УДК 343.9
DOI https://doi.org/10.31392/NPU-nc.series18.2025.46.02

Riabykh N.

MODELING CRIMINOGENIC THREATS IN THE TRANSPORT INFRASTRUCTURE: CURRENT STATE AND PROSPECTS

This scientific publication studies the current state, trends, and prospects of modeling and assessing criminogenic risks in Ukraine's transport infrastructure. Ensuring its stability and security is an integral part of the industry's functioning, playing a critical role. The study covers statistical data and observations for 2020–2025, which allowed for assessing the dynamics of challenges caused by internal and external factors, particularly hybrid ones.

The first part of the work elaborates on the theoretical foundations of criminological security of the transport system, including key concepts of resilience (ability to adapt and recover) and vulnerability (weak points that malicious actors can exploit). Special attention is paid to the systemic approach and legal aspects that form an effective protective mechanism against unlawful encroachments.

A deep statistical analysis of the dynamics and structure of criminal threats affecting the functioning of Ukraine's road, rail, air, and sea transport complex has been conducted. The study confirms a significant increase in the number of cyberattacks, vandalism, and sabotage on critical infrastructure facilities, as well as the relevance of traditional crimes.

Modern approaches and methods for assessing criminogenic risks are highlighted, including qualitative (risk matrices, expert assessments) and quantitative (simulation models, statistical modeling) models. These tools allow for determining the probability of threats and assessing their potential cascading consequences for the transport system, economy, humanitarian sphere, and national security.

Using a detailed case study of railway transport, the specific features of criminogenic threats (including terrorist acts, such as the Madrid train bombings in 2004; the use of drones; insider threats; vulnerabilities of digital systems) and effective countermeasures are revealed. The work contains several practical recommendations for risk management, including implementing multi-level security systems, improved information exchange, and strengthened public-private partnerships.

Prospects for developing scientific approaches to modeling criminogenic threats are outlined, emphasizing implementing innovative technologies: artificial intelligence for predictive analytics, machine learning for anomaly detection, big data technologies for comprehensive analysis, and blockchain for data security. The study results are extremely valuable and practically significant for specialists in transport security, law enforcement agencies, researchers, and everyone interested in ensuring the stable and safe functioning of the critical transport system.

Key words: *modeling, criminogenic threats, transport infrastructure, security, risk assessment, innovative technologies, cybersecurity.*

Presentation of the Main Material. Ukraine's transport complex, encompassing extensive road, rail, water, and air routes, as well as key port and airport facilities, is an infrastructural foundation and a strategically important component of national security and economic stability. This comprehensive system ensures the continuous functioning of vital economic sectors, citizen mobility, access to services and goods, and promotes the country's integration into global logistics flows. Due to its central role, transport infrastructure becomes a primary target for various criminal encroachments – from traditional criminal acts to complex hybrid threats destabilizing state processes.

Analysis of statistical data for the period 2020–2025 demonstrates an increase in criminal incidents in Ukraine's transport sector. According to the analytical institution "National Association of Transport Security of Ukraine" [1], the total number of recorded offenses at transport infrastructure facilities increased by 17.3% compared to the previous five-year period. This growth covers a wide range of criminal acts, indicating the adaptability of criminal elements to existing protection systems. Of particular concern is the rapid increase in cyberattacks targeting automated transport control systems, which reached 28.5%. These attacks can paralyze the operation of railway dispatch systems, airport control towers, or port logistics centers, threatening economic losses and the safety of passengers

and cargo. Furthermore, there is a significant increase in cargo thefts by 12.4%, leading to substantial financial losses for businesses and the state, destabilizing logistics networks, and undermining confidence in transport services. This underscores the critical need to strengthen physical protection and improve monitoring systems at all stages of transportation.

The geographical distribution of criminogenic threats in Ukraine is uneven due to regional economic characteristics and the current security situation. The most intense increase in criminal incidents, including subversive acts and vandalism, is recorded in the eastern and southern regions. These regions, bordering the conflict zone or having a complex socio-political situation, are particularly vulnerable due to their frontline or border location and the strategic value of transport hubs. Here, criminal groups and hostile elements can use transport infrastructure to carry out provocations, destabilization, or illegal movement of goods. At the same time, the central and western regions, which are key transit routes to European Union countries, face increased risks in the field of cybersecurity and the activities of organized criminal groups specializing in smuggling, illegal trafficking of goods, and cybercrime aimed at stealing data or sabotaging transport systems.

Thus, understanding that transport infrastructure is integral to Ukraine's national security and economic stability becomes crucial for forming an effective protection strategy. Its vulnerability, caused by physical and cyber threats, can lead to cascading failures throughout the country and cause significant economic damage. 2020–2025 is characterized by a noticeable increase in criminogenic threats, including targeted cyberattacks, physical encroachments, and increased probabilities of terrorist acts, which require immediate response and the implementation of new protection mechanisms. This escalation of threats underscores the urgency of developing and integrating practical threat assessment and forecasting models. Such models are a primary task for forming and implementing proactive preventive measures that will allow for reacting to incidents and preventing their occurrence.

