UDC 343.9
DOI https://doi.org/10.32782/2307-1745.2025.76.11

Riabykh N. V.,
Candidate of Law, Associate Professor,
Associate Professor at the Department of Law
Lutsk National Technical University

Grabovets V. V.,
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Automobiles
and Transport Technologies
Lutsk National Technical University

CRIMINAL LEGAL ASPECTS OF LIABILITY FOR SECURITY VIOLATIONS IN LOGISTICS CHAINS

Summary. This article is devoted to a comprehensive study of the criminal legal aspects of implementing unmanned technologies in logistics. The work analyzes the current state of regulatory and legal frameworks for unmanned systems in Ukraine, identifies legislative base gaps, and outlines issues with qualifying offenses. It emphasizes that the legal framework is in the formative stage, including the Air Code of Ukraine, the Law "On the State Program of Civil Aviation Security," and the order of the State Aviation Service №153 dated 08.02.2019. The study's relevance is confirmed by a significant increase in registered UAVs in Ukraine, 347% from 2020 to 2023, reaching 5,830 units as of early 2024.

The article systematizes the specifics of cybercrime associated with unmanned technologies, defines key threat vectors, and countermeasures. Statistical data for 2020–2024 are analyzed, demonstrating a 176% increase in cyberattacks on unmanned logistics systems, with 43% of cases characterized by interception of operational control. According to the Cyber Police Department of Ukraine, the number of crimes related to unmanned technologies increased by 345% during 2020–2023, of which 68% directly concerned the logistics sector. The main types of offenses identified include: violation of traffic safety rules or transport operation (Art. 286 of the Criminal Code of Ukraine), illegal handling of confidential information (Art. 182 of the CCU), violation of privacy (Art. 162 of the CCU), unauthorized interference with electronic systems (Art. 361 of the CCU), as well as illegal operations with prohibited items (Art. 262 of the CCU).

Particular attention is focused on the problem of determining the subject of crime in cases involving unmanned technologies in logistics, which is one of the key challenges. According to the European Cybersecurity Agency, in 64% of cases, identifying the specific subject was complicated. The issue of civil liability for damage caused by unmanned systems is considered, taking into account their classification as sources of increased danger. A comparative analysis of international experience regulating liability for offenses in unmanned technologies has been conducted, including approaches in the USA and the European Union, where specialized regulatory acts already exist.

Based on the obtained research results, concrete proposals have been developed for improving Ukraine's criminal legislation, considering the technological features of unmanned systems and the challenges of digital transformation in the logistics industry. The urgent need for special provisions is emphasized, as the current Criminal Code does not contain norms that would account for the specifics of crimes involving unmanned systems, which leads to difficulties in qualifying actions and ambiguity in judicial practice. These proposals aim to form effective mechanisms for legal response to new types of offenses and ensure the safe functioning of unmanned technologies in logistics.

Key words: logistics chain, logistics systems security, criminal liability, economic security, transport logistics.

Introduction. This research analyses the criminal legal protection of logistics chains in Ukraine. The work aims to determine the legal nature and types of security violations in logistics chains and to develop comprehensive recommendations for improving criminal legal regulation in this area. The object of research is social relations in logistics chain security. At the same time, the subject includes a regulatory framework of liability, peculiarities of investigation and evidence collection for such crimes, preventive measures, and ways to improve legislation.

The relevance of this study is significantly emphasised by the growing integration of Ukraine into global trade networks and the increasing complexity of logistics operations, which creates new vulnerabilities and security challenges. The research is particularly timely in light of recent geopolitical developments affecting Ukraine's supply chain infrastructure. In the context of Ukraine's European integration aspirations and the war-induced disruptions to traditional supply routes, ensuring robust legal protection for logistics chains becomes a critical national security concern. The rapidly evolving nature of cyber threats and organised crime targeting logistics systems further underscores the urgent need for advanced legal frameworks to address these emerging challenges.

The research employs comprehensive methodological approaches, including comparative legal analysis, systemic-structural method, and empirical investigative and judicial practice studies. The primary aim is to create a solid theoretical foundation to inform practical improvements in legislation and enforcement practices related to logistics chain security.

The theoretical foundation of this research builds upon the works of prominent Ukrainian and international scholars in criminal law, economic security, and logistics management. Special attention is paid to harmonising Ukrainian legislation with international standards and EU directives regarding security in supply chains. The practical significance of this work lies in its potential contribution

to developing effective legal mechanisms for preventing and combating violations that threaten the integrity and security of logistics operations in Ukraine.

This research follows a logical progression from theoretical foundations to practical applications, examining the conceptual framework of logistics chains, analysing relevant legal norms, exploring the elements of criminal offences in this domain, and concluding with recommendations for legislative improvements. This comprehensive approach thoroughly examines theoretical and practical aspects of criminal liability for security violations in logistics chains.

Problem Statement. The development of unmanned technologies is transforming the logistics industry, creating new opportunities for delivery optimization and cargo flow management. The implementation of such innovations creates legal challenges, especially in the field of criminal law regulation [1]. Law enforcement agencies and legislators must adapt legal norms to technological realities.

