UDC 343.35:620.9(477)
DOI: 10.63341/naia-herald/1.2026.104

ISSN 2410-3594
E-ISSN 2786-7382

# Constructivist framework for analysing the criminal liability of officials for abuse in the energy market as a threat to Ukraine's critical infrastructure

**Mariia Shatalinska***
Postgraduate Student
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0009-0000-9077-1025

**Olena Tykhonova**
Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-3848-3023

■ **Abstract.** The purpose of the study was to determine to what extent the current model of criminal liability of officials in the energy market is effective and relevant to modern security challenges in the field of critical infrastructure. The research methodology combined historical-legal, systemic-structural, and discourse analysis of Ukrainian normative legal acts, as well as analytical reports. The research established that the current system of criminal-legal protection is a consequence of historical inertia and has inherited the shortcomings of the Soviet model, which was oriented towards ideological rather than technogenic threats. It was revealed that the general articles of criminal legislation on official crimes are qualitatively incapable of reflecting the specificity and scale of potential harm, as they are oriented towards individual consequences, rather than the threat of systemic collapse resulting from attacks on vital systems. It was proven that the privatisation processes in the 1990s created a gap in defining the subjects of liability among managers of private energy infrastructure operators. A significant gap was identified between outdated legal norms and new societal security expectations, formed under the influence of full-scale war. The conclusions were that the existing system of criminal liability is ineffective and requires immediate reform. The urgent necessity for developing and implementing into the Criminal Code specialised criminal offences with sanctions proportionate to the level of public danger of such acts was substantiated; this is intended to enhance the state's resilience and ensure the inevitability of punishment. The practical significance of the study lies in the fact that its results can be used by law-making bodies to develop effective legal mechanisms to protect the energy market as a subject of influence on the critical infrastructure of Ukraine

■ **Keywords:** national security; legal regulation; legislative gaps; strategic facilities; privatisation processes; energy infrastructure; energy market

## ■ Introduction

The resilience of energy infrastructure is a fundamental pillar of national security, economic welfare, and social stability for any modern state. For Ukraine, under conditions of ongoing full-scale military aggression, this issue has acquired fundamental significance. Systematic and targeted attacks on energy,

■ **Suggested Citation:**
Shatalinska, M., & Tykhonova, O. (2026). Constructivist framework for analysing the criminal liability of officials for abuse in the energy market as a threat to Ukraine's critical infrastructure. *Scientific Journal of the National Academy of Internal Affairs,* 31(1), 104-118. doi: 10.63341/naia-herald/1.2026.104.

■ *Corresponding author

■ Received: 28.10.2025; Revised: 26.01.2026; Accepted: 31.03.2026; Published: 02.04.2026

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

transport, and communication networks have transformed the protection of critical infrastructure from a purely managerial task into a key element of national survival and resilience. Against this backdrop, the problem of the adequacy and effectiveness of existing legal mechanisms arises, particularly the norms of criminal liability for officials who, by virtue of their authority, are directly responsible for the security and uninterrupted functioning of these vital systems.

Despite the obvious escalation and qualitative transformation of threats, the existing normative framework demonstrates signs of a clear incongruity with contemporary realities, creating a dangerous gap between the actual scale of challenges and the effectiveness of the state's legal response. These threats extend beyond traditional kinetic attacks, encompassing the cyber domain. H. Durojaye & O. Raji (2022) emphasised that state and state-sponsored actors deliberately exploit vulnerabilities in energy infrastructure to destabilise, spread disinformation, and diminish the defensive potential of the attacked state. As an example, the authors cited precisely Russia's cyberattack on Ukrainian energy companies in 2015, which led to power outages. The complexity of detecting and attributing such attacks makes the cyber domain a priority area for hybrid aggression, requiring cooperation between the public and private sectors. G. Ocieczek (2024) analysed key elements of ensuring security in the EU, paying particular attention to the new directives on the resilience of critical entities (CER) and on a high common level of cybersecurity (NIS 2). In the European Security Strategy (2020-2025), the protection of critical infrastructure and cybersecurity are defined as priorities. Against this backdrop, in Ukraine, the criminal-legal protection of critical infrastructure facilities is characterised by a lack of systematisation and fragmentation; certain terminological constructs in the Criminal Code[1] have lost their relevance, which complicates law enforcement (Fedyuk, 2025), and the universal norms on official crimes are incapable of reflecting the specificity and catastrophic scale of potential harm to vital systems (Office of the UN High Commissioner for Human Rights, 2024). This problem is not limited to a formal-dogmatic analysis of legislative acts, as legal norms are not static; they are social constructs, dynamically shaped by specific historical conditions, political interests, economic factors, and dominant societal perceptions of threats, responsibility, and justice.

The basis for a deep analysis of this problem is social constructivism. This approach, as noted in his work "Constructivism", S. Park (2023), has allowed for an understanding of how certain ideas and norms become generally accepted and how, in turn, societal changes become possible, challenging traditional rationalist theories. Examining constructivist approaches and institutional constructivism in the legal science of the European Union, D. Kostakopoulou (2024) refers to constructivism as the fourth force in theories of European integration, which testifies to its methodological maturity and significant influence on contemporary legal studies. Applied to the legal system, constructivism explains that laws are not an objective given, but are the result of a continuous process of social interaction, where various actors promote their interests and interpretations. Revealing the theoretical, methodological, and practical potential of social constructivism, V.P. Gorbatenko & O.V. Kukuruz (2021) emphasised its significant heuristic value for studying and transforming the political and legal reality precisely in Ukraine. The relevance of this approach for criminal law research is confirmed by the fact that the concepts of 'crime' and 'liability' are socially variable. For instance, defining "relativity (social constructivism)" as one of the key features of criminality, A.A. Ternavska & Y.A. Turlova (2024) emphasise its constructed nature. The application of this methodology allows not merely stating the existing shortcomings of legislation, but also understanding their genesis: why they arose, which historical events and political decisions shaped them, and why they have proven so resistant to change even under conditions of necessity.

Analysis of scientific literature indicates that the problem of critical infrastructure protection is actively researched by Ukrainian legal scholars. Thus, in the work of O.M. Gerasimenko (2024), based on an analysis of legislation and foreign experience, the conclusion is made about the relevance of the task of countering criminal offences at critical infrastructure facilities elements of which are also energy market objects, and the necessity of improving the corresponding legislative policy of Ukraine is substantiated. Researching the current state of criminal-legal protection of critical infrastructure facilities, S.E. Kucherina & D.O. Oleinikov (2021) conclude that it is unsystematic and fragmented, which, as the authors note, is due to the absence in criminal legislation of an individualised approach to critical infrastructure as a separate object of legal protection and the disregard in criminal law norms of the modern organisational and legal foundations for the functioning of such facilities. V. Fedyuk (2025), analysing the qualifying feature of critically important infrastructure facilities, additionally pointed out that the definition of the term "critically important infrastructure facilities", provided in the note to Art. 259

[1] Criminal Code of Ukrainian SSR. (1960, December). Retrieved from https://ips.ligazakon.net/document/view/kd0006?an=0&ed=1961_06_27.

