiv/rynok-pratsi-it-sektoru-v-umovakh-viyny-realiyi-ta-perpektyvy
10. Dergachova, G. M., & Koleshnia, Ya. O. (2020). Tsyfrova transformatsiia biznesu: sutnist, oznaky, vymohy ta tekhnolohii [Digital business transformation: Essence, features, requirements, and technologies]. *Ekonomichnyi Visnyk NTUU "KPI" – Economic Bulletin of NTUU "KPI"*, 17, 280–290.
11. Chapco-Wade, C. (2018). Digitization, Digitalization, and Digital Transformation: What's the Difference? Retrieved from https://medium.com/@colleenchapco/digitizationdigitalization-anddigital-transformation-whats-thedifference-eff1d002fbdf
12. Bloomberg, J. (2018). Digitization, Digitalization, and Digital Transformation: Confuse Them at Your Peril. Retrieved from https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/?sh=89ee0042f2c7
13. Omelchenko, A. V. (2022). Orhanizatsiino-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Organizational and legal bases of cybersecurity of Ukraine]. *Kyivskyi Chasopys Prava*, (3), 140–145. https://doi.org/10.32782/klj/2021.3.22
14. Movchan, K. O. (2023). Ryzyky kiberbezpeky v epokhu robototekhniky [Cybersecurity risks in the age of robotics]. *Vcheni Zapysky TNU Imeni V. I. Vernadskoho. Seriia «Tekhnichni Nauky»*, 34(4), 79–83. https://doi.org/10.32782/2663-5941/2023.4/13

15. Neretin, O., & Kharchenko, V. (2022). Zabezpechennia kiberbezpeky system shtuchnoho intelektu: analiz vrazlyvostei, atak i kontrzakhodiv [Ensuring artificial intelligence systems cybersecurity: Analysis of vulnerabilities, attacks, and countermeasures]. *Visnyk Natsionalnoho Universytetu «Lvivska Politekhnika»*, (12), 7–22. https://doi.org/10.23939/sisn2022.12.007
16. Reynolds, G. (2003). *Ethics in information technology*. Toronto: Thomson.
17. PwC. (2024). Corporate culture and its impact on business performance. Retrieved from https://www.pwc.com/gx/en/services/workforce/organisational-culture-and-purpose.html
18. EGA. (2023a). Methodology. Retrieved from https://ncsi.ega.ee/methodology/
19. EGA. (2023b). National Cyber Security Index. Retrieved from https://ncsi.ega.ee/compare/
20. NCSI. (2023a). Archived data from 2016–2023. Retrieved from https://ncsi.ega.ee/country/ua_2022/
21. NCSI. (2023b). Ukraine. Retrieved from https://ncsi.ega.ee/country/ua/
22. Molokanova, V. (2023). Earned Value Method in Public Project Monitoring. In *Advanced, Contemporary Control - Proceedings of the XXI Polish Control Conference, PCC 2023, Gliwice, Poland, 26-29 June 2023, Volume 1* (pp. 86–102). Lecture Notes in Networks and Systems. Springer. https://doi.org/10.1007/978-3-031-35170-9_9
23. Natsionalna rada z vidnovlennia Ukrainy vid naslidkiv viiny. (2024). *Uriadovyi portal. Yedynyi veb-portal orhaniv vykonavchoi vlady Ukrainy*. Retrieved from https://www.kmu.gov.ua/diyalnist/konsultatyvno-doradchi-orhany/nacionalna-rada-z-vidnovlennya-ukrayini-vid-naslidkiv-vijni
24. DREAM – ekosystema upravlinnia vidbudovoiu infrastruktury. (2023). *Ministerstvo rozvytku hromad, terytorii ta infrastruktury Ukrainy*. Retrieved from https://promo.dream.gov.ua
25. Kamara, B. M., & Zemlynskyi, V. (2024). Rol' etyky ta dilovoi reputatsii, sformovanoi liudskym potentsialom, u dosiahnneni konkurentospromozhnosti pidpryiemstva [The role of ethics and business reputation, formed by human potential, in achieving enterprise competitiveness]. *Visnyk Khmelnytskoho Natsionalnoho Universytetu*, (5), 499–506. https://doi.org/10.31891/2307-5740-2024-334-75