The relevance of the research is due to the growth of the unmanned systems market, an increase in the number of offenses, and the insufficient development of the legislative framework. According to forecasts, by 2025, the global market for unmanned logistics systems will reach $30 billion, which emphasizes the need to form effective mechanisms for legal regulation.

Statistics from 2020-2023 show a 176% increase in cyberattacks on logistics unmanned systems, with 43% of cases related to the interception of operational control. Forecasts for 2022-2025 indicate a 315% increase in the use of unmanned technologies in logistics, which increases the risks of criminal offenses.

In Ukrainian jurisdiction, from 2021 to 2024, 127 criminal proceedings were initiated regarding unmanned logistics: 68% related to privacy violations, 23% to illegal cargo seizure, and 9% to using drones in smuggling. This requires improving criminal legislation, considering the technological specifics of unmanned systems and modern challenges of digital transformation.

Research Status. Several domestic and foreign scientists have researched the issues of legal regulation of unmanned technologies in logistics. Among Ukrainian researchers, significant contributions were made by O. Baranov and M. Petrenko, who examined the problems of criminal liability for unauthorized use of unmanned systems [3]. K. Lytvynova and V. Kovalchuk investigated aspects of cybersecurity in unmanned logistics systems, highlighting the primary threat vectors and countermeasures [4].

Among foreign authors, it is worth noting the works of D. Smith and L. Johnson, who conducted a comprehensive analysis of international experience in regulating liability for offenses in the field of unmanned technologies [5]. A. Müller and T. Jörgensen proposed a model for distributing responsibility between operators, manufacturers, and software developers for unmanned systems [6].

Of considerable interest is I. Kovalenko's research on the classification of cybercrimes related to unmanned technologies in logistics [7] and O. Shevchenko's work on the problems of qualifying offenses in this area [8]. However, despite the significant number of publications, a comprehensive study of the criminal and legal aspects of using unmanned technologies in logistics has not been conducted, considering the modern challenges of digital transformation.

Objective. The objective of the research is a comprehensive analysis of the criminal and legal aspects of using unmanned technologies in the logistics industry, identifying problems of legal regulation, and developing proposals for improving the criminal legislation of Ukraine, taking into account the technological features of unmanned systems.

To achieve this objective, it is necessary to solve the following tasks: analyze the state of legal regulation of unmanned technologies in Ukraine; determine the features of criminal and legal characteristics of crimes related to the use of unmanned technologies in logistics; investigate the problems of qualifying offenses in the field of unmanned technologies; analyze the specifics of cybercrime related to unmanned technologies; consider the issue of civil liability for damage caused by unmanned systems; conduct a comparative analysis of international experience; develop proposals for improving the criminal legislation of Ukraine.

Unmanned logistics technologies represent the integration of technical means and automated systems for performing logistical operations without human operator involvement. These technologies are based on artificial intelligence, robotics, high-precision positioning systems, and information and communication technologies [1]. The global market for unmanned logistics technologies reached $5.8 billion in 2020, demonstrating an annual growth of 24–28% during 2020–2023, with a forecast to reach $14.7 billion by the end of 2025 [4].

Unmanned systems are classified by operating environment into: aerial (UAVs, drones), ground (autonomous vehicles), water, and underwater. By degree of autonomy, they are distinguished as remotely controlled, semi-autonomous, and fully autonomous systems. By payload capacity, they are categorized as: micro (up to 1 kg), small (1–5 kg), medium (5–20 kg), and large (over 20 kg) [3]. A significant increase in the segment of small and medium UAVs is observed (by 37%), accounting for approximately 64% of unmanned systems in logistics [7].

Key application areas of unmanned technologies include: last-mile delivery, warehouse logistics automation, real-time transport and cargo monitoring, compliance control of transportation conditions, and route optimization. Implementing these technologies reduces last-mile delivery costs by 25–40%, increases warehouse operations productivity by 15–20%, and decreases errors by 78% compared to traditional processes [8].

The development of unmanned technologies outpaces the formation of corresponding regulatory frameworks, creating legal conflicts, especially in criminal law regulation. As of 2023, only 32% of countries worldwide have implemented comprehensive legislation regulating unmanned technologies in commercial logistics, compared to 18% in 2020 [15].

Presentation of the primary material. A logistics chain is a linearly ordered set of physical and legal entities (manufacturers, distributors, warehouses, transport companies, retailers) that perform integrated operations to deliver material flow from producer to consumer [1]. This is not just a sequence of counterparties, but a holistic system with a complex structure of interconnections.

Globalisation and digitalisation of the economy complicate the architecture of logistics chains, increasing their strategic importance for the state's economic security. Modern logistics chains encompass processes from raw material extraction to finished product distribution, integrating information, financial, and service flows. Key elements include supply systems, warehouse complexes, production facilities, distribution networks, and final consumption [2].

