components in order to effectively achieve the specified properties; such a solution, ideally, should also be characterized by economical and environmental friendliness.

Thus, the main areas of research in this work are:

• selection of energy-saving synthesis for the necessary fillers;

• study of morphological features and functional characteristics;

• choice justification for matrices based on the study of polymer materials' properties;

• influence determination for the amount and nature of fillers' distribution on the characteristics of composites;

• establishment of fillers' influence on the complex of basic properties;

• composition optimization for composites to ensure broadband EM wave absorption;

• laboratory samples' manufacturing for products in the form of various configuration elements;

• practical recommendations for the research results.

CYBERSECURITY AS A STRATEGIC PRIORITY FOR UKRAINE'S INTEGRATION INTO THE EU DIGITAL SPACE

PhD student: Yevhenii Ippolitov
Research supervisor: DSc., Prof. Maryna Mashchenko
Department of Entrepreneurship, Trade and Logistics,
English language supervisor:
Associated Professor Natalya Turlakova,
Cross-Cultural Communication and Foreign Language Department
National Technical University "Kharkiv Polytechnic Institute"

Abstract. This article examines the important role of cybersecurity in Ukraine's integration into the EU digital space. It examines current challenges, harmonization of legislation with EU standards, and the impact of military aggression on cyber defense. The study highlights key European regulatory acts, Ukraine's national cybersecurity infrastructure, and international cooperation. Particular attention is paid to the importance of alignment with the NIS2 Directive and GDPR. Strengthening cybersecurity is presented as a critical factor in ensuring Ukraine's digital resilience and successful European integration.

Keywords: cybersecurity, EU integration, digital security, cyber threats, legislation, cooperation, critical infrastructure.

Introduction.

Topicality. In the modern world, cybersecurity plays a key role in the digital transformation of states and societies. For Ukraine, which is actively integrating into the European digital space, the issue of cyber protection has gained strategic importance. Given the growing number of cyber threats, especially under conditions of military aggression, an effective cybersecurity system is a prerequisite for the country's stable development. The European Union (EU) sets high cybersecurity standards, and their implementation is an important step for Ukraine's European integration. Therefore, the study of this topic is both relevant and necessary for understanding the challenges and prospects of cyber protection. With the development of digital technologies, the number of cyber threats is increasing, posing a danger to public institutions, businesses, and citizens. In times of war, Ukraine has become the target of constant cyberattacks, which requires strengthened security measures and international cooperation. Moreover, the EU imposes strict requirements on the protection of the digital space, and compliance with these standards is a key condition for Ukraine's integration. Improving cybersecurity will enhance national resilience and build trust in Ukraine as a partner. As a result, cybersecurity becomes one of the priority areas of state policy.

The object of the study is the measures taken to adapt to European standards.

The subject of the study is the process of Ukraine's integration into the EU digital space.

A significant number of researchers have addressed the issue of ensuring Ukraine's cybersecurity. For instance, explored the problems of the digital society related to cybersecurity and personal data protection in the EU [1]. Similarly, Zhurbynskyi D.A. and Kostenko V.O. analyzed the specifics of cybersecurity during martial law in Ukraine [2]. In turn, Mykytenko D.O. focused on information protection and cybersecurity in the context of Ukraine's national security [3]. However, certain aspects of cybersecurity in the process of Ukraine's integration into the EU digital space still require further clarification and development.

The purpose of the research is to determine the role of cybersecurity in Ukraine's integration into the EU digital space and to analyze the measures taken to adapt to European standards.

Presentation of the main research material.

It should be noted that cybersecurity plays a crucial role in Ukraine's European integration, as ensuring reliable digital protection is one of the EU's core requirements. Ukraine seeks to harmonize its legislation with European standards, which is an essential step toward digital integration. Furthermore, enhanced cyber protection fosters trust between Ukraine and its European partners, opening up opportunities for cooperation in digital economy and security. In addition, effective cybersecurity also helps protect critical infrastructure, public institutions, and citizens from cyberattacks – especially

relevant in times of war. Joint initiatives with the EU enable Ukraine to receive expert support, technological resources, and access to European cybersecurity platforms. Thus, integration into the EU digital space is impossible without establishing a robust cybersecurity system.