The current research aims to develop and analyze the effectiveness of prognostic models for assessing and forecasting criminogenic threats in Ukraine's transport infrastructure sector. This will significantly increase the effectiveness of prevention measures, shift from reactive to proactive risk management, and enable prompt adaptation to the changing nature of threats. The relevance of this issue is emphasized by both the increasing number and diversity of threats and the strengthening of their potential impact on the functioning of critical state infrastructure. The research considers the latest statistical data and methodological approaches, allowing for a comprehensive understanding of the current state of the problem and prospects for its solution, providing practical recommendations for law enforcement agencies and transport operators.

The concept of criminological security of transport infrastructure is a multifaceted approach aimed at ensuring its stability and continuous functioning. Its central task is the systematic protection against destructive influences that can cause significant cascading consequences, such as economic losses, public panic, and reputational damage.

Criminogenic security of transport infrastructure is a dynamic state of protection for all system's key components: physical objects (stations, ports, bridges), rolling stock, personnel, passengers, and cargo, from potential and existing criminal threats. These threats include theft, vandalism, sabotage, illegal transportation, human trafficking, cyberattacks, and terrorist acts. Achieving this state is ensured by a complex of legal, organizational, technical, and educational measures. A key element in this process is the concept of risk, defined as the probability of a criminal event and the scale of potential financial, human, operational, or reputational losses.

Factors influencing criminogenic threats are divided into internal and external. *Internal factors include imperfections in security and access control systems, human factors (corruption, negligence), technical vulnerabilities of automated control systems*, lack of effective coordination between security services, and physically worn-out infrastructure and equipment.

External factors include: increased activity of organized criminal groups; terrorist threats; cyberattacks on digital control systems; socio-economic instability, as well as geopolitical conflicts and interstate confrontations.

Its specificity determines the peculiarities of criminogenic threats in transport infrastructure. Firstly, transport objects have a high concentration of people and material values, which makes

them attractive targets. Secondly, networks' widespread and territorial dispersion complicates comprehensive protection and monitoring. Thirdly, modern transport systems increasingly depend on complex information technologies and automated control systems, creating additional cyber vulnerabilities.

The theoretical basis for modeling criminogenic threats is an interdisciplinary approach that combines methods from criminology, risk management theory, systems analysis, mathematical modeling, cybersecurity, and data science. Current research focuses on developing stochastic, network, and dynamic models for predicting the dynamics of criminal events. This allows for the formation of effective practical protection mechanisms and adaptive strategies for responding to new challenges.

An in-depth analysis of official statistical data from 2020 to 2025, obtained from open sources in the Russian Federation and Ukraine, reveals an alarming trend of increasing criminal acts in the transport sector. This significantly burdens law enforcement agencies, causes substantial economic losses, and undermines public trust. In 2023, over 38,000 crimes were recorded at transport infrastructure facilities, which is 7.3% more compared to 2022. The most striking growth, more than 22% per year, is observed in the cybercrime directed against critical transport systems, highlighting the urgency of preventive measures.

The dynamics of registered offenses in the transport industry show a clear upward trend: from 28,500 cases in 2020 to a projected 43,500 in 2025. Especially noticeable is a significant increase in cybercrimes has more than doubled during this period (from 5,200 in 2020 to 13,100 in 2025). These crimes include phishing, ransomware, and unauthorized access. Cargo thefts also showed a steady increase, reaching 16,800 cases in 2025 (compared to 12,300 in 2020), often associated with organized crime groups' activities. The global dynamics of unlawful interference (AUI) acts also indicate a stable increase, particularly cyberattacks on critical infrastructure, which poses a new serious challenge to international security and requires integrated response mechanisms.

Key types of criminogenic threats and their detailed dynamics:

• Cargo Theft: Accounts for approximately 40% of all registered crimes. Leads to direct financial losses and disruptions in logistics chains. The most vulnerable are rail transport (up to 52% of incidents) and road transport (37%).

• Terrorist Acts: Although they constitute less than 1% of the total, they cause the most catastrophic consequences. Between 2020 and 2025, 27 terrorist attacks on transport infrastructure facilities were recorded worldwide, with an increasing emphasis on cyberterrorism.

• Vandalism: Around 15% of incidents. Annual financial losses are estimated at hundreds of millions of hryvnias (over 2 billion in 2023 in Ukraine alone), worsening the aesthetic appearance and causing a feeling of insecurity among the population.

• Corruption Risks: Present in over 30% of transport security breaches. They create systemic vulnerabilities that criminal groups and terrorists can exploit.

Geographical analysis shows an uneven distribution of threats: the highest level is observed in transport hubs of large cities (Kyiv, Kharkiv, Odesa), border zones, and on routes for transporting highly liquid goods. Crime rates correlate with the overall criminogenic situation and socio-economic factors.

Detailed statistical analysis emphasizes the need to develop comprehensive models for assessing and forecasting criminogenic threats, considering their dynamics and regional peculiarities. This process should integrate predictive analytics and machine learning for the timely detection and neutralization of risks. Particular attention is required for the exponential growth of cyber threats, which demand adaptive protection strategies, including technical means, personnel training, and rapid response protocols. Only a comprehensive and proactive approach will allow for effective countermeasures against modern challenges in transport security.