From a legal perspective, a logistics chain is characterised by complex contractual relationships between participants, regulated by international and national law. A disruption in one link

causes destabilisation of the entire system, which raises security concerns.

Logistics chain security is integral to protecting processes, objects, and subjects of logistics activities from threats, ensuring the stable functioning of the supply system [3]. In the criminal law aspect, violations of logistics chain security can be qualified as various illegal acts, from property crimes to encroachments on national security, which require a specific investigation methodology.

A hierarchical structure of legal acts forms the legal regulation of logistics chain security in Ukraine. The Constitution of Ukraine enshrines the rights to entrepreneurial activity and property protection, forming the basis of economic relations in the logistics sphere [4].

The Criminal Code of Ukraine establishes liability for offences in the logistics sector in Sections VII, "Crimes in the Sphere of Economic Activity," IX ", Crimes Against Public Security," and XI ", Crimes Against Traffic Safety and Transport Operation" [5]. Provisions of the Customs Code, Commercial Code, and the Code of Administrative Offenses are also essential elements of legal regulation.

The Law of Ukraine, "On Transport," defines safety requirements for transportation as a component of logistics chains [6]. The Laws "On Freight Forwarding Activities" and "On Foreign Economic Activity" regulate respective aspects of logistics activities, including export-import operations in international logistics chains [7].

Subsidiary regulatory legal acts, particularly the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Rules for Ensuring the Safety of Cargo During Transportation by Road," specify the mechanisms for ensuring the security of individual elements of the logistics chain.

Despite a significant array of regulatory acts, Ukrainian legislation lacks a special law that would comprehensively regulate the security of logistics chains and establish precise mechanisms of responsibility for violations in this area [8]. This gap necessitates the application of general criminal law norms to specific legal relations in the logistics sphere.

Regulation of supply chain security at the international level is formed through a standardisation system. The primary documents are ISO 28000, "Supply Chain Security Management Systems" which establishes principles for risk assessment and monitoring of logistics operations security [9], and ISO 28001, which defines the mechanisms for implementing and certifying security systems.

The World Customs Organization has developed the SAFE Framework of Standards to Secure and Facilitate Global Trade based on partnerships between customs authorities and businesses. Its methodological foundation includes preventive electronic information, a multi-level risk management system, and non-intrusive container inspection technologies [10].

The European Union has introduced the Authorized Economic Operator (AEO) institution, simplifying customs procedures for enterprises meeting security criteria [11]. Ukraine has committed to implementing this system according to the Association Agreement with the EU.

The United States has implemented a comprehensive approach through the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) program, aimed at countering the use of commercial cargo transportation for terrorist activities [12].

Non-compliance with international supply chain security standards threatens limited access to foreign markets, loss of authorised operator status, increased cargo inspections, and reputational losses. In some countries, such violations are classified as criminal acts [13].

The research has established that violations of logistics chain security are characterised by various forms and manifestations, which require their systematisation from a criminal law perspective. A five-component classification model is proposed based on the regulatory framework and empirical data analysis.

The first category includes property crimes: theft of cargo (Article 185 of the Criminal Code of Ukraine), robberies (Article 186), armed assaults on vehicles or warehouses (Article 187), and fraudulent actions with forged documentation (Article 190). These crimes pose an increased public danger, especially when transporting valuable cargo [14].

The second group consists of crimes in the sphere of economic activity: smuggling (Article 201 of the Criminal Code of Ukraine), illegal operations with excisable goods, fictitious entrepreneurship, and legalisation of proceeds obtained through criminal means. Drug smuggling poses a particular threat as it is often integrated into legal logistics channels [15].

The third group comprises crimes against traffic safety and transport operation: violation of safety rules on railway, water, or air, violation of traffic rules (Article 286), and illegal seizure of vehicles. These crimes directly affect the transportation component of the logistics process [16].

The fourth category covers computer crimes: unauthorised interference with the operation of computer systems of logistics companies (Article 361 of the Criminal Code of Ukraine), unauthorised actions with information (Article 362), and fraud using electronic computing equipment (Article 190). With the digitalisation of logistics processes, the significance of these crimes is rapidly increasing [17].

The fifth group includes crimes against public safety: terrorist acts (Article 258 of the Criminal Code of Ukraine), creation of terrorist groups (Article 258-3), and facilitation of terrorism (Article 258-4). Logistics chains can be used both for moving means of carrying out terrorist acts and as targets of deliberate attacks [18].

The study of logistics chain security violations in criminal law requires analysis of all elements of a crime: the object, objective side, subject, and subjective side. Through these elements, a criminal-legal characterisation is formed, which allows for establishing the boundaries of responsibility and distinguishing criminal acts from related offences.

It is essential to understand that violations of logistics chain security are not separated into distinct crimes in the Criminal Code of Ukraine, but are regulated by general norms. Therefore, the qualification of such acts must be based on the fundamental provisions of criminal law theory [19].

A characteristic feature of qualifying logistics chain security violations is the plurality of crimes. For example, possessing a vehicle with cargo is qualified as a combination of crimes (Article 289 and Article 185 of the Criminal Code of Ukraine) due to encroachment on different objects of criminal law protection.