What is more important is that the EU's cybersecurity policy aims to create a resilient, safe, and secure digital space for all member states. One of the key documents is the NIS2 Directive, which sets cybersecurity requirements for critical infrastructure, businesses, and public institutions, obliging member states to implement high protection standards. Equally important is the General Data Protection Regulation (GDPR), which ensures the safety of personal data and imposes strict rules for its processing. The EU Agency for Cybersecurity (ENISA) coordinates cybersecurity efforts and provides support for building effective national systems.

To prevent cyber threats, the EU has adopted the European Cybersecurity Strategy, which focuses on enhancing cooperation among countries, improving response capabilities to cyberattacks, and protecting digital infrastructure. In 2023, the European Cyber Shield was launched to bolster defense against large-scale attacks and facilitate information exchange among member states. Moreover, the EU is actively developing the Digital Single Market, where data and information systems security is a top priority. Cooperation with third countries, including Ukraine, plays a crucial role in harmonizing cybersecurity standards and combating global threats. In addition, the EU cybersecurity policy includes funding programs for innovation in the security sector, aimed at developing new technologies and increasing cyber resilience. Thanks to this comprehensive approach, the EU is building an effective cybersecurity system that serves as a model for countries aspiring to integrate into the European digital space.

Ukraine's national cybersecurity system comprises several key bodies responsible for protecting the digital domain. The main coordinating authority is the National Security and Defense Council of Ukraine (NSDC), which develops strategies and sets priorities in cybersecurity. The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) provides technical information security, sets cybersecurity standards, and coordinates incident response measures. The Security Service of Ukraine (SBU) plays a crucial role in countering cyber espionage and terrorism and conducts investigations in the field of information security. In addition, the Cyber Police investigate cybercrimes such as financial fraud, account breaches, and attacks on IT infrastructure. Additionally, the CERT-UA team and other specialized units respond to cyber incidents in real-time.

In recent years, Ukraine has made significant progress in cybersecurity by developing a National Cybersecurity Strategy [4] and aligning its legislation with EU standards. Ukrainian authorities actively cooperate with international partners, including the EU, NATO, and the USA, gaining access

to technological and expert support. Public-private partnerships in cybersecurity are also thriving, helping engage businesses and civil society in the fight against cyber threats.

Nevertheless, Ukraine faces serious challenges. Constant cyberattacks from the aggressor state have increased the load on the cybersecurity system, demanding continuous improvement of protection mechanisms. Cybercrime remains widespread, particularly financial fraud, phishing, and data breaches. There is also a shortage of qualified cybersecurity professionals, hindering swift response to emerging threats. Moreover, many public and private institutions still rely on outdated security systems, making them vulnerable to attacks.

The full-scale war has significantly intensified the cybersecurity situation, turning cyberspace into an additional battlefield. Ukrainian government bodies, critical infrastructure, and businesses are subjected daily to massive DDoS attacks, database breaches, and cyber espionage attempts. Russian hacker groups coordinate attacks on government institutions, the energy sector, banking systems, and media outlets to disrupt the functioning of key systems.

To strengthen cyber defense, Ukraine is expanding cooperation with international partners, particularly the EU and NATO, enabling access to cutting-edge technologies and experience in combating cyberattacks. Efforts are also being made to improve cyber hygiene among civil servants and businesses through training and awareness programs. Ukraine is introducing new digital security standards and expanding its network of cyber volunteers who help protect the country's IT infrastructure. Additionally, new methods of detecting and countering cyberattacks are being developed, and the cyber police are intensifying their work in digital investigations. In the context of war, cybersecurity has become one of the key priorities for ensuring state stability and protecting digital infrastructure.

Harmonizing Ukrainian legislation with EU cybersecurity norms is a vital step toward digital integration and enhancing national cyber protection. The EU sets high cybersecurity standards, and compliance is a mandatory requirement for full integration into the European digital market.