of the Criminal Code of Ukraine[1], has lost its relevance, which complicates law enforcement. Concurrently, the issue of officials' liability is considered in a broader context. The peculiarities of criminal liability of officials of legal entities under private law were researched by D.M. Tychyna (2025), who, focusing on problematic aspects of qualification and law enforcement, substantiated the expediency of strengthening legislative regulation and state monitoring of anti-corruption measures in the private sector, which is of primary importance given the privatisation of part of the energy infrastructure facilities. The unconstitutionality of criminal liability for submitting inaccurate information in Ukraine was examined by A. Vozniuk *et al.* (2021), who concluded that the decision of the Constitutional Court declaring Article 366-1 of the Criminal Code[2] unconstitutional was insufficiently substantiated and lacked proper arguments regarding the absence of public harm in the act. This aspect is complemented by research on the legal regulation of ethics of conduct for public officials, in which V.S. Chernousov (2021) emphasised that reforming the public service is impossible without changes in the ethical attitude of officials, since their goal is the professional performance of the functions of a legal and social state. However, despite a significant body of research diagnosing the existence of the problem, its genesis remains insufficiently studied.

Thus, a significant lacuna exists in the scholarly discourse: there is a lack of comprehensive research explaining how and why the norms of criminal liability in the sphere of energy infrastructure were constructed in such a way that, as of 2025, they have proven ineffective. The purpose of the study was to analyse the evolution of the norms of criminal liability of officials in the energy market as a threat to the critical infrastructure of Ukraine. The central hypothesis of the study posited that applying a constructivist framework – which considers the conditions of the legislation's emergence, stakeholder interests, historically formed norms, political and economic factors, law enforcement practices, and alignment with societal demands – allows for demonstrating that Ukrainian legislation in this sphere contains profound historical lacunae. These lacunae, inherited from previous legal and political epochs, substantially diminish the effectiveness of legal regulation and render it maladapted to the complex threats of 2025.

## Materials and Methods

This study was grounded in the principles of qualitative methodology within the social constructivist paradigm. This approach enabled the examination of legal norms not as static and objective prescriptions, but as dynamic social constructs that are formed and transformed under the influence of historical conditions, political discourse, economic factors, and societal perceptions of threats and liability. The chosen methodological framework allowed for a profound analysis of the causes of lacunae in the legislation and its misalignment with contemporary challenges. To achieve the set goal and test the hypothesis, a complex of general scientific and special methods of cognition was applied. The historical-legal method was key to researching the genesis of the norms of criminal liability for public officials. Its application allowed for tracing the evolution of legislation from 1960 to 2025 – from the Soviet period, represented by the Criminal Code of the Ukrainian SSR of 1960[3], to the modern stage, encompassing the provisions of the current Criminal Code of Ukraine[4]. Its application was directed at identifying the continuity and transformation of legal approaches across different historical epochs, particularly after the proclamation of Ukraine's state independence in 1991. Systemic-structural analysis was used to study normative-legal acts as a unified system. This method was applied with the aim of establishing connections and contradictions between general norms of criminal law and special legislation, such as the Law of Ukraine "On Critical Infrastructure"[5] and CMU Resolution No. 415[6], which regulates the maintenance of the Register of Critical Infrastructure Objects. Its application was directed at identifying systemic lacunae and a lack of coherence in legal regulation. Discourse analysis was applied to study analytical reports and official documents. This method allowed for analysing how the concepts of "energy infrastructure",

[1] Criminal Code of Ukrainian SSR. (1960, December). Retrieved from https://ips.ligazakon.net/document/view/kd0006?an=0&ed=1961_06_27.
[2] Decision of the Constitutional Court of Ukraine in Case No. 1-24/2020(393/20) on the Constitutional Submission of 47 People's Deputies of Ukraine Regarding the Compliance with the Constitution of Ukraine (constitutionality) of Certain Provisions of the Law of Ukraine "On Prevention of Corruption" and the Criminal Code of Ukraine. (2020, October). Retrieved from https://zakon.rada.gov.ua/laws/show/v013p710-20#Text.
[3] Criminal Code of Ukrainian SSR. (1960, December). Retrieved from https://ips.ligazakon.net/document/view/kd0006?an=0&ed=1961_06_27.
[4] Ibidem, 1960.
[5] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[6] Resolution of the Cabinet of Ministers of Ukraine No. 415 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing and Providing Information from It". (2023, April). Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.

"critical infrastructure", "threat", and "liability" were constructed in expert and political discourse. The analysis of sources such as the report by S.I. Kondratov & O.M. Sukhodolia (2020), dedicated to the organisational and legal principles of critical infrastructure protection, was used to identify key ideas and narratives that dominated the expert discourse and influenced the process of forming the relevant legislation. The informational basis for the research comprised a complex of interconnected sources. To assess the current state of threats and the effectiveness of state policy, data from international and national reports were used. Specifically, these included the report by the Office of the UN High Commissioner for Human Rights (2024), the chronology of cyberattacks from the European Parliament (2022), as well as the analytical reports "The State Critical Infrastructure Protection System in the National Security System" (2020) and ACTED (2020). For the legal analysis within a broader socio-political context, scholarly works illuminating the transformation processes of Ukrainian society were engaged.

## Results

**The historical evolution and socio-cultural construction of norms of criminal liability for public officials in the sphere of Ukraine's energy infrastructure.** The analysis of criminal liability for public officials in the sphere of Ukraine's critical infrastructure in general, and in the energy market, in particular, through the prism of a constructivist framework required detailed elaboration within the historical context of the formation of the relevant legislation. The norms regulating this sphere are not static or objectively predetermined. They are the result of the interaction of social, political, economic, and cultural factors that have been constructed over decades. Understanding this evolution allowed for uncovering the roots of existing lacunae and imbalances that may diminish the effectiveness of contemporary legal regulation. Historically, the concept of "critical infrastructure" in Ukraine, as in other post-Soviet states, evolved under the influence of the Soviet administrative-command management system. During this period, key life-sustaining facilities – particularly, energy complexes (power plants, distribution networks), transport hubs (railways, port facilities, airports), as well as communication systems (telecommunication networks, radio relay stations) – were exclusively state-owned and operated under the centralised control of relevant sectoral ministries and departments (for example, the Ministry of Energy and Electrification of the USSR, the Ministry of Railways of the USSR, etc.).

The system of liability for public officials within this paradigm was predominantly focused on preventing actions that could harm the functioning of these "strategically important" facilities, which were perceived as elements of a unified national economic complex. Criminal-legal liability, as enshrined in the relevant articles of the Criminal Code of the Ukrainian SSR of 1960[1] (for instance, Art. 61 "Wrecking" (which was interpreted as the non-performance or negligent performance of certain duties with the aim of undermining industry, transport, agriculture, the monetary system, trade, etc.), Art. 60 "Sabotage" (committing, with the aim of weakening the state, explosions, arson, or other actions aimed at the mass destruction of people, inflicting bodily harm or other injury to their health, damaging or destroying enterprises, structures, routes and means of communication, means of communication or other state or collective property), as well as Art. 172 "Official Negligence" (negligent attitude towards service, which caused substantial harm)), was aimed at protecting state security in its traditional understanding. This implied countering actions that would undermine the economic or defensive might of the state. However, the key focus of this regulation was on protecting the stability of state governance and economic integrity, rather than on the comprehensive protection against a broad spectrum of modern threats. These include phenomena such as high-tech cyberattacks, international terrorism with its asymmetric methods, or large-scale emergencies of technogenic and natural character, which lacked a direct ideological basis. The absence of corresponding legal constructs and managerial practices in the Soviet system was conditioned by a different nature of threats, perceptions of technology, and the political doctrine, which formed certain historical lacunae in the subsequent development of Ukrainian legislation.

