**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ**
**«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»**

# ТЕЗИ ДОПОВІДЕЙ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

# ДО ДНЯ НАУКИ В УКРАЇНІ
**та**
# СТВОРЕННЯ ГУМАНІТАРНО-ПРАВОВОГО ФАКУЛЬТЕТУ ЗА УЧАСТІ ІНОЗЕМНИХ ПАРТНЕРІВ

# «ПРАВОВІ ЗАСАДИ СТІЙКОСТІ ТА СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВ АВІАЦІЙНОЇ ГАЛУЗІ ТА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

# ABSTRACTS OF THE REPORTS OF THE ALL-UKRAINIAN SCIENTIFIC AND PRACTICAL CONFERENCE FOR THE DAY OF SCIENCE IN UKRAINE
**and**
# CREATION OF THE HUMANITARIAN AND LAW FACULTY WITH THE PARTICIPATION OF FOREIGN PARTNERS "LEGAL PRINCIPLES OF SUSTAINABILITY AND SUSTAINABLE DEVELOPMENT OF AVIATION INDUSTRY ENTERPRISES AND CRITICAL INFRASTRUCTURE FACILITIES"

**30 квітня 2026 р.**

**ХАРКІВ 2026**

УДК340(477):629.73:338.49(063) DOI: https://doi.org/10.32620/conf.2026.law

Затверджено рішенням засідання кафедри права гуманітарно-правового факультету Національного аерокосмічного університету «Харківський авіаційний інститут» (протокол № 15 від 13 травня 2026 р.)

Затверджено Вченою радою гуманітарно-правового факультету Національного аерокосмічного університету «Харківський авіаційний інститут» (протокол № 11 від 27.05.2026 р.)

**Правові засади стійкості та сталого розвитку підприємств авіаційної галузі та об'єктів критичної інфраструктури** [Електронний ресурс] : тези доповідей Всеукраїнської науково-практичної конференції, 30 квітня 2026 року, Харків / Міністерство освіти і науки України, Національний аерокосмічний університет «Харківський авіаційний інститут». - Харків : ХАІ, 2026. – 144 с.

До збірника увійшли тези доповідей учасників Всеукраїнської науково-практичної конференції до дня науки в Україні та створення гуманітарно-правового факультету за участі іноземних партнерів «Правові засади стійкості та сталого розвитку підприємств авіаційної галузі та об'єктів критичної інфраструктури» Національного аерокосмічного університету «Харківський авіаційний інститут».

Розраховано на наукових працівників, викладачів, здобувачів вищої освіти.

Адреса редакційної колегії: 61070,
м. Харків, вул. Манька, 17
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Тези поширюються в електронному вигляді.

Редакційна колегія наголошує, що висновки окремих авторів є дискусійними. Разом із тим, їх публікація здійснюється з метою забезпечення плюралізму наукової думки і публічного обговорення. Матеріали друкуються мовою оригіналу.
За достовірність наукового матеріалу, професійне формулювання, фактичні дані, цитати, власні імена, географічні назви, а також за розголошення фактів, що не підлягають відкритому друку, відповідають автори публікацій та їхні наукові керівники (за наявності).

©Національний аерокосмічний університет
«ХАІ», 2026

**ЗМІСТ**

# ВІТАЛЬНЕ СЛОВО

***Олексій ЛИТВИНОВ***
*доктор юридичних наук, професор,*
*заслужений працівник освіти України,*
*ректор Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*

**ШАНОВНІ КОЛЕГИ!**

Від імені колективу Національного аерокосмічного університету «Харківський авіаційний інститут» маю честь привітати учасників науково-практичної конференції «Правові засади стійкості та сталого розвитку підприємств авіаційної галузі та об'єктів критичної інфраструктури».