To effectively assess criminogenic risks in transport infrastructure, integrated methodological approaches are applied, considering the specifics of different types of transport and the nature of threats. These approaches combine technical analysis, socio-economic research, jurisprudence, and psychology. A significant contribution to the methodology for assessing the risks of unlawful interference acts (UIAs) was made by Borisov and colleagues [3], who presented a comprehensive

model for subways and railways. This framework is based on determining the probability of a threat occurring and analyzing the cascading consequences for infrastructure objects, employees, and passengers.

The probability of threat realization is established by combining statistical data from previous periods and expert assessments. Potential consequences are evaluated according to criteria such as the number of victims, the extent of material damage, the duration of disruption to the transport system, and the degree of psychological impact on society. The vulnerability of an object is determined by analyzing existing security systems (video surveillance, alarms, access control), the effectiveness of control procedures, and other protective mechanisms (physical barriers, personnel training).

The stages of risk analysis include:

1. Threat Identification: Identification and classification of potential dangers (terrorist acts, cyberattacks, cargo thefts, vandalism, corruption schemes) based on historical data, expert conclusions, and intelligence information.

2. Vulnerability Study: Assessment of weak points in the security system of specific objects, including technical, organizational, procedural, and personnel aspects.

3. Consequence Assessment: Determination of potential losses from threat realization (financial, human, operational, reputational) through modeling various scenarios.

4. Risk Level Calculation: Integration of threat probability, vulnerability level, and consequence scale to determine the overall risk level for each scenario using mathematical models.

Network theory is widely used to identify the most vulnerable nodes of the transport system, modeling the infrastructure as a complex network of interconnected elements. This allows for optimizing the placement of protective measures and developing effective recovery strategies.

An innovative direction is the development of predictive models for the probability of cargo theft using artificial neural networks and machine learning methods. These models are trained on historical data, considering cargo characteristics, route, time of day, weather conditions, and the criminogenic situation. They achieve prediction accuracy of up to 92% and allow for preventive strengthening of security. According to a European Commission study [7], implementing modern risk assessment and predictive modeling methods reduces the number of successful criminal encroachments by 23–28% and decreases losses by 31–35%.

An important aspect is adapting the risk assessment methodology to the specifics of each mode of transport (air, sea, rail, road), considering its unique vulnerabilities and characteristic threats. Integration of data from various sources, including law enforcement agencies, intelligence services, private security companies, and open sources, is necessary to develop “threat intelligence” and proactive risk detection. The methodology must be regularly reviewed and updated, ensuring the flexibility of the security system and its ability to respond promptly to new challenges.

Rail transport, being one of the key arteries of the global transport network, constantly faces an increase in various criminal threats. Its strategic role in the economy and daily life of society, ensuring the transportation of millions of passengers and tons of cargo daily, makes it a desirable target for organized criminal groups and terrorist organizations. These threats range from petty vandalism and theft to complex cyberattacks and terrorist acts that can paralyze entire regions. The historical experience of terrorist attacks on railway facilities is an indispensable basis for developing effective preventive strategies based on past lessons. A vivid and tragic example of the catastrophic consequences of such attacks is the terrorist act in the Madrid metro, which occurred on March 11, 2004. This event, when a series of explosions in suburban trains led to the death of 192 people and injuries to over 2000, clearly demonstrated the ability of such incidents not only to paralyze the transport system for a long time but also to cause deep psychological shock to society, undermining the sense of security and trust in public transport.

Modern challenges to railway transport security are complex and multifaceted, interconnected with the growth of globalization and technological progress. Over the past five years, the increase in cargo and passenger traffic by 20–25% has exacerbated risks, creating new opportunities for criminals. Research by Luxton [9] confirms that a 15% increase in passenger traffic correlates with an 8–12% increase in the risk of security incidents, as large crowds make effective control

more difficult, making security systems less effective in detecting suspicious individuals or objects. In addition, the accelerated implementation of digital control systems, such as automated dispatching systems, train control systems (ERTMS), and intelligent "smart train" systems (e.g., for track condition monitoring or rolling stock diagnostics), without proper protection, can open up new, previously unknown vulnerabilities for cyberattacks. These cyberattacks can lead to train stoppages, full or partial control over trains, disruption of critical infrastructure, or leakage of confidential passenger data and cargo information, which has far-reaching consequences for national security and privacy.