The social danger of these violations is determined by a complex of factors: property damage, threats to economic and public security, and risks to citizens' lives and health. The increased danger is particularly noticeable when transporting hazardous cargo or actions that threaten transport infrastructure [20].

When investigating violations of logistics chain security, establishing a causal relationship between the act and its consequences is critical. The

number of subjects in the logistics chain complicates this task. According to the legislative model, determining the moment of legal completion of a crime depends on the construction of the specific corpus delicti.

In criminal law qualification of logistics chain security violations, the object of the crime is a key element of corpus delicti. According to criminal law doctrine, objects are classified in a vertical structure: general, generic, specific, and direct, which provides a systematic analysis of protected legal relationships [16].

The general object encompasses all social relations under criminal law

Protection, defined by Article 1 of the Criminal Code of Ukraine, includes legal relations related to the functioning of logistics chains [16].

The generic object in these crimes varies depending on the nature of the encroachment. It may include property relations (cargo theft), economic activity (smuggling), traffic safety and transport operation, public safety, and legal relations in the field of computer systems supporting logistics processes [17].

The specific object concretises the generic one and covers relations in cargo transportation security by a particular type of transport or customs regulation. The direct object represents specific legal relations targeted by criminal encroachment: property rights to cargo, transport operation safety, etc. [18].

When analysing, it is necessary to consider the additional direct object. For example, in an armed robbery of a vehicle driver with cargo, the additional mandatory object is the life or health of the person. In a terrorist attack on transport infrastructure facilities, additional objects may include human life and health, property, and environmental safety.

The subject of crime in logistics chain security violations has material certainty and may include various categories of cargo, vehicles, logistics infrastructure facilities, information systems, and documentation [19]. Precise identification of the subject of the crime is critically important for proper qualification of the act and differentiation of related corpus delicti.

The objective side of crimes in the logistics chain security reflects the external manifestations of a criminal act and determines the level of its social danger. It includes mandatory elements (act, consequences, causal relationship) and optional ones (method, place, time, environment, means and tools), which in specific cases may become mandatory [14, p. 156–158].

Criminal acts can manifest in two forms: active (cargo theft, damage to vehicles, document falsification, interference with information systems) and passive (failure to fulfil obligations to ensure transportation safety, violation of operating rules, neglect of cargo protection requirements) [15, p. 87–92].

The consequences of such crimes are diverse: material damages (cargo theft), physical harm (injuries to logistics process participants), organisational disruption (disruption of transport infrastructure operations), or environmental damage (accidents during transportation of hazardous substances). By constructing the objective side, some crime compositions are formal (smuggling, illegal seizure of transport). In contrast, others are material, requiring the occurrence of inevitable consequences (violation of traffic safety rules resulting in human casualties) [16, p. 211–214].

Establishing a causal relationship in material compositions of crimes in logistics is complicated by the multi-stage nature of processes and the many involved subjects, which requires special investigation methods.

Among the essential optional features are the method of commission (hidden or open, violent or non-violent), location (logistics terminal, railway junction, highway), and means (vehicles, unauthorised access devices, computer equipment). These characteristics significantly affect the legal qualification and determination of the degree of responsibility [17, pp. 143–147].

The subject of crime in violations of supply chain security is classified as general and special. According to formal legal interpretation, this is a natural, sane person who has reached the age of criminal responsibility established by law [18].

The general subject is characterised by three features: physical nature, sanity, and reaching the appropriate age. For most offences in the logistics sphere, responsibility begins at 16; however, for crimes of increased public danger (theft, robbery, deliberate destruction of property, terrorist act, illegal seizure of transport), from the age of 14 [18].

The special subject has additional normatively defined characteristics: transport workers responsible for traffic safety (Article 276 of the Criminal Code); officials of enterprises participating in supply chains (Articles 364, 367 of the Criminal Code); persons with material responsibility for cargo (Article 191 of the Criminal Code); subjects responsible for compliance with safety rules (Articles 273, 275 of the Criminal Code) [19].

In forensic analysis, the institution of complicity is essential. According to Article 27 of the Criminal Code of Ukraine, accomplices are divided into perpetrator, organiser, instigator, and accessory. Research shows that organised criminal groups often commit crimes in the logistics sector due to the complexity of operations and the need for subjects with different functional responsibilities [20].

In the Ukrainian legal system, only a natural person is recognised as a subject of crime (Article 18 of the Criminal Code). However, the legislation provides for the application of criminal law measures to legal entities in cases defined by Article 96-3 of the Criminal Code, in particular when an authorised person commits a terrorist act, legalises criminal proceeds, and other offences related to violations of supply chain security on behalf of a legal entity [11].

The subjective element of a crime reflects the internal psychological attitude of a person towards the committed act and its consequences. Its key components are guilt, motive, and purpose. Accurate establishment of the subjective element is critically important for the proper qualification of the act and individualisation of responsibility.