Key EU regulatory acts aligned with Ukrainian legislation include:

1. NIS2 Directive (Network and Information Security Directive 2) – a revised EU regulation setting cybersecurity requirements for critical sectors such as energy, transport, finance, healthcare, and public administration. Ukraine is gradually adapting its legal framework to this directive, which involves mandatory risk management measures, enhanced oversight of strategic sectors, and the implementation of incident response systems.

2. General Data Protection Regulation (GDPR) – the EU's legislative framework for personal data protection. Ukraine is moving toward GDPR compliance, which includes stricter controls over data processing and storage,

requirements for transparency and user consent, and penalties for data protection violations.

3. EU Cybersecurity Act – governs the creation of a unified cybersecurity certification system in the EU. Ukraine is currently developing national certification standards aligned with this act.

4. Critical Infrastructure Protection Directive – obliges EU countries to identify and protect critical infrastructure from cyberattacks.

Although Ukraine has already adopted relevant legislation, including the Law of Ukraine "On the Basic Principles of Cybersecurity" [5] and the Law "On Personal Data Protection" [6], further harmonization is needed. This can be achieved through:

1) closer cooperation with European institutions;
2) strengthening state institutions;
3) enhancing control over cybersecurity in critical sectors;
4) deeper integration into the European cyberspace.

*Conclusions.*To sum up, Ukraine's further integration into the EU digital space requires ongoing reforms in cybersecurity, contributing to increased digital resilience across the country.

References:

1. Boyko V.D., Vasylenko M.D. Cybersecurity and personal data protection in the EU: problems of the digital society. *Scientific works of the National University of the Ukrainian Academy of Sciences*. 2019. Vol. 23. p. 34-47. URL: https://hdl.handle.net/11300/12580
2. Zhurbynskyi D. A. Kostenko V. O. The relevance of strengthening Ukraine's cybersecurity under martial law in the context of European integration. *Public management and administration in Ukraine*. No. 34. 2023. p. 74-77. DOI: https://doi.org/10.32782/pma2663-5240-2023.34.14
3. Mykytenko D. O. Information protection and cybersecurity as a component of the national security of Ukraine. *Legal scientific electronic journal*. – 2020. No. 8. URL: http://www.lsej.org.ua/8_2020/96.pdf
4. On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". *Decree of the President of Ukraine*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
5. On the Basic Principles of Cybersecurity in Ukraine. Law of Ukraine. *The Official Bulletin of the Verkhovna Rada (BVR)*. 2017. No. 45, Article 403. URL: https://zakon.rada.gov.ua/laws/show/en/2163-19#Text

6. On Personal Data Protection. Law of Ukraine. *Official Bulletin of the Verkhovna Rada of Ukraine (BVR)*, 2010, No. 34, Art. 481. URL: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text

INCREASING THE EFFICIENCY OF CONTAINER HANDLERS WHEN USING DOUBLE CYCLES

D.O. Ivanov
PhD student, Department of Lifting and Transport Machines and Equipment, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
V.V. Strizhak
Associate Professor, Department of Lifting and Transport Machines and Equipment, PhD in Technical Sciences, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
T.L. Polyakova
Associate Professor, Department of Intercultural Communication and Foreign Language, PhD in Philology, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Abstract. The article considers increasing the throughput capacity of intermodal terminals in conditions of limited space for their scaling. The method of double cycles in the operation of container transhipments is considered.
Keywords: double-loop method, intermodal terminals, marine terminals.

Introduction. The double-loop method is a well-known approach to optimizing the throughput of intermodal and marine terminals. Foreign publications contain a significant number of publications devoted to the theoretical foundations of double-loops, their planning algorithms and economic advantages of their use. In general, double-loops are widely used to optimize the operation of not only container transhippers, but also other transhipment machines. For example, in [1] it is recommended to use this technique for port transhippers together with a reduction in the number of tractors traditionally used to arrange containers in front of the transhipper.

Results. The double-cycle method is a well-known approach to optimizing the throughput of intermodal and marine terminals. Foreign publications contain a significant number of publications devoted to the theoretical foundations of double-cycles, their planning algorithms and economic advantages of their use. In general, double-cycles are widely used to optimize the operation of not only container transhipment trucks, but also other transhipment machines.