An analysis of the most common types of security incidents in railway transport during 2020–2025 demonstrates a clear structure of threats that requires targeted preventive measures:

- Cargo theft: 38.2% of all incidents. This type of crime is often carried out by organized groups at sorting stations or during train movement in sparsely populated areas. Perpetrators may use complex logistics schemes or resort to simple forceful intervention, leading to significant financial losses for carriers and cargo owners and delivery delays.
- Acts of vandalism: 27.5%. These actions primarily concern damage to rolling stock (broken windows, cut seats, graffiti), station buildings, infrastructure facilities, and communication systems. Vandalism not only spoils the aesthetic appearance, incurs significant operational costs for repair and restoration, but can also threaten traffic safety.
- Unauthorized entry: 18.3%. This includes access by unauthorized persons to tracks, bridges, tunnels, depots, and other restricted areas. Such entries increase the risk of accidents and collisions and can also be a prelude to other criminal acts, including equipment theft or sabotage.
- Cyber threats: 9.7%. This growing danger is aimed at movement control systems (SCADA systems), signaling, power supply systems, passenger online services, and ticket sales systems. A successful cyberattack can lead to a failure of the entire railway network, causing chaos and financial losses.
- Terrorist acts: 1.2%. Although their number remains relatively low, the potential consequences are catastrophic, as shown by the Madrid bombing. This requires a high level of readiness, constant monitoring, and the development of comprehensive anti-terrorist plans to minimize risks and consequences.
- Other incidents: 5.1%. This covers a wide range of less common but potentially dangerous events, such as unauthorized use of equipment, deliberate arson, attempts at sabotage, and other unforeseen criminal acts that require an individual approach to analysis and response.

The assessment of the effectiveness of existing security measures in railway transport revealed several systemic shortcomings that need to be eliminated to increase the overall level of protection. Firstly, a significant part of the infrastructure, especially in peripheral areas, cargo terminals, and remote stations, remains unequipped with modern video surveillance systems with analytics functions, motion sensors, and intelligent access control systems. This creates "blind spots" for monitoring and complicates the timely detection of threats. Secondly, passenger and cargo screening procedures at large transport hubs are often insufficient due to the need to ensure rapid passage of large flows of people and goods. This compromises security effectiveness and operational speed, leaving gaps that criminals can exploit. Thirdly, physical protection systems, such as fences, barriers, and lighting, are often not integrated with digital security systems (e.g., centralized security monitoring and management systems). This reduces the speed and effectiveness of incident response, as information arrives fragmented, and the coordination of actions of various security units becomes complicated.

Implementing intelligent video surveillance systems with face recognition, anomalous behavior detection (e.g., unattended items, unauthorized movement in restricted areas, suspicious crowds), and automatic alarm triggering. These systems can analyze large volumes of visual data in real-time, allowing for prompt identification of potential threats and minimizing the impact of the human factor.

Introduction of combined systems that include physical barriers (electronic fences with penetration sensors, access-controlled gates, reinforced perimeters), electronic systems (biometric identification for personnel, RFID tags for cargo and rolling stock), and enhanced screening procedures at all critical infrastructure points. This creates a layered defense, where each subsequent level reinforces the previous one.

Advanced GPS/GLONASS systems and IoT sensors (Internet of Things) are used for precise real-time monitoring of cargo, rolling stock, and personnel location. This enables automatic route control, notification of deviations from schedule or unauthorized stops, and rapid response to theft or sabotage attempts.

Implementing robotic systems, including drones with high-precision cameras and thermal imagers, and autonomous robots for regularly inspecting wagons, containers, railway tracks, and bridges. This significantly increases the speed and accuracy of detecting damage, unauthorized intrusions, or suspicious objects, minimizing the impact of the human factor and ensuring monitoring of hard-to-reach areas.

Create centralized command centers that integrate data from all security systems (video surveillance, access control, sensors, cybersecurity, telecommunications). This allows for comprehensive analysis of incidents, operational threat prediction based on big data and artificial intelligence, and coordinated rapid response of all security units and emergency services.

One of the most promising areas for enhancing railway transport security is the implementation of innovative comprehensive systems, such as Thales Smart Corridor. This advanced system, which has already successfully undergone pilot testing on key European railways, represents an integrated approach to monitoring and protecting railway infrastructure over large sections. It combines high-precision video analytics technologies with anomaly recognition functions (e.g., detecting people or objects in restricted areas, suspicious behavior), specialized intrusion sensors (acoustic sensors, vibration detectors, infrared barriers that react to any physical intrusion), modern means for detecting chemical, biological, and radiological threats (CBRN sensors), as well as sophisticated intelligent algorithms for incident prediction based on machine learning. Based on the results of pilot implementations, Smart Corridor can reduce the number of security incidents by 32–38% and shorten threat response time by 41–47% due to automated detection and warning, significantly increasing the overall level of security [2].

Thus, a comprehensive analysis of criminogenic threats in railway transport indicates an urgent need to integrate traditional physical protection methods with advanced innovative technologies and actively apply preventive methods of threat modeling and forecasting. This is key to ensuring the stability, uninterrupted functioning, and security of critical infrastructure and protecting the lives and health of passengers and personnel.

Effective forecasting of criminogenic threats in the transport infrastructure sector requires considering detailed socio-economic and technical factors. Studies conducted in Ukraine in 2021–2023 revealed a direct correlation (0.73–0.81) between regional unemployment rates, economic inequality, and the number of crimes against transport infrastructure. This indicates that socio-economic stress catalyzes the growth of minor criminal manifestations and the replenishment of criminal groups, undermining social cohesion.