**Table 1.** Evolution of criminal liability of officials for offences in the energy market (1960-2025)

| Period | Regulatory document | Example articles | Regulatory focus | Key limitations |
|---|---|---|---|---|
| 1960-1991 (USSR/ Ukrainian SSR) | Criminal Code of the Ukrainian SSR[2] (1960) | Art. 60 "Sabotage", Art. 61 "Wrecking", Art. 172 "Official Forgery" | Protection of state security, countering wrecking | Focus on ideological threats, disregard for technological and cyber risks |
| 1991-2000 | Post-independence transition period | General articles of the Criminal Code of Ukraine | Adaptation of the Soviet model | Lack of special provisions for critical infrastructure |

[1] Criminal Code of Ukrainian SSR. (1960, December). Retrieved from https://ips.ligazakon.net/document/view/kd0006?an=0&ed=1961_06_27.

[2] Ibidem, 1960.

*Table 1. Continued*

| Period | Regulatory document | Example articles | Regulatory focus | Key limitations |
|---|---|---|---|---|
| 2001 | Criminal Code of Ukraine[1] (new version) | Art. 364, Art. 367 | Universal liability of officials | No qualifying attribute of "critical infrastructure" |
| 2010-2020 | Legislative amendments, international influences | Art. 364-1 (Officials of private legal entities) | Partial expansion of subjects | Failure to account for the specifics of private critical infrastructure operators |
| 2021 | Law of Ukraine "On Critical Infrastructure"[2] | – | Definition of sectors, objects, subjects | No amendments introduced to the Criminal Code of Ukraine |
| 2025 (Current State) | Current State | – | Need for specialised offence compositions | Sanctions do not correspond to the scale of public danger |

**Source:** created by the authors based on an analysis of the following sources: S.I. Kondratov & O.M. Sukhodolia (2020), Office of the UN High Commissioner for Human Rights (2024)

Ukraine's attainment of independence in 1991 opened up new opportunities for the formation of its legal system. However, a significant part of the legislation, particularly in the sphere of security and infrastructure management, was based on inherited Soviet approaches. The relevant articles of the Criminal Code of Ukraine[3] (CCU) concerning official offences (e.g., Art. 364 "Abuse of Authority or Office", Art. 367 "Official Negligence") were adapted, but their underlying logic remained within the framework of classical criminal law, failing to account for the specifics and growing complexity of critical infrastructure.

An analysis of the key CCU[4] articles has allowed for the identification of systemic shortcomings in their application to the sphere of critical infrastructure, indicative of historically formed gaps. Firstly, the general nature of the object of the crime and its consequences is defining. All the mentioned CCU[5] articles operate with such broad categories as "legally protected rights, freedoms, and interests of individual citizens, or state or public interests, or the interests of legal entities". Criminal-legal consequences are defined through "substantial harm" and "grave consequences", tied to an economic criterion – a multiple exceeding of the non-taxable minimum income of citizens (Part 3, 4 of the Note to Art. 364 CCU[6]). However, these formulations do not reflect the unique nature and potentially catastrophic scale of harm that can be inflicted upon critical infrastructure. Disruption of the functioning of its objects can lead to systemic collapse (e.g., a national blackout, cessation of water supply, complete blockage of telecommunication networks), which poses an existential threat to the state and society, extending far beyond purely economic losses or harm to the rights of individual citizens. Such consequences may include threats to national security, mass casualties, and long-term social and economic destabilisation, which are not fully captured by the current definition of "serious consequences," "significant losses," or "significant harm."

Secondly, a key shortcoming is the lack of focus on specific threats. Articles 364 and 367 of the CCU[7] are concentrated on general intentional abuse or negligent performance of official duties. However, they do not contain references to the unique risks and threats characteristic of critical infrastructure, such as targeted cyberattacks, terrorist acts, physical sabotage, or large-scale technological disasters caused by the actions or inaction of officials. This leads to, for example, official negligence that resulted in a critical vulnerability of a system to a cyberattack being qualified in the same manner as negligence in any other sphere, without due consideration of the potentially catastrophic consequences for the country's vital sustenance. Thirdly, there is an issue with defining the subject of the offence, particularly in the private sector. Although Art. 364-1[8] of the CCU expands the range of subjects, including officials of private legal entities, its application to energy market operators, who are often private companies or operate under complex concession/lease agreements, remains challenging. The definition of an "official" in the Note to Art. 364 CCU[9], although broad, is still predominantly oriented towards traditional state and municipal structures or legal entities with a dominant state/municipal share. In the case of complex

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[4] Ibidem, 2001.
[5] Ibidem, 2001.
[6] Ibidem, 2001.
[7] Ibidem, 2001.
[8] Ibidem, 2001.
[9] Ibidem, 2001.

corporate structures or international energy market operators, clearly identifying the specific individual responsible for compliance with specific energy infrastructure security standards, which do not always coincide with general "administrative-economic" or "organisational-administrative functions", remains a significant challenge, creating a field for the "diffusion" of personal responsibility. Fourthly, there is an observed inadequacy of sanctions relative to the scale of the threats. The sanctions provided for by Articles 364 and 367 of the CCU (namely, probationary supervision, restriction of liberty, or imprisonment for a term of up to three to six years, fines) may prove disproportionate to the public danger of acts leading to significant disruptions in the functioning of energy market facilities, and as a consequence, critical infrastructure, especially under martial law. For instance, official negligence resulting in the death of a person (Part 3, Art. 367) is punishable by imprisonment for a term of five to eight years.

However, a system failure at an energy infrastructure facility caused by similar negligence could lead to a significantly larger number of casualties or destabilisation on a nationwide scale, necessitating a review of the adequacy of the punishment. Finally, a substantial gap is the absence of a special qualifying attribute of "critical infrastructure". None of the aforementioned articles contains such a qualifying feature as "committing a crime that disrupted the functioning of critical infrastructure". This means that the legal system does not construct an elevated public danger for such acts, treating them as ordinary official crimes, ignoring their strategic impact on national security and societal viability. The stakeholders at this stage were state structures: law enforcement agencies, the Security Service of Ukraine, ministries managing relevant sectors (which exercised control over the critical infrastructure object and were responsible for its current functioning[1]). The private sector, which, starting from the 1990s, began to play a significant role in the operation and management of part of the critical infrastructure, had minimal influence on the formation of these norms (Snelbecker, 1995). This created a certain asymmetry, whereby the norms were constructed without fully considering the interests and challenges faced by private operators.