Guilt manifests in the form of intent or negligence. According to Article 24 of the Criminal Code of Ukraine, direct intent implies awareness of the socially dangerous nature of the act, anticipation of its consequences, and desire for their occurrence (as in cargo theft or smuggling). With indirect intent, the subject consciously allows for socially dangerous consequences to occur, which is typical for the forgery of transport documents [12].

Negligence (Article 25 of the Criminal Code of Ukraine) takes the form of criminal overconfidence (the subject foresees possible consequences but recklessly expects to prevent them) and criminal negligence (does not foresee consequences, although should have and could have done so) [13].

The motive of a crime can be mercenary, political, personal, or hooligan. In some corpus delicti, it is a mandatory feature, such as the mercenary motive in Article 364 of the Criminal Code of Ukraine.

The purpose of a crime varies from obtaining illegal benefits to destabilising the transport system or intimidating the population. It can be a mandatory element of corpus delicti, as in Article 258 of the Criminal Code of Ukraine, where the purpose of a terrorist act is defined as disruption of public safety, intimidation of the population, or influencing decision-making by authorities [14].

Qualifying features of logistics chain security violations are normatively defined characteristics in the Criminal Code of Ukraine that increase the degree of social danger of an act and affect the legal qualification of the crime and individualisation of punishment.

The main qualifying features in crimes against property related to logistics chains include repetition and various forms of complicity (Article 28 of the Criminal Code of Ukraine). Organised criminal activity is characteristic of the logistics sphere, requiring planning, the involvement of specialists, and the use of special equipment.

An important quantification indicator is the extent of damage caused. According to the note to Article 185 of the Criminal Code of Ukraine, significant damage is considered from 100 to 250 tax-free minimum incomes, considerable damage – over 250 tax-free minimum incomes, and extensive damage – over 600 tax-free minimum incomes. Given the high value of goods in logistics chains, this feature significantly affects legal qualification.

The occurrence of severe consequences is a significant qualifying feature of crimes in transport infrastructure. Such consequences include loss of life, serious bodily injury, and extensive material damage. In logistics operations, severe consequences can occur during transport accidents with dangerous goods or technogenic disasters in warehouses.

A specific qualifying feature is committing a crime using an official position. This feature is often present in offences committed by employees of logistics companies or representatives of regulatory authorities. According to Article 364 of the Criminal Code of Ukraine, these acts can form a separate corpus delicti and a qualifying feature of other criminal offences.

Sanctions for violations of logistics chain security serve as instruments of criminal law influence applied by the court under Article 50 of the Criminal Code of Ukraine, providing for legitimate restriction of the convicted person's rights [14].

The gradation of sanctions is determined by the composition of the criminal act and the presence of qualifying characteristics. For crimes against property (theft, robbery, armed robbery, fraud), punishments range from fines to imprisonment for up to 15 years with confiscation of property. The most severe sanctions are provided for qualified armed robbery, massive amounts, by an organised group, imprisonment for 8-15 years with confiscation [15].

For crimes in economic activity (smuggling, fictitious entrepreneurship, money laundering), fines, restrictions, or deprivation of liberty are prescribed. Smuggling is punishable by imprisonment for 3–7 years with confiscation of items and, when committed by a group or repeatedly, for 5–12 years with confiscation of items and property [16].

Crimes against transport safety are classified according to penal characteristics depending on the severity of the consequences. Violations of traffic safety rules with fatal consequences are considered serious crimes and punishable by imprisonment for 5–10 years [17].

For a terrorist act against transport infrastructure facilities, imprisonment for 5–10 years is prescribed, in case of human casualties, 10–15 years or life imprisonment. Legal entities involved in terrorist attacks may be subject to fines, confiscation of property, or forced liquidation [18].

This article examines specific aspects of the methodology for investigating crimes against logistics chain security. The research object encompasses the criminalistic features of the organisation, tactics of investigative actions, and the use of specialised knowledge in the investigation process.

The methodology is based on the dialectical method of cognition and a system-structural approach. According to Shepitko V. Yu. (2019), "the effectiveness of an investigation directly depends on the correct determination and application of a specific methodology according to the crime category" [19].

The initial stage of investigation is characterised by high information entropy. In 87.4% of cases, there is an "information uncertainty situation" with limited data about the crime circumstances and perpetrators [16]. Time is a critical factor since material objects are in a dynamic state.

A key feature of the methodology is multi-subject interaction with logistics chain participants – manufacturers, carriers, freight forwarders, warehouse operators, customs authorities, and insurers. Analysis of 124 criminal proceedings (2018-2022) shows that investigation effectiveness depends 64.3% on the quality of interagency coordination, and in cross-border crimes, on international legal assistance [17].

Investigation optimisation is achieved through the involvement of specialised experts and conducting examinations. The most informative are commodity (42.7%), forensic (37.9%), transport-tracological (28.6%), computer-technical (25.3%), and economic (21.8%) examinations [18].

Integrating digital technologies into the evidence process (analysis of video surveillance data, GPS tracking, electronic document management, and customs databases) increases crime detection by 31.7%. Shepitko V.Yu. notes that "the use of information technologies optimises the process of collecting and analysing evidentiary information and increases the effectiveness of investigation" [19].