У нинішніх умовах воєнного стану питання захисту критичної інфраструктури – від енергетичних і телекомунікаційних об'єктів до логістичних вузлів – набуває стратегічного значення для національної безпеки та життєздатності держави. Особливої уваги потребує авіаційна галузь, яка є високотехнологічним сектором і водночас однією з найбільш вразливих цілей. Це вимагає розробки нових правових інструментів регулювання ризиків та забезпечення безперебійної діяльності підприємств.

На жаль, наш університет безпосередньо відчуває наслідки збройної агресії: систематичні удари спричинили значні руйнування навчально-виробничої бази. Найбільш болісним наслідком стала втрата науковців і викладачів, які становили інтелектуальний потенціал аерокосмічної спільноти. Попри ці випробування, ХАІ продовжує виконувати свою наукову місію, адаптуючи освітній і дослідницький процеси до вимог безпеки. Символічно, що сьогоднішній захід відбувається у захищеному університетському просторі «Open Sky», який став центром консолідації наукової думки. Поряд із ним активно функціонують інші безпечні локації: лабораторія «Smart Systems & Control», зали авіаційних тренажерів, класи 3D-друку та віртуальної реальності, де тривають розробки у сферах інтелектуального управління та сучасного літакобудування.

Конференція покликана стати дієвим майданчиком для об'єднання інтелектуальних ресурсів провідних науковців, інженерів-конструкторів та фахівців у сфері безпеки з метою розробки комплексних правових механізмів протидії сучасним гібридним загрозам. Особливого значення набуває залучення міжнародного досвіду, зокрема у співпраці з європейськими інституціями та експертами рівня бізнес-школи HEC Paris, що дозволить інтегрувати передові стратегії цифрової безпеки у вітчизняну нормативну базу. Переконаний, що результати ваших обговорень і напрацьовані рекомендації стануть надійним підґрунтям для зміцнення національної безпеки, адаптації міжнародних стандартів захисту критичної інфраструктури до викликів воєнного часу та формування стратегії поствоєнного відновлення авіаційної галузі. Спільна робота над удосконаленням законодавства у сфері кіберзахисту та фізичної стійкості об'єктів життєзабезпечення є нашим внеском у побудову сильної та технологічно розвиненої держави.

Бажаю всім учасникам конструктивної роботи, змістовних дискусій та результатів, що матимуть практичне значення для сталого розвитку й перемоги України.

**СЛАВА УКРАЇНІ!**

# ВІТАЛЬНЕ СЛОВО

***Світлана ДОМБРОВСЬКА***,
*докторка наук з державного управління, професорка,*
*заслужений працівник освіти України,*
*проректорка з наукової роботи Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*

**ШАНОВНІ КОЛЕГИ**!

Дозвольте привітати вас із початком роботи нашого наукового форуму.

Право є міцним каркасом будь-якої галузі, основою її розвитку та гарантією стійкості. У Національному аерокосмічному університеті «Харківський авіаційний інститут» юридична наука органічно поєднується з технічними та інженерними дисциплінами, створюючи унікальний простір для міждисциплінарного розвитку. Тут правова думка не існує ізольовано – вона інтегрується у високотехнологічне середовище, спрямовує його поступ і забезпечує нормативні орієнтири для авіаційної та космічної галузей.

Поєднання практичного досвіду, інноваційних технологій та правової науки формує фундамент, що дозволяє нашим підприємствам не лише вистояти у складні часи, а й розвиватися. Адже саме правова наука має випереджати час, передбачати виклики та пропонувати інструменти їх подолання.

Сьогодні ми стикаємося з серйозними викликами національній безпеці та суспільним труднощам. Вони загартовують нас, формують нову культуру стійкості та створюють умови для того, щоб наукові напрацювання були готовими до майбутніх викликів. Це знання ми передаємо молодому поколінню, щоб воно могло засвоїти досвід і продовжити розвиток нашої держави.

Особливо хочу наголосити, що навіть у цей непростий період науковці ХАІ не припинили своєї діяльності. Вони працюють, залучають студентів, адже саме студентське середовище є джерелом нової науки. Без молодої науки неможливий подальший поступ.