Political and economic factors also played a decisive role in the construction of these norms. The period of privatisation and the formation of oligarchic structures in the 1990s and early 2000s led to a significant portion of energy infrastructure (particularly in energy and transport) being transferred to private enterprises or controlled by financial-industrial groups (Minakov, 2023). This created a paradoxical situation: assets vital to the functioning of the state and society came under the influence of private interests. However, legislation on the liability of public officials was not adequately adapted to these new realities. Significant gaps existed in defining the subjects of liability, their powers, and duties within the context of private management of energy infrastructure. The absence of clear mechanisms for state control and an adequate level of liability for private operators' failure to comply with safety requirements created circumstances where societal interests could be ignored for the sake of profit.

The formation of the concepts of "energy infrastructure" and "critical infrastructure" as a distinct legal field in Ukraine began considerably later, under the influence of European and international standards, especially after the Orange Revolution of 2004 (OSCE, 2004) and the Council of Europe Office in Ukraine (2015). These events stimulated aspirations for Euro-integration and the modernisation of the legal system. However, even then, the process of implementing international practices was slow and fragmented due to the absence of a unified state strategy and the dispersion of responsibility among various agencies. Active discussion on the necessity of a systemic definition and protection of energy infrastructure, involving expert communities and analysis of EU country experiences, began only in the late 2010s, particularly following the 2015-2016 cyberattacks on Ukraine's energy system, which demonstrated the vulnerability of critical sectors (European Parliament, 2022). This discussion encompassed issues of terminology, criteria for designating assets as an energy and critical infrastructure, and mechanisms for interagency cooperation. The relevant legislation, namely the Law of Ukraine "On Critical Infrastructure"[2], was adopted only in 2021. Prior to the adoption of this Law, criminal liability of public officials in this sphere was regulated exclusively by general norms of the Criminal Code of Ukraine[3], such as Articles 364, 367, and, in the case of sabotage or terrorist acts, Articles 113 and 258 respectively. These norms did not account for the unique risks and threats specific to critical infrastructure and were insufficient to ensure its comprehensive protection.

These historically formed norms and law enforcement practices demonstrated significant gaps. Firstly, the absence of a clear legislative definition of "critical infrastructure" and its components in Ukrainian

[1] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[2] Ibidem, 2021.
[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

regulatory acts prior to the adoption of the Law of Ukraine "On Critical Infrastructure"[1] in 2021 complicated the qualification of crimes related to its disruption. This lack of unified criteria for criticality and identification of relevant assets created legal uncertainty, potentially hindering the investigation of incidents and the prosecution of individuals whose actions or omissions led to failures in the functioning of vital systems.

**There is still no legislative definition of the "energy market".** Secondly, even with the existence of general norms on official crimes, a problem could arise in determining the subjects of criminal liability. Within the context of the complex ownership and management structure of energy infrastructure assets, encompassing state, municipal, and private enterprises, as well as companies operating under concession or lease agreements, the absence of specialised legislation could complicate the identification of the specific public official bearing direct responsibility for compliance with safety standards and the uninterrupted functioning of the relevant asset. The third gap lay in the inadequacy of sanctions to the nature of the threats. Even in cases where public officials were held liable under general articles of the Criminal Code of Ukraine[2], the penalties did not reflect the actual scale of harm caused by the disruption of energy infrastructure. This indicated that the legislation was not constructed with due regard for modern risks, such as mass cyberattacks, terrorist acts, or large-scale technological disasters, where liability should be significantly more severe.

Criticism and proposals from interested agencies, such as national security experts, human rights organisations, and international partners (Aebi *et al.*, 2024). They noted that Ukrainian legislation does not meet modern societal demands for security and protection and is not adapted to new challenges. In particular, after 2014, in the context of hybrid aggression by the Russian Federation, the issue of protecting energy infrastructure, including energy networks, telecommunications, and transport routes, acquired existential significance (European Parliament, 2022). However, despite the need, introducing systemic amendments to criminal legislation was protracted, reflecting the difficulty of political consensus and the influence of various interests on the law-making process.

Thus, the historical evolution of criminal liability of public officials in the sphere of energy market as a threat to Ukraine's critical infrastructure, demonstrated that the norms were constructed under the influence of different eras and challenges, often without sufficient awareness of the unique threats associated with vital systems. This led to the formation of a legal field containing significant gaps in definitions, subject composition, crime qualification, and the adequacy of sanctions. These gaps, in turn, substantially reduce the effectiveness of legal regulation and leave the system vulnerable to new, dynamic challenges of 2025, especially under the conditions of the ongoing Russo-Ukrainian war, where energy infrastructure becomes a primary target and the energy market is gaining in importance.

**Current status and law enforcement practices in identifying gaps in the regulation of criminal liability of officials in the energy market as a threat to critical infrastructure.** Despite the adoption of the Law of Ukraine "On Critical Infrastructure"[3] in 2021, as well as the subsequent adoption of related regulatory acts, in particular CMU Resolution No. 415[4], systemic gaps, whose roots lie in the historical construction of norms, continue to affect the effectiveness of legal regulation. These gaps are revealed not only at the level of legislative definitions but also in real law enforcement practices, reflecting the complex interaction between legislative intent, stakeholder interests, and objective challenges, especially under conditions of full-scale war. The Law "On Critical Infrastructure"[5] became a primary step in defining the very concept of "critical infrastructure" and its sectors, identifying objects and subjects responsible for ensuring their security. It outlined general principles and powers of state authorities in this sphere. However, from the perspective of criminal law, this law did not introduce systemic changes to the Criminal Code of Ukraine[6] that would create special offences specifically targeting violations in the sphere of energy market and critical infrastructure. Public officials are still held liable under general articles of the Criminal Code of Ukraine[7] on official crimes (abuse of power/official position, official

[1] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[4] Resolution of the Cabinet of Ministers of Ukraine No. 415 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing and Providing Information from It". (2023, April). Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.
[5] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[6] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[7] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

negligence, embezzlement of property), and, in some cases (where the actions of a public official affect the functioning of a system), under articles on crimes against public safety or production safety. This approach ignores the unique nature of threats and potential consequences of violations concerning energy market facilities. The absence of special norms leads to criminal liability often failing to reflect the full social danger of the acts.

Conformity with modern societal demands and challenges of 2025 is defined by the fact that russia's war against Ukraine has transformed energy market facilities and critical infrastructure objects into systemic targets, and society – vulnerable to disruptions in the provision of vital services. In the period from October 2022 to March 2023, Russian forces carried out large-scale attacks on the Ukrainian energy system, leading to the destruction or damage of over 50% of the country's generating capacity and mass disruptions of electricity, heating, and water for millions of civilians (Office of the UN High Commissioner for Human Rights, 2024). Similar attacks recurred in 2024: in January and March, combined missile and drone strikes on thermal power plants and substations were recorded, leading to prolonged disruptions in Kyiv, Kharkiv, Dnipro, and other cities, and in June 2024, Ukrainian government structures reported a peak-hour electricity deficit of up to 1.5 GW (Office of the UN High Commissioner for Human Rights, 2024). The scale and regularity of these attacks demonstrated that the disruption of energy supply had become not a temporary phenomenon, but a strategy of the aggressor aimed at destabilising society. In this context, societal expectations in 2025 include not only the physical restoration of damaged assets but also the creation of mechanisms for full legal liability of public officials for the inadequate provision of resilience and functioning of energy infrastructure. According to the analytical report by the S.I. Kondratov & O.M. Sukhodolia (2020), Ukraine had not completed the creation of a unified register of critical infrastructure objects, had not implemented a full-fledged system for certification and categorisation of such objects, in particular, energy infrastructure, and the regulatory framework remained fragmented among various bodies (Table 2).