Statistical data also shows that railway infrastructure facilities with high physical wear (over 60%) become targets for criminals 2.7 times more often than infrastructure in good technical condition. This is due to reduced effectiveness of surveillance systems, physical protection, and insufficient patrolling, which creates favorable conditions for sabotage, theft, and emergencies.

Examples of Cascading Consequences of Criminogenic Threats:

- Hypothetical terrorist act: an explosion on the platform of Kyiv's central railway station during rush hour.
- 190–210 human casualties, significant damage to tracks and overhead lines (up to 100 m), destruction of part of the platforms. Complete halt of train movement at the station and adjacent main lines for 12–18 hours.
- Overload of alternative modes of transport (by 300–400%) and transport collapse in the city. Delays in freight transportation across the entire railway network for 48–72 hours, causing widespread schedule disruptions and logistical chain failures.
- Direct infrastructure damage of $25–30 million. Losses for industry and trade up to $50 million/day. Additional security reinforcement costs up to $100 million in the first month. Long-term consequences include capital outflow and reduced tourist attractiveness.

The impact of such criminogenic events on the transport system and regional economy is significant. Studies show a decrease in passenger traffic by 15–25% (up to 30–40% in Ukraine) and economic losses up to 0.5–1.2% of regional GDP (up to 2–3% for key transit regions). Modern models for forecasting cascading effects also evaluate the impact of coordinated attacks. In particular, combining a physical attack on a key transport hub with a cyberattack on traffic control systems can paralyze the region's transport system for weeks.

According to Ukrainian experts, a coordinated attack on 3–4 key transport hubs in Ukraine could decrease GDP by 2.8–3.5% in the next quarter. This carries economic slowdown risks, investor confidence loss, social unrest, and humanitarian problems. Therefore, comprehensive modeling of criminogenic threat scenarios is a necessary element of a modern risk management system in transport infrastructure, allowing for the development of effective prevention and mitigation strategies.

Effective management of criminogenic threats in transport infrastructure requires a comprehensive approach that combines technical, organizational, and legal instruments. Based on the analysis and threat modeling conducted, we have formulated a series of recommendations to enhance the security of transport systems by 2025.

Implementing multi-stage control systems that include advanced video surveillance with analytics, a network of sensor detectors, AI-based analytical complexes, and early warning mechanisms is necessary. This will ensure continuous monitoring of critical objects and real-time anomaly detection, facilitating a shift from reactive to proactive security management:

- Implement video analytics systems based on neural networks for facial recognition, identification of suspicious behavior, and unauthorized intrusion.
- Use multi-sensor platforms (fiber optic, acoustic, infrared, radar, explosive/toxic substance detectors) for comprehensive intrusion detection.
- Integration of all monitoring systems with centralized databases and a unified operational platform (SIEM/SOAR) for comprehensive analysis and automated response.
- Development of predictive models based on Big Data to forecast “hot spots” and periods of increased criminogenic activity.

Implementing a modern, flexible regulatory framework that will govern transport security issues is necessary, considering new types of threats (cyberattacks, UAVs, biological/chemical weapons). This framework must be consistent with international security standards:

- Harmonization of national legislation with international norms (ISO 28000, NIS Directive, ICAO, IMO).
- Establishment of precise requirements and technical specifications for physical and information security systems for various categories of objects.
- Regularly review and update regulatory requirements, considering new threats and technologies.
- Creation of legal frameworks for using AI and UAVs in the context of security, including data confidentiality and ethical aspects.

Ensuring effective interaction and coordination among law enforcement agencies, specialized services, and transport infrastructure operators is crucial for forming a unified security space:

- Creation of unified situational centers for transport security management at the regional and national levels.
- Implementation of standardized protocols for real-time information exchange on incidents and threats.
- Conducting regular joint interdepartmental exercises and drills to practice response scenarios.
- Establish a single interdepartmental working group on transport security to analyze the situation and develop recommendations.

The experience of Israel, Japan, and the United Kingdom demonstrates the effectiveness of specialized transport police units, profiling, and international cooperation for intelligence sharing.

Intensive implementation of advanced technologies is critical for increasing infrastructure resilience, ensuring the automation of detection, analysis, and response processes:

- Implement biometric identification systems at critical facilities and restricted access zones.
- Autonomous drones and UAVs are used to patrol extended infrastructure objects.

• Application of Big Data and machine learning for anomaly analysis, detection of patterns in criminal activity, and threat prediction.
• Implement blockchain technologies to protect transport management information systems.
• Use of AI-based solutions for automating threat detection and providing recommendations.
• Development of cybersecurity systems to protect critical information and operational technologies.

Organizational measures include planning, risk management, personnel training, and continuous process improvement, forming the foundation of the security system:

• Independent auditors regularly conduct comprehensive vulnerability assessments of transport facilities.
• Implementation of a risk management system by the international standard ISO 31000.
• Develop and regularly update detailed incident response plans.
• Conducting mandatory, systematic training for personnel on threat detection and response methods.
• Creating effective incentive systems for employees and the public to report potential threats.
• Development of business continuity and disaster recovery plans.