26. Petrukha, N., Petrukha, S., Zhmayev, A., & Synkevych, M. (2024a). Kiberbezpeka ekonomiky ta derzhavnykh finansiv: istoriohrafiia ta povojenna traiektoriia rozvytku [Cybersecurity of the economy and public finances: Historiography and post-war development trajectory]. *Biznes Inform*, (7), 64–79. https://doi.org/10.32983/2222-4459-2024-6-64-79
27. Petrukha, N., Petrukha, S., Zhmayev, A., & Synkevych, M. (2024b). Tsyfrovyzatsiia ekonomiky ta derzhavnykh finansiv: suchasni tendentsii ta povojenna paradyhma [Digitalization of the economy and public finances: Current trends and post-war paradigm]. *Nauka i Tekhnika Siohodni*, 7(35), 152–172. https://doi.org/10.52058/2786-6025-2024-7(35)-152-172
28. Petrukha, N., Klymenko, K., & Petrukha, S. (2024c). Ekonomika ta derzhavni finansy – fenomen ukrainskoi nezlamnosti [Economy and public finances – the phenomenon of Ukrainian resilience]. *Vcheni Zapisky Universytetu "KROK"*, (2), 42–55. https://doi.org/10.31732/2663-2209-2024-74-42-55
29. Shubalii, O. M., Petrukha, S. V., Kosinskyi, P. M., & Petrukha, N. M. (2023). Formuvannia systemy informatsiino-analitychnoho zabezpechennia rozvytku biopalivnykh vyrobnytstv na bazi pidpryiemstv ahrosektoru [Formation of the information and analytical support system for the development of biofuel production based on agricultural enterprises]. *Naukovi Pratsi NDFI*, (3), 133–147. https://doi.org/10.33763/npndfi2023.03.133
30. Ryzhakov, D. A., Pokolenko, V. O., Petrukha, S. V., Ivakhnenko, I. S., Predun, K. M., Prykhodko, O. O., & Nikolaiev, H. V. (2022). Informatsiino-analitychni novatsii ta biznes-modeli upravlinnia pidpryiemstvom v suchasnii systemi budivelnoho developmentu [Information-analytical innovations and business management models in the modern construction development system]. *Upravlinnia Rozvytkom Skladnykh System*, (52), 103–112. https://doi.org/10.32347/2412-9933.2022.52.103-112
31. Akselrod, R. B., Trach, R. V., Chernyshov, D. O., Ryzhakov, D. A., Petrukha, S. V., & Khomenko, O. M. (2021). Innovatsiini napriamy onovlennia operatsiinykh system budivelnykh pidpryiemstv v umovakh nestabilnoho biznes-seredovyshcha proiektu [Innovative directions of updating operational systems of construction enterprises in an unstable business environment project]. *Upravlinnia Rozvytkom Skladnykh System*, (48), 102–113. https://doi.org/10.32347/2412-9933.2021.48.102-113
32. Chernyshov, D. O., Ryzhakov, D. A., Khomenko, O. M., Petrukha, S. V., Kucherenko, O. I., & Horbach, M. V. (2021). Tsyfrovi tekhnolohii yak innovatsiini trendy strukturno-transformatsiinykh zrushen u systemi upravlinnia pidpryiemstv-steikholderiv budivnytstva [Digital technologies as innovative trends in structural-transformational changes in the management system of construction stakeholder enterprises]. *Upravlinnia Rozvytkom Skladnykh System*, (46), 118–130. https://doi.org/10.32347/2412-9933.2021.46.118-130
33. Kotlyrevskiy, Y., Petrukha, S., Mandzinovska, Kh., Brynzei, B., & Rozumovych, N. (2022). Impact of modern information and communication technologies on economic security in the context of COVID-19. *International Journal of Computer Science and Network Security*, 22(1), 199–205. Retrieved from http://paper.ijcsns.org/07_book/202201/20220127.pdf