**Table 2.** Identified gaps and societal expectations regarding criminal liability in the sphere of critical infrastructure (2020-2025)

| Category | Status prior to 2020 | Challenges 2022-2024 | Societal expectations in 2025 |
|---|---|---|---|
| Register of critical infrastructure objects | Non-existent, fragmented departmental databases | CMU Resolution No. 415[1] formalised the register | Full population of the register, transparent access |
| Liability Subject | Uncertainty for private operators | Increased role of private energy companies | Clear criminal liability for managers of private structures |
| Offence qualification | General Articles of the CCU (364, 367)[2] | Mass cyberattacks and shelling (2022-2024) | Introduction of specialised offence elements |
| Sanctions | Universal, disproportionate | Blackouts, deficit up to 1.5 GW, harm to millions | Proportional punishments, considering the scale of consequences and the martial law state |
| Social dimension | Lack of a culture of accountability | Dependence of people's lives on CI (hospitals, water supply) | Formation of a "culture of accountability" among officials and society |

**Source:** created by the authors based on the analysis of the following sources: S.I. Kondratov & O.M. Sukhodolia (2020), ACTED (2020), Office of the UN High Commissioner for Human Rights (2024)

Consequently, there was uncertainty regarding the personal liability of operators and officials: on the one hand, certain Resolutions of the Cabinet of Ministers of Ukraine defined requirements for cyber protection and technical accounting, on the other hand – criminal legislation lacked specialised elements of offences for gross official negligence or failure to fulfil duties related to preparing resilience plans in the sphere of critical infrastructure (Kondratov & Sukhodolia, 2020). A key step was the adoption of the Resolution of the Cabinet of Ministers of Ukraine No. 415[3], which for the first time formalised the procedure for maintaining a centralised state register of critical infrastructure objects. However, even after its adoption, questions regarding the coordination of inter-agency mechanisms, the practical

[1] Resolution of the Cabinet of Ministers of Ukraine No. 415 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing and Providing Information from It". (2023, April). Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 415 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing and Providing Information from It". (2023, April). Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.

implementation of certification, and determining the liability of officials for failure to perform their duties remain open, indicating the necessity for further changes in legislation and law enforcement.

International assessments confirm the critical nature of the problem. In September 2024, Office of the UN High Commissioner for Human Rights (2024) noted that attacks on energy infrastructure have "reverberating consequences" for healthcare, education, and the economy, as power cuts deprived hospitals of access to oxygen concentrators and ventilators, and schools of the ability to continue the educational process. Simultaneously, the report by the ACT-ED (2020) emphasised that the absence of systemic monitoring and a shared database on technogenic and natural threats significantly limits preparedness for crisis situations, including repeated attacks on energy and water systems.

Thus, in 2025, the formation of legal norms and state policy should be based on the understanding that energy infrastructure is not merely "strategic objects", as in Soviet terminology, but a complex of vital systems, upon which the survival of society depends during war. Clear elements of criminal offences are needed, encompassing: a) intentional acts – sabotage or collaboration with the aggressor, which lead to the destruction of energy infrastructure; b) gross official negligence, which prevented the uninterrupted functioning or restoration of objects; c) breaches of duties regarding planning and preparation, which create systemic risks. Furthermore, it is worth enshrining a norm on the priority provision of energy and water to social sphere objects (hospitals, water purification systems, educational institutions) (Office of the UN High Commissioner for Human Rights, 2024). Only such an approach will meet societal demands and the challenges of wartime, adequately reflecting the increased danger of new types of threats and ensuring citizens' trust in state institutions.

**Effectiveness, compliance, and adaptation: constructivist proposals for enhancing the criminal liability of officials in the energy market as a prerequisite for ensuring the security of critical infrastructure.** The constructivist approach in researching the criminal liability of officials in the sphere of critical infrastructure allows for the formulation of specific directions for improving legislation, taking into account the real societal challenges of 2025. The current articles of the Criminal Code of Ukraine[1], namely Art. 364 "Abuse of Power or Official Position" and Art. 367 "Official Negligence", remain universal and do not account for the specifics of critical infrastructure functioning in general, and energy infrastructure in particular. In this regard, it is advisable to develop separate, specialised articles: "Failure to Comply with Critical Infrastructure Security Requirements" – to criminalise inaction or intentional violation of established standards for the physical or cyber protection of critical infrastructure objects. "Disruption of Critical Infrastructure Functioning" – to cover acts or omissions that led to disruptions in the provision of electricity, water supply, transport, or communications. "Concealment of Information about Threats or Incidents in the Sphere of Critical Infrastructure" – to establish liability for officials who knowingly failed to report or distorted data about attacks, sabotage, or technogenic accidents. Furthermore, sanctions for such offences must be differentiated depending on the criticality level of the object and the scale of the harm. Thus, if official negligence led to a local incident, the punishment could be milder; however, in cases of systemic blackouts or a national power outage, the sanction should be significantly more severe. The qualifying feature "commission of a crime during the martial law state" must necessarily be considered, as it increases the level of public danger and requires enhanced punishment. Thirdly, the subject composition of criminal liability requires clarification. According to the note to Art. 364 of the CCU[2], officials are defined as representatives of authority or persons with organisational-administrative functions. However, this definition does not encompass managers of private companies who, on the basis of concession or lease agreements, manage critical infrastructure objects. It is necessary to legislatively establish that they also bear criminal liability for non-compliance with security requirements on an equal footing with officials of state and municipal enterprises. Fourthly, an important direction is strengthening inter-agency coordination. The Law of Ukraine "On Critical Infrastructure"[3] of 2020 and the CMU Resolution No. 415 of 28 April 2023[4] define the general principles for the accounting and management of critical infrastructure objects, including energy infrastructure, but do not regulate mechanisms for responding to crimes. For this purpose, it is necessary to create protocols for interaction between the Prosecutor's Office, the Security Service of Ukraine, the State Service for Special Communications and Information Protection, the Ministry of

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Ibidem, 2001.
[3] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[4] Resolution of the Cabinet of Ministers of Ukraine No. 415 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing and Providing Information from It". (2023, April). Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.

Energy, and operators of critical infrastructure objects, which would ensure a rapid response to incidents. Furthermore, investigating crimes in the sphere of critical infrastructure requires specialised knowledge in the fields of energy, transport, IT, and cybersecurity. Therefore, it is necessary to introduce training programmes for investigators and prosecutors, who will possess the competence to qualify such crimes and establish the causal link between official negligence and the large-scale consequences for society.