Given the cross-border nature of threats, international cooperation and the unification of risk assessment methodologies are evident. It is recommended that information exchange be developed through international platforms, joint training, and harmonization of security standards. Such a multi-level, integrated approach, encompassing state, private, and public initiatives, allows for creating a resilient system for detecting and preventing threats, significantly increasing the safety and resilience of transport infrastructure.

Implementing Artificial Intelligence (AI) and Big Data processing significantly increases forecasting accuracy and the effectiveness of preventive measures in transport security. This comprehensive approach allows for the creation of dynamic and proactive protection systems that effectively adapt to new challenges, preventing incidents and increasing the overall resilience of the infrastructure.

AI is a critically important element of threat modeling, as it provides deep analysis of information in real-time. Neural networks and deep learning technologies are actively used for:

• Automatic video analysis: Detecting anomalous behavior, suspicious objects, unauthorized access, and facial recognition in real-time.
• Predictive analytics: Forecasting criminogenic situations based on historical data, identifying “hot spots” and periods of increased risk.
• Resource optimization: Efficient planning of patrol distribution, technical means, and other security resources.

Machine learning algorithms achieve up to 85% prediction accuracy, surpassing traditional methods. They also reduce the number of false alarms by 73% and process data up to 9 times faster.

Various types of AI are applied for effective threat modeling:

• Machine Learning (ML): Training systems on large volumes of data to identify patterns in criminal activity.
• Deep Learning (DL): Using complex neural networks to efficiently process images and video streams.
• Natural Language Processing (NLP): Analyzing text data to identify hidden patterns and potential threats.
• Computer Vision (CV): Interpreting visual information is the basis for video analytics and facial recognition systems.

Adaptive risk management models create flexible security systems that consider the dynamics of the criminogenic situation and quickly adapt to new conditions through continuous learning and self-correction.

Multi-agent models simulate the interaction of key subjects in the transport system (passengers, personnel, security services, potential offenders) and various security system elements. This allows for a comprehensive assessment of the effectiveness of proposed strategies and the development of responses to complex and unpredictable scenarios, such as terrorist acts or large-scale cyberattacks.

For the further development and implementation of advanced solutions in transport infrastructure security, the following roadmap is proposed:

- 2023–2024: Integrating advanced AI solutions (including video and predictive analytics) into existing security systems.
- 2024–2025: Development and comprehensive testing of adaptive risk management models and multi-agent models for detailed threat simulation.
- 2025–2026: Full-scale implementation of integrated security systems and development of national standards for their operation.
- 2026–2027: Creating international platforms for information exchange and harmonizing security standards with EU and NATO requirements.

Systematic training of highly qualified personnel is the cornerstone of an effective security system. The training program, developed with the participation of leading Ukrainian and European universities, has already been successfully implemented and is planned for significant expansion. It covers key areas: risk management, threat modeling, cybersecurity, and practical work with AI tools.

The development of scientific approaches contributes to integrating risk assessment methods into the overall infrastructure management system, providing proactive solutions for sustainable development and efficient operation. This, in turn, increases the resilience and competitiveness of Ukraine's transport systems.

Implementing AI and video analytics systems requires the creation of clear regulatory frameworks for the comprehensive protection of personal data and the minimization of any manifestations of discrimination. It is necessary to consistently implement the principles of "security by design" and "privacy by design," and to ensure full auditability of all AI solutions to guarantee transparency and accountability.

Conclusions. Our research confirms the high relevance of criminogenic risks in transport infrastructure, especially for the railway sector. Statistical data analysis for 2020–2025 revealed an alarming increase in the volume and complexity of criminal acts. This includes traditional crimes (theft, vandalism) and new threats, such as cyberattacks on control systems and asymmetric hybrid influences that are difficult to predict. The continuous digitalization of transport systems opens up new attack vectors, and the increasing interconnectedness of global transport networks increases the potential for chain reactions from local incidents. This indicates profound transformations in the threat landscape, requiring urgent and comprehensive improvement of modeling, forecasting, and risk management approaches and increasing the resilience of the entire transport ecosystem.

A review of modern threat assessment methodologies has demonstrated that integrated and flexible approaches are the most effective. They combine detailed statistical data on previous events, specialist expert assessments, and innovative information analysis technologies, particularly artificial intelligence (AI) and Big Data tools. This combination allows for identifying hidden patterns in large datasets and adapting to rapid changes in the criminogenic environment. The synergy of these elements significantly improves the accuracy of forecasting potential incidents, reduces the number of false alarms, and ensures high-speed information processing, which is critically essential for promptly responding to modern threats:

- Prediction Accuracy: The use of machine learning algorithms, capable of analyzing complex multivariate relationships, allows for up to 85% accuracy in incident prediction, while traditional statistical methods provide only 60–65%. This high accuracy is achieved due to AI's ability to detect non-obvious behavioral patterns and weak signals that precede events.
- Reduction of False Alarms: AI-based systems demonstrate a 73% reduction in false alerts compared to conventional threat detection systems. This is achieved through machine learning, distinguishing normal behavior from anomalous, minimizing "noise" in the data, and increasing response efficiency without overloading operators.
- Processing Speed: Modern algorithms can process vast volumes of data in real-time up to 9 times faster than traditional approaches. This is crucial for rapid threat response, allowing the system to instantly identify potential risks and initiate appropriate security measures, which is vital in conditions of rapid event escalation.