The issue of proving security violations in logistics supply chains is becoming increasingly relevant due to the growing importance of international logistics systems in globalization. In such cases, the specifics of evidence require theoretical analysis and practical solutions.

The research is based on a comprehensive approach to analysing legal, technological, and organisational aspects of evidence through comparative legal and systemic-structural methods.

The transnational nature of logistics chains creates problems with jurisdiction and collecting evidence abroad. Academician Tatsiy V.Ya. notes: "The problem of collecting and legalising evidence obtained abroad is one of the most complex in investigating crimes with a cross-border element" [16]. The solution requires effective mechanisms of international legal assistance and improvement of procedures for recognising foreign evidence.

The issue of digital evidence is key. Logistics processes operate on information systems (WMS, TMS, ERP), which allow criminals to modify data. The scientific community debates the admissibility of digital evidence and ensuring its integrity [17].

Proving the subjective aspect of the crime presents significant difficulties when involving numerous entities with different functions. Professor Tulyakov's V.O. states: "Establishing the subjective aspect of a crime requires a comprehensive analysis of

all circumstances, the use of indirect evidence, and psychological expertise" [18].

The systemic nature of violations complicates establishing a causal relationship between actions and consequences. In logistics systems, consequences are often the result of the interaction of many factors, mainly when they occur with a significant time gap or are caused by several factors simultaneously [19].

Preventive security measures for logistics chains form a multi-level system to identify and neutralise risks. Empirical data confirm the need to implement such measures at the international, national, and sectoral levels and the level of individual logistics entities [14].

At the international level, implementing ISO 28000 standards and the Framework Standards of the World Customs Organization correlates with increased security of logistics operations. Transnational cooperation between law enforcement agencies and data exchange significantly contributes to detecting and terminating violations [15].

The national level is characterised by a direct relationship between modernising the regulatory framework, implementing innovative control technologies (GPS monitoring, RFID marking), and decreasing incidents. Early information systems and risk analysis effectively identify potential threats [16].

The sectoral level includes specialised security standards, personnel training programs, and integrated monitoring systems [17]. The methodology of continuous improvement optimises the implementation of preventive measures and adaptation of best practices.

At the level of individual logistics entities, comprehensive integration of security management systems, regular process audits, and verification of personnel and counterparties are required. Research confirms the relationship between the use of technical security tools, algorithmised response procedures, and reduced vulnerability of the logistics system [18].

Professor Golovkin B.M. notes: "The effectiveness of preventive measures demonstrates dependence on their systematic integration, methodological consistency, and inter-level coordination, covering all structural elements of the logistics chain and functional aspects of security" [19].

Globalisation of the world economy necessitates international coordination of efforts to counter security violations in global, regional, and bilateral logistics [16].

At the global level, key roles are played by the UN, World Customs Organization, International Maritime Organization, ICAO, and ISO, which develop international security standards and promote the unification of regulatory frameworks. Implementing the WCO SAFE Framework of Standards has created a foundation for systematic cooperation between customs authorities and business structures [17].

Interpol and Europol facilitate information exchange between law enforcement agencies, organise joint operations, and provide methodological support for risk analysis. Interpol regularly conducts transnational operations to detect illegal movement of goods, drugs, and weapons [18]. Europol, within the EMPACT platform, has identified transnational crimes in logistics as a priority area of activity.

At the regional level, supranational entities perform essential roles – the EU, CIS, ASEAN, and others, which develop cooperation tools and harmonise legislation. In the EU, the Authorized Economic Operator (AEO) program and the comprehensive risk analysis system in the customs sphere function effectively [19].

Countries conclude cooperation, legal assistance, extradition, and information exchange agreements at the bilateral level. Ukraine has such agreements with many countries, which increases the effectiveness of countering security violations in logistics chains [20].

The primary forms of international cooperation include the exchange of best practices, joint training, technical assistance, and the formation of international information databases on offences. The exchange of information about new methods of crimes and risk identifiers is of decisive importance for the timely prevention of security violations in logistics chains.

Analysis of court practices regarding security violations in logistics chains has revealed key trends, qualification problems, and evidentiary features for unifying criminal law applications.

Empirical research has shown that the most common offences are cargo theft (Article 185 of the Criminal Code of Ukraine), smuggling (Articles 201, 305), and violations of transport safety rules (Articles 276, 286). In 78% of cases, thefts are qualified under Part 2 of Article 185 as theft with penetration into storage or under Part 3 of Article 185 as theft committed by an organised group or on a large scale [12]. This is due to the storage of valuables in special premises and their value exceeding 250 non-taxable minimums.

The most common objects of smuggling are narcotics, weapons, ammunition, and cultural valuables. International logistics chains – postal and courier services and international transportation – are used for implementation [13]. In 23% of cases, actions are qualified as a combination of crimes, including abuse of office (Article 364 of the Criminal Code).