Finally, the paramount objective is the cultivation of a "culture of responsibility". Critical infrastructure, and especially energy facilities, must be perceived by society and public officials not as ordinary strategic assets, but as the foundation of national survival and state resilience. This necessitates not only the inevitability of punishment for crimes in this sphere but also public awareness campaigns that foster an understanding of the significance of critical infrastructure security for citizens' lives. Such measures are consistent with international recommendations, particularly the conclusions of the Office of the UN High Commissioner for Human Rights (2024), which emphasised the vital importance of protecting energy infrastructure for population access to healthcare, education, and essential services. Collectively, these proposals are aimed at remedying historical gaps in legal regulation and establishing a criminal law mechanism capable of adequately responding to the challenges of war and post-war recovery, thereby ensuring the efficacy, relevance, and adaptability of legislation to contemporary societal needs.

## Discussion

The results of this study indicate that the criminal law framework for protecting critical infrastructure in Ukraine is in a phase of active development, yet simultaneously faces a complex of systemic problems, caused both by the war and by global transformations in the security domain. A key finding is the necessity of transitioning from the universal provisions of the Criminal Code of Ukraine, such as Article 364 ("Abuse of Power or Official Position") and Article 367 ("Official Negligence"), to specialised criminal offences that account for the specificities of critical infrastructure operations, including energy facilities. This confirms that public consciousness in Ukraine has undergone significant changes in recent years: infrastructure assets are no longer perceived as abstract strategic assets but are regarded as vital life-support systems, upon which the survival of society and the state during war and in the process of post-war recovery depends.

The application of a constructivist approach has allowed for the explanation of this transformation. As emphasised by D.M. McCourt (2022), it is norms, ideas, and social perceptions that determine not only the behaviour of states but also the content of legal institutions. M. Buckley (2025), in this context, stressed that constructivism proceeds from the active role of thought, which creates social reality, and consequently, laws are formed not in isolation from society but as a reflection of its needs and collective perceptions. The obtained results demonstrate precisely this process: a new norm is emerging in Ukraine, according to which negligence in the infrastructure sphere is deemed equivalent to a threat to national security, and responsibility for the continuity of its operation is becoming a societal expectation. This conclusion is consistent with international research. A. Locatelli (2021) demonstrated that following the end of the Cold War, the concept of security underwent a radical revision. Traditional military threats gradually lost their dominant significance, giving way to the prominence of issues related to internal conflicts, terrorism, and attacks on infrastructure. A similar dynamic is evident in the Ukrainian experience, where in 2022-2025 the primary targets of Russian attacks were energy and communication systems. Y. Yigit *et al.* (2024) proved that modern threats combine both physical and cyber components, and the protection of critical infrastructure is impossible without the integration of technical, legal, and social solutions. This correlates with the finding of this study on the necessity of creating new criminal offences that would consider not only negligence in physical management but also cyber threats and the concealment of information about them. Concurrently, the identified problems in Ukraine align with global trends, confirming the universality of challenges in critical infrastructure protection, as shown in the analysis of the legal systems of Poland (Roman & Cygańczuk, 2022) and international legal approaches in general (Ilic, 2023). However, the specificity of the Ukrainian context lies in the fact that reform is hampered not only by objective threats but also by the state of national legal scholarship. As noted by V.V. Sokurenko (2023), Ukrainian criminology, despite moving towards the implementation of modern methodologies, remains influenced by outdated approaches, which explains the identified historical inertia of legislation and the persistence of inefficient legal constructs identified in the study.

An illustration of the dynamics of societal perceptions is provided by the research of M. Sallinen (2021), dedicated to the shift in American discourse on cyber weapons following the discovery of Stuxnet. The author showed that over a decade, not only political decisions changed but also the informal norms that defined society's attitude towards cyber operations. Similar processes are observed in Ukraine, where mass shelling of the energy system and cyberattacks by Russia have transformed public expectations regarding what is permissible and

what should be criminalised at the legislative level. J.N. Pardede & P.H. Poluakan (2021) supplement this conclusion, asserting that critical constructivism in law allows for avoiding the absolutisation of norms and preserving space for their constant re-evaluation. The Ukrainian example confirms this view: the formulation of new articles of the Criminal Code cannot be merely a declarative act; it must be based on the continuous analysis of societal risks, technological changes, and international experience.

A similarity to results in pedagogy is demonstrated by the research of K. Meli *et al.* (2022), who showed that teaching fundamental scientific principles becomes effective only when students themselves participate in building conceptual models. Similarly, legal provision in the sphere of energy infrastructure cannot be imposed exclusively "from above"; it must be formed through the interaction of the state, operators, and society, which confirms this study's conclusion on the necessity of cultivating a culture of responsibility. The research of H. Wijesinghe *et al.* (2024) on the Russian-Ukrainian war showed that the reactions of neighbouring states to Russia's aggressive policy are determined not only by contemporary realities but also by historically formed perceptions and collective memory. This aligns with the Ukrainian experience, where citizens' demands for enhanced criminal liability for negligence in the infrastructure sphere are based not only on the actual blackouts of 2022-2025 but also on a long history of vulnerability to external threats. Applying a constructivist approach to power exchange in the context of the Russian-Ukrainian conflict, B.W. Nugroho (2024) showed that it is precisely norms, shared identities, and dominant discourses and narratives that play a key role in shaping power relations between states. This fully correlates with this study's conclusion that the new societal demand for enhanced responsibility for infrastructure protection is a result of the formation of a new national security narrative, generated by the war. A similar effect was described by A. Matczak (2024), who analysed the role of public voice in criminology and emphasised that citizens' perceptions of crime and punishment are dynamic and depend on the dominant discourse. The results demonstrate an analogous process: the expectation of strict liability for official negligence in the energy sector reflects a change in societal norms, not merely a situational reaction to a crisis.

A theoretical summary is the confirmation of the conclusions of F. Kratochwil & H. Peltonen (2022), who noted that constructivism in political and social sciences has undergone waves of development and transformations; however, it is precisely during crisis periods that its analytical potential is fully revealed. The Ukrainian case proves that only through a constructivist approach can one explain why society demands the creation of new norms, even if the existing legislation formally already covers certain acts. In this context, the works of C. Larrinaga & J. Bebbington (2021) on the institutionalisation of sustainability reporting also provide a parallel example. They proved that new practices are formed not instantaneously but through the gradual combination of institutional conditions, actors, and discourse. In Ukraine, the process of creating criminal law protection for energy infrastructure follows a similar logic, where various institutions and societal forces step by step build a new system of norms.