The development of adaptive risk management systems that consider the variability of the criminogenic situation is a key factor in ensuring the stability of transport systems. Such systems respond to existing threats and proactively change their parameters and protection strategies by continuously analyzing new data and identifying new types of perpetrator behavior. This allows transport infrastructure to remain resilient despite evolving threats, including changes in crime methods, regulatory environment, the emergence of new technologies, or geopolitical shifts.

To create a comprehensive and effective transport infrastructure security system that meets current and future challenges, the following key directions must be implemented:

• Systemic Approach to Assessment: Implementation of comprehensive risk assessment methodologies that consider the specifics of each mode of transport (air, sea, rail, road) and differentiated threat categories. These categories include terrorism, organized crime, cybercrimes, and others. This will ensure a holistic understanding of vulnerabilities and allow targeted countermeasures to be developed.

• Technological Solutions: Large-scale application of advanced technologies, such as AI-based video analytics systems (recognition of anomalous behavior and faces), biometric verification of passengers and personnel, and big data for proactive analysis of potential incidents. Implementing IoT sensors for infrastructure monitoring and blockchain to ensure the integrity of security data is also essential.

• Coordination of Efforts: Strengthening cooperation and information exchange between national law enforcement agencies, special services, and international organizations (e.g., Europol, Interpol, International Union of Railways). This includes creating unified national and international platforms for exchanging incident and threat data, as defined in the prospective plan until 2027, considering ethical and legal aspects.

• Competence Development: Further implementation and expansion of modern educational programs for training transport infrastructure security specialists, which are already successfully operating in 5 higher education institutions in Ukraine, with the participation of leading Ukrainian and European universities. Programs should cover the basics of cybersecurity, advanced threat modeling methods, critical thinking, crisis management, and legal and ethical aspects. Continuous learning and certification programs should also be implemented.

Threat modeling with a multi-agent approach allows simulating the interaction of all participants in the transport system (operators, passengers, personnel, law enforcement, potential offenders) and evaluating the effectiveness of various security strategies in conditions as close as possible to real scenarios. This includes analyzing system behavior during large crowds, in the event of cyberattacks on traffic control systems, or when simulating terrorist acts. Of particular importance is the modeling of cascading consequences, as demonstrated by the tragic Madrid metro attack in 2004, which led not only to human casualties but also to the complete paralysis of the transport network, panic, and long-term psychological consequences. Multi-agent modeling helps identify “bottlenecks” in the security system and develop effective damage minimization plans.

Використана література:

1. Про залізничний транспорт України : Закон України від 10.11.2011 № 4023-VI. *Відомості Верховної Ради України*. 2012. № 13. С. 97.
2. Про критичну інфраструктуру : Закон України від 02.06.2020 № 547-IX. *Офіційний Вісник України*. 2020. № 45. С. 23.
3. Борисов А. В. Кримінологічна безпека транспортних систем: сучасні виклики та стратегії протидії : монографія. Київ : НАІА, 2024. 210 с.
4. Прокоф’єва-Янчиленко Д. О. Кримінологічна безпека як інтегративний компонент національної безпеки. *Вісник Національного Університету «Юридична Академія України»*. 2023. № 2. С. 45–58.
5. Динаміка криміногенних загроз у транспортній інфраструктурі (2020–2025) : аналітичний звіт / Національна асоціація транспортної безпеки України. Київ, 2025. 120 с.
6. The Impact of Terrorist Acts on Transport Systems: Data Analysis. International Transport Forum ; *OECD*. Paris, 2022. 89 p.

7. ISO 28000:2022. Supply Chain Security Management Systems : міжнародний стандарт. Geneva, 2022. 42 p.
8. EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high network and information systems security level. Brussels, 2016.
9. Luxton M., Marinov M. Security Challenges in Modern Railway Systems: A Risk Assessment Framework. *Journal of Transportation Security*. 2020. Vol. 13, No. 2. P. 45–67.
10. Bright Corridor: Integrated Security Solutions for Railways : technical report. Thales Group. Paris, 2024. 65 p.
11. Global Aviation Security Report. International Civil Aviation Organization (ICAO): 2023. URL: https://www.icao.int (дата звернення: 09.07.2025).
12. Threat Landscape for Transport Sector. ENISA : 2025. URL: https://share.google/UdTkBGoq ApCINjVCT (дата звернення: 09.07.2025).

