DOI https://doi.org/10.36059/978-966-397-601-3-124

INVESTIGATION OF CRIMINAL OFFENCES AT CRITICAL INFRASTRUCTURE FACILITIES: EU EXPERIENCE

Oleh BATIUK
Doctor of Law, Professor,
Leading Researcher of the Research Laboratory of Construction and Operational Application
National Academy of the National Guard of Ukraine
Kharkiv, Ukraine

The rise of organized cybercrime, large-scale attacks targeting critical infrastructure and the fast pace of technological adoption affecting social and economic development highlight the far-reaching economic impacts of cybersecurity.

The current stage of society's development is characterized by the growing role of critical infrastructure as the basis for the functioning of the state, economy and social sphere. In the context of hybrid threats, digitalization and armed conflicts, there is a significant increase in the vulnerability of critical infrastructure facilities to criminal offenses, in particular sabotage, terrorist acts and cyberattacks. This is confirmed by statistical data: in 2024, more than 4,300 cyber incidents were recorded, which is almost 70% more than the previous year, and in 2025 their number exceeded 5,900 cases, demonstrating a further increase of more than 30%. Such dynamics indicate the escalation of cyber threats and their systemic nature[1].

The EU experience shows that the investigation of criminal offenses at critical infrastructure facilities is complex and based on a combination of legal, organizational and technological mechanisms. It is worth noting that statistical data confirm the relevance of the problem in the European space: in 2024, the number of cyberattacks on critical infrastructure in the EU countries actually doubled, and up to 30% of all incidents were associated with disruption of key services. This situation indicates an increase in threats to basic life support sectors and the need to improve pre-trial investigation mechanisms. Globally, the number of such attacks is growing by at least 15% annually, and financial losses from cyber incidents reach an average of $4–5 million per case[2].

[1] International cybersecurity reports. (2025). Global cyber threat statistics report 2024–2025. URL: https://surl.li/sbcsyu

[2] International cybersecurity reports. (2025). Global cyber threat statistics report 2024–2025. URL: https://surl.li/sbcsyu

The final text of the Critical Entities Resilience Directive (CER) critical infrastructure' means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service[3].

We believe that critical infrastructure is defined as a set of facilities and systems, the disruption of which can cause significant or catastrophic consequences for society and the state. At the same time, the modern EU approach has transformed from the concept of "protection" to the concept of "resilience" of critical infrastructure, which involves not only countering threats, but also the ability to quickly recover from incidents.

The organizational system of investigation in the EU is characterized by a tendency towards centralization and unification of procedures, which is implemented through the activities of Europol, Eurojust and the European Public Prosecutor's Office (EPPO). We believe that an important feature of the investigation of criminal offenses at critical infrastructure facilities is the development of cross-border cooperation, in particular the creation of joint investigation teams and the application of the principle of mutual recognition of court decisions, which will allow for the effective investigation of crimes of a transnational nature.

As scientists rightly point out, an essential element is the use of an integrated approach to investigation, which combines the sectoral specificity of critical infrastructure facilities with a risk-based analysis of threats. At the same time, in modern conditions, a proactive investigation model is of particular importance, which involves the identification of potential threats at an early stage. This is achieved through the use of modern technologies, in particular, big data analysis, artificial intelligence and cyber incident monitoring systems[4].

We agree with the scientist Gerasymenko O.M. that the analysis of practical aspects of pre-trial investigation of criminal offenses at critical infrastructure facilities in the EU and the USA allows us to identify a number of problems and outline prospects for improving this activity. Thus, the key problems are: 1) technological challenges associated with the constant development and complication of attack methods; 2) legal restrictions that complicate the collection of electronic evidence and the conduct of cross-border investigations; 3) insufficient qualifications of investigators in the field of high technologies; 4) difficulties in establishing a balance between ensuring security and protecting the rights and freedoms of citizens; 5) problems of

[3] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[4] Herasymenko, O. M. (2025). Experience of pre-trial investigation of criminal offenses at critical infrastructure facilities in the EU and the USA: Theoretical, legal and organizational aspects. Analytical and Comparative Jurisprudence, (2), 973–982.

coordination between various bodies and agencies involved in the investigation.

At the same time, the analysis of the EU experience allows us to identify a number of problems in the field of investigation of criminal offenses on critical infrastructure facilities. These include the complexity of attribution of cyberattacks, jurisdictional conflicts between states, restrictions on access to electronic evidence, a shortage of qualified personnel, as well as the need to ensure a balance between security and respect for human rights. The problem of cross-border access to data is particularly relevant, which requires the unification of procedural mechanisms and the creation of common standards of evidence.

Taking into account the above, promising areas for improving the investigation of criminal offenses at critical infrastructure facilities are: harmonization of legislation of EU member states; development of digital justice; introduction of innovative technologies, in particular artificial intelligence; strengthening international cooperation; and improving the level of professional training of investigators.

As a **conclusion**, we can state that effective investigation of criminal offenses at critical infrastructure facilities in EU countries is possible only under the conditions of formation of a comprehensive, integrated and technologically oriented system that combines legal, organizational and innovative mechanisms for countering threats. The use of this experience is important for improving the national criminal justice system of Ukraine in the context of modern security challenges.