Overall, the results of the study have a dual significance. Firstly, they outline specific directions for reforming Ukrainian criminal legislation towards the introduction of specialised criminal offences that would correspond to the modern challenges of war and post-war recovery. At the same time, as shown by the comparative study of the public official as a victim of criminal insult and defamation, A. Borovyk *et al.* (2023) demonstrated that models of criminal liability of officials in different jurisdictions vary significantly, balancing the principle of freedom of speech and the necessity of protecting representatives of authority. This indicates that the reform process in Ukraine must consider international experience, not through copying, but by creating balanced legal constructs adapted to the national context. Secondly, they confirm the global trend of transforming perceptions of security, where not only technical or legal mechanisms play a key role, but also the norms, discourses, and collective perceptions of society. In this sense, the Ukrainian experience is consistent with the conclusions of D.M. McCourt (2022), M. Sallinen (2021), and Y. Yigit *et al.* (2024) and simultaneously contributes to the international discussion, showing that energy infrastructure in the 21st century is becoming not only an object of physical or cyber protection but also a component of societal identity and a mechanism of collective survival.

## Conclusions

The conducted research comprehensively confirmed the central hypothesis and established that the current system of criminal liability of officials in the field of energy market protection, as a subject of influence on critical infrastructure in Ukraine, is a result of historical evolution, rather than deliberate design in response to contemporary threats. It was ascertained that the legislation contains profound structural gaps that diminish its preventive and punitive potential. The analysis demonstrated that the roots of the problem trace back to the Soviet legal doctrine, which was oriented towards ideological threats to state security and ignored technological and specific infrastructural risks. The general norms of the Criminal Code inherited after 1991, namely

Articles 364 and 367, proved qualitatively incapable of encompassing the full scope of the social danger of acts encroaching upon vital systems. Their blanket wording of "substantial harm" fails to capture the potentially catastrophic, cascading effects of power grid outages, especially under martial law. Privatisation processes further complicated the issue, creating uncertainty regarding the subject composition of criminal liability in the private sector managing strategic facilities. Thus, it was proven that the full-scale aggression of 2022-2025 acted as a catalyst, revealing a critical discrepancy between the outdated legal framework and the new social norm that views energy infrastructure security as an existential condition for the nation's survival.

The obtained results hold significant practical importance. Based on them, a number of recommendations aimed at reforming criminal legislation have been formulated. The primary task is the development and implementation of specialised criminal offences into the Criminal Code of Ukraine. These norms should criminalise acts directly pertaining to the sphere of energy infrastructure, namely: intentional or grossly negligent failure to comply with established standards of physical and cyber protection; inaction that led to the disruption of a energy infrastructure facility's operation; concealment of information about incidents or threats. Sanctions for such crimes must be proportional to the scale of the consequences, and the commission of an act under martial law should constitute an aggravating circumstance that significantly intensifies liability. Furthermore, it is recommended to broaden the definition of the subject of a crime, explicitly extending it to the managers of private companies that are energy infrastructure operators.

The research had certain limitations. Firstly, it was focused predominantly on normative-legal analysis and constructivist interpretation, without including an empirical study of judicial-investigative practice due to the objective difficulty of accessing relevant data during a period of active hostilities. Secondly, the analysis was conducted under conditions of a dynamic security and legal situation; therefore, the conclusions reflect the state of the problem at the current moment, requiring their further clarification and updating in future research.

Directions for further scientific research may include: an in-depth comparative legal analysis of the legislation and practice of holding officials accountable for abuse in the energy market as a threat to critical infrastructure in countries with experience in countering hybrid threats; an empirical study of court decisions in the relevant category of cases after accumulating a sufficient amount of data; a sociological study of the level of legal awareness and culture of responsibility among the management of energy market facilities in Ukraine.

## Acknowledgements

None.

## Funding

The study was not funded.

## Conflict of Interest

None.

**References**

[1] ACTED. (2020). *Analytical report "The status of Ukrainian legislation regulating environmental and technogenic risks in the context of the priorities of the Sendai Framework for Disaster Risk Reduction"*. Retrieved from https://archive.r2p.org.ua/wp-content/uploads/2020/10/report on eco tech risks 3p-consortium.pdf.

[2] Aebi, S., Hauri, A., & Kamberaj, J. (2024). *Critical infrastructure resilience in Ukraine: Energy, transportation, and communication*. Zürich: Center for Security Studies. doi: 10.3929/ethz-b-000662463.

[3] Borovyk, A., Tkachenko, I., Derevyanko, N., & Diakin, Y. (2023). Public official as a victim of criminal insult and defamation: Comparative research. *Cuestiones Políticas*, 41(78). doi: 10.46398/cuestpol.4178.50.

[4] Buckley, M. (2025). Constructivism. In *Encyclopedia of global justice* (pp. 1-4). Berlin, Heidelberg: Springer Berlin Heidelberg.

[5] Chernousov, V.S. (2021). *Legal regulation of the ethics of behaviour of civil servants*. Retrieved from https://surl.lu/zmsllz.

[6] Council of Europe Office in Ukraine. (2015). *Revolution of dignity*. Retrieved from https://www.coe.int/en/web/kyiv/report-on-maidan-investigations.

[7] Durojaye, H., & Raji, O. (2022). Impact of state and state sponsored actors on the cyber environment and the future of critical infrastructure. *arXiv*. Retrieved from https://arxiv.org/abs/2212.08036.

[8] European Parliament. (2022). *Russia's war against Ukraine: A chronology of cyberattacks*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS BRI(2022)733549 XL.pdf.

[9] Fedyuk, V. (2025). Critically important infrastructure objects (part 2, article 259 of the criminal code of Ukraine) as a circumstances aggressing criminal liability. *Propylaea of Law and Security*, 6-7, 103-105.