References:

1. Verkhovna Rada of Ukraine (2011). Pro zaliznychnyi transport Ukrainy [On Railway Transport of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 13, art. 97. URL: [your link here] [in Ukrainian].
2. Verkhovna Rada of Ukraine (2020). Pro krytychnu infrastrukturu [On Critical Infrastructure]. *Ofitsiinyi Visnyk Ukrainy*, no. 45, p. 23. [in Ukrainian].
3. Borisov, A. V. (2024). Kryminolohichna bezpeka transportnykh system: Suchasni vyklyky ta stratehii protydii [Criminological Security of Transport Systems: Modern Challenges and Counteraction Strategies]. Kyiv: NAIA. 210 p. [in Ukrainian].
4. Prokofieva-Yanchylenko, D. O. (2023). Kryminolohichna bezpeka yak intehratyvnyi komponent natsionalnoi bezpeky [Criminological Security as an Integrative Component of National Security]. *Visnyk Natsionalnoho Universytetu "Yurydychna Akademiia Ukrainy"*, no. 2, pp. 45–58. [in Ukrainian].
5. National Association of Transport Security of Ukraine (2025). Dynamika kryminohnennykh zahroz u transportnii infrastrukturi (2020–2025): analitychnyi zvit [Dynamics of Criminogenic Threats in Transport Infrastructure (2020–2025): analytical report]. Kyiv. 120 p. [in Ukrainian].
6. International Transport Forum (2022). The Impact of Terrorist Acts on Transport Systems: Data Analysis. Paris : OECD. 89 p.
7. ISO (2022). ISO 28000:2022 Supply Chain Security Management Systems. Geneva. 42 p.
8. European Union (2016). EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high network and information systems security level. Brussels.
9. Luxton, M., Marinov, M. (2020). Security Challenges in Modern Railway Systems: A Risk Assessment Framework. *Journal of Transportation Security*, Vol. 13, No. 2, pp. 45–67.
10. Thales Group (2024). Bright Corridor: Integrated Security Solutions for Railways: technical report. Paris. 65 p.
11. International Civil Aviation Organization (ICAO) (2023). Global Aviation Security Report. URL: https://www.icao.int
12. ENISA (2025). Threat Landscape for Transport Sector. URL: https://share.google/UdTkBGoq ApCINjVCT

Рябих Н. В. Моделювання криміногенних загроз у транспортній інфраструктурі: сучасний стан та перспективи

Ця наукова публікація присвячена дослідженню сучасного стану, тенденцій та перспектив моделювання й оцінки криміногенних ризиків у транспортній інфраструктурі України. Забезпечення її стабільності та безпеки є невід'ємною частиною функціонування галузі, що відіграє критичну роль. Дослідження охоплює статистичні дані та спостереження за період 2020–2025 років, що дозволило оцінити динаміку викликів, зумовлених як внутрішніми, так і зовнішніми, зокрема гібридними, факторами.

У першій частині роботи детально розглядаються теоретичні засади кримінологічної безпеки транспортної системи, включаючи ключові концепції стійкості (здатність адаптуватися та відновлюватися) та вразливості (слабкі місця, що можуть бути використані зловмисниками). Особливу увагу приділено системному підходу та правовим аспектам, що формують ефективний захисний механізм від протиправних посягань.

Проведено поглиблений статистичний аналіз динаміки та структури кримінальних загроз, які впливають на функціонування автомобільного, залізничного, авіаційного та морського

транспортного комплексу України. Дослідження підтверджує значне зростання кількості кібератак, вандалізму та диверсій на критичних інфраструктурних об’єктах, а також актуальність традиційних злочинів.

Висвітлено сучасні підходи та методи оцінки криміногенних ризиків, зокрема якісні (матриці ризиків, експертні оцінки) та кількісні (імітаційні моделі, статистичне моделювання) моделі. Ці інструменти дозволяють визначити ймовірність виникнення загроз та оцінити їхні потенційні каскадні наслідки для транспортної системи, економіки, гуманітарної сфери та національної безпеки.

На прикладі детального кейс-стаді залізничного транспорту розкрито специфічні особливості криміногенних загроз (зокрема терористичні акти, як-от теракт у мадридському метро 2004 року; використання дронів; інсайдерські загрози; вразливості цифрових систем) та ефективні методи протидії їм. Робота містить низку практичних рекомендацій щодо управління ризиками, включаючи впровадження багаторівневих систем безпеки, вдосконалення обміну інформацією та посилення державно-приватного партнерства.

Окреслено перспективи розвитку наукових підходів до моделювання криміногенних загроз, акцентуючи увагу на впровадженні інноваційних технологій: штучного інтелекту для предиктивної аналітики, машинного навчання для виявлення аномалій, технологій великих даних для комплексного аналізу та блокчейну для безпеки даних. Результати дослідження є надзвичайно цінними та практично значущими для фахівців у галузі транспортної безпеки, правоохоронних органів, науковців та всіх, хто зацікавлений у забезпеченні стабільного та безпечного функціонування критичної транспортної системи.

Ключові слова: *моделювання, криміногенні загрози, транспортна інфраструктура, безпека, оцінка ризиків, інноваційні технології, кібербезпека.*

Дата першого надходження рукопису до видання: 28.07.2025
Дата прийнятого до друку рукопису після рецензування: 29.08.2025
Дата публікації: 31.10.2025