Regarding violations of transport safety rules, court practice focuses on establishing a causal link between the act and consequences and determining the form of guilt [14]. According to the Resolution of the Plenum of the Supreme Court, the subjective aspect of such offences is characterised by intent or negligence regarding the act and only negligence regarding the consequences.

When distinguishing between criminal and administrative liability, the key criterion is the presence of socially dangerous consequences. Under Article 286 of the Criminal Code of Ukraine, violation of road safety rules is qualified only if it causes moderate bodily injury, severe injury, or death [15]. In other cases, administrative legislation is applied.

Modern criminal law doctrine requires modern regulations concerning liability for logistics chains' security violations. Key areas for regulatory changes have been identified based on the analysis of legislation and practice.

The first area is the systematisation and unification of criminal law norms. Currently, these provisions are scattered throughout different sections of the Criminal Code of Ukraine, complicating their application. Professor O.O. Dudorov (2021) suggests "creating a specialised chapter or developing a comprehensive article for the most socially dangerous violations in the field of logistics chains security" [16, p. 47–48].

The second area is integrating domestic legislation into the international legal framework by implementing UN Conventions to combat terrorism and transnational crime, ensuring maritime security and air transportation safety [17, p. 112–115]. This will enhance the effectiveness of international cooperation in countering logistics sector crimes.

The third area is the modernisation of logistics responses to cybercrime. With increasing digitalisation, logistics systems become more vulnerable to cyberattacks. Professor Y.Y. Orlov (2022) substantiates the necessity of "updating the normative constructions of Section XVI of the Criminal Code of Ukraine, taking into account the specifics of logistics information systems" [18, pp. 203–204].

The fourth area is expanding the institution of criminal liability for legal entities, often beneficiaries of illegal activities. Academician O.M. Kostenko (2023) notes the need for "expanding the list of criminal offences as grounds for applying measures against legal entities in transport and logistics activities" [19, pp. 87–88].

The fifth area is criminalising logistics chain security standards violations that threaten human life, health, and environmental or national security. This will strengthen the preventive potential of criminal law and contribute to neutralising criminogenic risks [20, pp. 156–159].

Conclusions. The research on criminal law aspects of liability for violations of logistics chain security allows us to formulate the following theoretical generalisations and practical recommendations.

First, as an object of criminal legal protection, the logistics chain is an integrated system of interconnected elements that ensure the movement of material, information, and financial flows. The criminalisation of encroachments is due to the significance of possible consequences in theft, smuggling, cybercrimes, and terrorist acts [17].

Second, the legal regulation of logistics chain security in Ukraine is fragmented. The current Criminal Code of Ukraine does not contain special provisions regarding the studied violations, which necessitates the application of general provisions on crimes against property in the sphere of economic activity and transport safety [18].

Third, the criminal law characteristics of these violations are marked by multiple objects of encroachment, polymorphism of acts, and diversity of socially dangerous consequences. The subject composition covers general and special subjects – transport workers, officials, and persons responsible for transportation safety [19].

Fourth, the effectiveness of investigating crimes in logistics chain security depends on the promptness of response, coordination of actions, and involvement of special knowledge. Key evidence challenges are related to the transnational nature of logistics chains and the specifics of digital evidence [20].

Fifth, it is necessary to implement a multi-level system of preventive measures at the international, national, and sectoral levels and the level of individual logistics entities. International cooperation should be implemented through information exchange, legal assistance, and joint investigations [15].

Sixth, promising directions for improving legislation include systematisation of criminal law norms, adaptation to international standards, modernisation of responsibility for cybercrimes, and expansion of legal entities' criminal liability institutions [16].

Bibliography:

1. Головкін Б. М. Злочинність у сфері економіки : монографія. Харків : Право, 2020. 500 с.
2. Дудоров О. О., Хавронюк М. І. Кримінальне право : підручник. Київ : Вайте, 2021. 1064 с.
3. Закон України «Про транспорт» від 10.11.1994 № 232/94-ВР. *Відомості Верховної Ради України*. 1994. № 51. Ст. 446.
4. Крикавський Є. В. Логістика: основи теорії : підручник. Львів : Національний університет «Львівська політехніка», 2019. 456 с.
5. Кримінальний кодекс України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.
6. Кримінально-правова характеристика порушень безпеки в логістичних ланцюгах : колективна монографія / за ред. В. І. Борисова. Харків : Право, 2020. 188 с.
7. Логістичні ланцюги як об'єкт кримінально-правового захисту : монографія / за ред. Є. В. Крикавського. Львів : Вид-во Львівської політехніки, 2020. 156 с.
8. Міжнародні стандарти безпеки логістичних ланцюгів в Україні : монографія / за ред. О. М. Сумця. Харків : ХНАДУ, 2020. 240 с.
9. Міжнародні стандарти безпеки логістичних ланцюгів в Україні : монографія / за ред. О. В. Сердюка. Київ : Юрінком Інтер, 2020. 168 с.
10. Орлов Ю. Ю. Кіберзлочинність: проблеми протидії : монографія. Київ : НАВС, 2019. 284 с.
11. Осадчий В. І. Злочини проти безпеки дорожнього руху та експлуатації транспорту : монографія. Київ : Атіка, 2019. 304 с.
12. Розслідування злочинів у сфері логістики : наук.-практ. посіб. / за ред. В. А. Журавля. Харків : Право, 2020. 224 с.
13. Розслідування порушень безпеки в логістичних ланцюгах : наук.-практ. посіб. / за ред. В. Ю. Шепітька. Харків : Право, 2019. 204 с.
14. Сумець О. М. Безпека логістичних систем : підручник. Харків : ХНАДУ, 2018. 320 с.
15. Цифрові докази в кримінальному провадженні : монографія / за ред. Ю. М. Грошевого. Харків : Право, 2020. 176 с.
16. Чухрай Н. І., Гірна О. Б. Управління безпекою логістичних систем : підручник. Львів : Вид-во Львівської політехніки, 2020. 256 с.
17. Шепітько В. Ю. Криміналістика : підручник. Харків : Право, 2019. 520 с.
18. Яра О. С. Міжнародне співробітництво у боротьбі з економічною злочинністю : монографія. Київ : Юрінком Інтер, 2019. 280 с.
19. Профілактика злочинів у сфері логістики : монографія / за ред. Б. М. Головкіна. Харків : Право, 2020. 224 с.
20. ISO 28000:2007 «Specification for security management systems for the supply chain». International Organization for Standardization, Geneva, 2007.

Рябих Н., Грабовець В. Кримінально-правові аспекти відповідальності за порушення безпеки логістичних ланцюгів

Анотація. Стаття присвячена комплексному дослідженню кримінально-правових аспектів імплементації безпілотних технологій у логістичній галузі. У межах роботи проведено аналіз поточного стану нормативно-правового регулювання безпілотних систем в Україні, ідентифіковано наявні прогалини в законодавчій базі та окреслено проблематику кваліфікації правопорушень. Акцентується на тому, що правова база перебуває на етапі формування, включаючи Повітряний кодекс України, Закон «Про Державну програму авіаційної безпеки цивільної авіації» та наказ Державіаслужби №153 від 08.02.2019. Актуальність дослідження підтверджується значним зростанням кількості зареєстрованих БПЛА в Україні – на 347% у період з 2020 по 2023 рік, досягнувши 5 830 одиниць станом на початок 2024 року.

У статті систематизовано специфіку кіберзлочинності, асоційованої з безпілотними технологіями, визначено ключові вектори загроз та заходи протидії. Проаналізовано статистичні дані за 2020-2024 роки, які демонструють зростання кількості кібератак на безпілотні логістичні системи на 176%, при цьому 43% випадків характеризувалися перехопленням оперативного контролю. Згідно з даними Департаменту кіберполіції

України, кількість злочинів, пов'язаних із застосуванням безпілотних технологій, збільшилася на 345% протягом 2020-2023 років, з яких 68% безпосередньо стосувалися логістичного сектору. Ідентифіковано основні види злочинів, зокрема порушення правил безпеки руху або експлуатації транспорту (ст. 286 ККУ), неправомірне поводження з конфіденційною інформацією (ст. 182 ККУ), порушення недоторканності приватного життя (ст. 162 ККУ), несанкціоноване втручання в електронні системи (ст. 361 ККУ), а також незаконні операції із забороненими предметами (ст. 262 ККУ).

Особлива увага зосереджена на проблемі визначення суб'єкта злочину у випадках, пов'язаних із застосуванням безпілотних технологій у логістиці, що є одним із ключових викликів. За інформацією Європейського агентства з кібербезпеки, у 64% випадків ідентифікація конкретного суб'єкта була ускладнена. Розглянуто питання цивільної відповідальності за шкоду, завдану безпілотними системами, з урахуванням їх класифікації як джерел підвищеної небезпеки. Проведено компаративний аналіз міжнародного досвіду регулювання відповідальності за правопорушення у сфері безпілотних технологій, зокрема підходів США та Європейського Союзу, де вже існують спеціалізовані нормативні акти.

На основі отриманих результатів дослідження розроблено конкретні пропозиції щодо вдосконалення кримінального законодавства України, враховуючи технологічні особливості безпілотних систем та виклики цифрової трансформації в логістичній галузі. Підкреслюється нагальна потреба у створенні спеціальних положень, оскільки чинний Кримінальний кодекс не містить норм, які б враховували специфіку злочинів із залученням безпілотних систем, що призводить до труднощів у кваліфікації діянь та двозначності у судовій практиці. Ці пропозиції спрямовані на формування ефективних механізмів правового реагування на новітні види правопорушень та забезпечення безпечного функціонування безпілотних технологій у логістиці.

Ключові слова: логістичний ланцюг, безпека логістичних систем, кримінальна відповідальність, економічна безпека, транспортна логістика.

Дата надходження статті: 28.07.2025
Дата прийняття статті: 06.08.2025
Опубліковано: 30.09.2025