[10] Gerasimenko, O.M. (2024). Critical infrastructure of Ukraine as a subject of scientific knowledge: Theoretical aspect. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 4(85), 42-49. doi: 10.24144/2307-3322.2024.85.4.6.
[11] Gorbatenko, V.P., & Kukuruz, O.V. (2021). Construction of political and legal reality: Theory, methodology, practice. *Lawful State*, (32), 475-481. doi: 10.33663/0869-2491-2021-32-475-481.
[12] Ilic, G. (2023). "International legal aspects of the critical infrastructure protection against contemporary security threats" – Vesna Poposka. *Contemporary Macedonian Defense/Sovremena Makedonska Odbrana*, 23(45).
[13] Kondratov, S.I., & Sukhodolia, O.M. (2020). *The state critical infrastructure protection system in the national security system: The analytical report*. Kyiv: NISS.
[14] Kostakopoulou, D. (2024). Constructivist approaches and institutional constructivism in EU legal scholarship. In *Interdisciplinary research methods in EU law* (pp. 265-278). London: Edward Elgar Publishing.
[15] Kratochwil, F., & Peltonen, H. (2022). Constructivism. In *Oxford research encyclopedias: Politics*. Oxford: Oxford University Press.
[16] Kucherina, S.E., & Oleinikov, D.O. (2021). Current status of criminal law protection of critical infrastructure facilities. *Information and Law*, 1(36), 90-98. doi: 10.37750/2616-6798.2021.1(36).238187.
[17] Larrinaga, C., & Bebbington, J. (2021). The pre-history of sustainability reporting: A constructivist reading. *Accounting, Auditing & Accountability Journal*, 34(9), 162-181. doi: 10.1108/AAAJ-03-2017-2872.
[18] Locatelli, A. (2021). Critical infrastructure protection. In *Technology and international relations* (pp. 152-172). London: Edward Elgar Publishing. doi: 10.4337/9781788976077.00016.
[19] Matczak, A. (2024). Who is "the public" when we talk about crime?: Interpreting and framing public voices in criminology. In *Marginalised voices in criminology* (pp. 166-181). London: Routledge.
[20] McCourt, D.M. (2022). *The new constructivism in international relations theory*. Bristol: Policy Press.
[21] Meli, K., Koliopoulos, D., & Lavidas, K. (2022). A model-based constructivist approach for bridging qualitative and quantitative aspects in teaching and learning the first law of thermodynamics. *Science & Education*, 31(2), 451-485. doi: 10.1007/s11191-021-00262-7.
[22] Minakov, M. (2023). War, de-oligarchization, and the possibility of anti-patronal transformation in Ukraine. In B. Madlovics & B. Magyar (Eds.), *Ukraine's patronal democracy and the russian invasion* (pp. 141-165). Budapest: Central European University Press. doi: 10.1515/9789633866641-007e.
[23] Nugroho, B.W. (2024). Constructivist approach to the exchange of power in search of the possibility of the Russo-Ukraine conflict settlement. *International Journal of Social Science, Education, Communication and Economics (SINOMICS JOURNAL)*, 3(2), 245-260.
[24] Ocieczek, G. (2024). Selected legal aspects of national security and critical infrastructure protection in the European Union with particular reference to the Polish national legislation. In *Shielding Europe with the common security and defence policy: The EU legal framework for the development of an innovative European defence industry in times of a changing global security environment* (pp. 803-839). Budapest: Central European Academic Publishing.
[25] Office of the UN High Commissioner for Human Rights. (2024). *Attacks on Ukraine's energy infrastructure: Harm to the civilian population*. Retrieved from https://ukraine.ohchr.org/sites/default/files/2024-09/ENGAttacksonUkraine'sEnergyInfrastructure-Harm to the Civilian Population.pdf.
[26] OSCE. (2004). *Ukrainian presidential elections October 31, November 21 and December 26, 2004*. Retrieved from https://www.cvk.gov.ua/wp-content/uploads/2020/05/2004 osce pu.pdf
[27] Pardede, J.N., & Poluakan, P.H. (2021). Law and post-truth: Critical constructivism as an ideal legal reasoning method on Indonesia's post-truth era society. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, 4(1).
[28] Park, S. (2023). Constructivism. In *International organization and global governance* (pp. 133-143). London: Routledge.
[29] Roman, Ł., & Cygańczuk, K. (2022). Legal dimension of the protection of critical infrastructure – selected aspects. *Safety & Fire Technology*, 59(1), 166-181. doi: 10.12845/sft.59.1.2022.10.
[30] Sallinen, M. (2021). *Weaponized malware, physical damage, zero casualties–what informal norms are emerging in targeted state-sponsored cyber-attacks?: The dynamics beyond causation: An interpretivist-constructivist analysis of the US media discourse regarding offensive cyber operations and cyber weapons between 2010 and 2020*. (Master's thesis, Swedish Defence University, Stocholm, Sweden).
[31] Snelbecker, D. (1995). The political economy of privatization in Ukraine. *CASE Network Studies and Analyses*, 59. doi: 10.2139/ssrn.1476267.

[32] Sokurenko, V.V. (2023). Current state and prospects for the development of Ukrainian criminology. *Bulletin of the National Academy of Legal Sciences of Ukraine*, 30(3), 336-356. doi: 10.31359/1993-0909-2023-30-3-336.

[33] Ternavska, A.A., & Turlova, Y.A. (2024). Criminality in the field of radioecological safety as an object of criminological research. *Bulletin of the National Academy of Legal Sciences of Ukraine*, 31(2), 283-302. doi: 10.31359/1993-0909-2024-31-2-283.

[34] Tychyna, D.M. (2025). Peculiarities of criminal liability of officials of legal entities of private law for corruption crimes in the sphere of official activity. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 3(89), 281-287. doi: 10.24144/2307-3322.2025.89.3.42.

[35] Vozniuk, A., Kamensky, D., Dudorov, O., Movchan, R., & Andrushko, A. (2021). Unconstitutionality of criminal liability for filing inaccurate information in Ukraine: Critical legal analyses. *Cuestionas Politicas*, 39(69), 133-145. doi: 10.46398/cuestpol.3969.07.

[36] Wijesinghe, H., Suduwelikanda, D., & Karunasena, V. (2024). Ukraine-Russia war and the neighborhood: Understanding Russia-Eastern Europe relations through constructivist perspective. *Spectrum: Journal of Global Studies*. Retrieved from https://ss.kln.ac.lk/depts/intlSt/media/attachments/2024/03/21/journal-of-global-studies-2024---march-final.pdf#page=27.

[37] Yigit, Y., Ferrag, M.A., Sarker, I.H., Maglaras, L.A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical infrastructure protection: Generative AI, challenges, and opportunities. *arXiv*. Retrieved from https://arxiv.org/abs/2405.04874.

# Конструктивістська рамка аналізу кримінальної відповідальності службових осіб за зловживання на енергетичному ринку як загрози критичній інфраструктурі України

**Марія Шаталінська**
Аспірант
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0000-9077-1025
**Олена Тихонова**
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-3848-3023

■ **Анотація.** Метою дослідження було визначити, наскільки чинна модель кримінальної відповідальності службових осіб на енергетичному ринку є ефективною та релевантною сучасним безпековим викликам у сфері критичної інфраструктури. Методологія дослідження поєднувала історико-правовий, системно-структурний та дискурс-аналіз нормативно-правових актів України, а також аналітичних звітів. За результатами дослідження встановлено, що чинна система кримінально-правового захисту є наслідком історичної інерції та успадкувала недоліки радянської моделі, орієнтованої на ідеологічні, а не техногенні загрози. Виявлено, що загальні статті кримінального законодавства про службові злочини якісно не здатні відобразити специфіку й масштаби потенційної шкоди, оскільки вони орієнтовані на індивідуальні наслідки, а не загрозу системного колапсу, від атак на життєво важливі системи. Доведено, що процеси приватизації у 1990-х роках створили прогалину у визначенні суб'єктів відповідальності серед керівників приватних операторів енергетичного ринку. Констатовано суттєвий розрив між застарілими правовими нормами та сучасними суспільними очікуваннями щодо безпеки, що сформувалися під впливом повномасштабної війни. Висновки полягали в тому, що наявна система кримінальної відповідальності є неефективною та потребує негайного реформування. Обґрунтовано нагальну необхідність розроблення та імплементації до Кримінального кодексу України спеціалізованих складів злочинів із санкціями, пропорційними рівню суспільної небезпеки таких діянь, що має підвищити стійкість держави та забезпечити невідворотність покарання. Практична значущість дослідження полягає в тому, що його результати можуть використати законотворчі органи для розроблення дієвих правових механізмів захисту енергетичного ринку як суб'єкта впливу на критичну інфраструктуру України

■ **Ключові слова:** національна безпека; правове регулювання; законодавчі прогалини; стратегічні об'єкти; процеси приватизації; енергетична інфраструктура; енергетичний ринок