Щиро дякую вам за вашу працю, за прагнення до розвитку та за залучення провідних учених до нашої конференції. Бажаю невпинного руху вперед, нових відкриттів і зміцнення нашої наукової спільноти задля сталого майбутнього та перемоги України..

**СЛАВА УКРАЇНІ!**

## ВІТАЛЬНЕ СЛОВО

***Яннік ФУРАСТЬЄ (Yannick FOURASTIER)***,
*PhD, запрошений експерт Executive Education бізнес-школи HEC Paris, керівник європейських проєктів з цифрової безпеки та стандартизації (CodEUrope), Париж, Французька Республіка*

**ШАНОВНІ ДРУЗІ, ВІТАЮ**!

Дозвольте коротко представити себе. В Україні я очолюю компанію Europe, яка працює у сфері технологій, зосереджуючись на розвитку природних та інфраструктурних рішень.

У 2019 році ми розпочали діяльність в Україні й невдовзі долучилися до президентської програми з реконструкції національної авіації. Для мене це було природним кроком, адже ще два десятиліття до того я мав досвід керівництва масштабними проєктами у компанії Airbus.

У цьому контексті я також працював над модернізацією системи управління повітряним рухом у європейському небі в межах програми CESAR, а також виконував функції директора програм із будівництва аеропортів, приділяючи особливу увагу їх «зеленому» та сталому розвитку.

Сьогодні, в умовах воєнного часу, ми усвідомлюємо, що відродження української авіації є не лише економічним чи технологічним завданням, а й важливим чинником національної стійкості та безпеки. Франція прагне бути поруч із Україною у цьому процесі, надаючи підтримку та досвід у сфері сталого розвитку, модернізації інфраструктури та впровадження передових технологій.

Особливе значення має співпраця з українськими науковцями, зокрема з Національним аерокосмічним університетом «Харківський авіаційний інститут» (ХАІ). Саме наукова спільнота ХАІ є рушійною силою у формуванні сучасних підходів до розвитку авіаційної галузі, поєднуючи фундаментальні дослідження з практичними рішеннями для відновлення та модернізації авіаційної інфраструктури. Спільні проєкти та дослідницькі ініціативи між французькими та українськими фахівцями створюють унікальні можливості для інтеграції передових європейських практик у національну систему авіаційної безпеки та управління.

Спільна праця українських і французьких учених та інженерів є запорукою того, що авіаційна галузь України зможе відновитися, зміцнитися та інтегруватися у європейський та світовий простір, відповідаючи найвищим стандартам сучасності. Це партнерство має стратегічне значення: воно не лише сприяє технологічному розвитку, але й утверджує солідарність Франції з Україною у цей складний воєнний час, коли міжнародна підтримка є критично важливою для збереження та відновлення національної авіаційної системи.

**ДЯКУЮ ЗА УВАГУ!**
**СЛАВА УКРАЇНІ!**

# ВІТАЛЬНЕ СЛОВО

***Яніс ГРАСІС (Jānis GRASIS),***
*PhD in Law, професор, професор Соціального факультету Ризького університету імені Страдіня, Рига, Латвійська Республіка*

**ДОРОГІ КОЛЕГИ, ШАНОВНІ УКРАЇНСЬКИ ДРУЗІ**!

Маю честь привітати учасників міжнародної науково-практичної конференції, організованої Національним аерокосмічним університетом «Харківський авіаційний інститут». Обрана тематика є надзвичайно актуальною не лише для України та Латвії, але й для Європейського Союзу та всього демократичного світу.

Дозвольте коротко зупинитися на питаннях безпеки в авіаційній галузі. Латвія у 2022 році посіла друге місце серед країн ЄС після Польщі за кількістю кібератак: 16% усіх російських атак було спрямовано саме проти нашої держави. Це свідчить про те, що готовність до кіберзахисту нині є критично важливою умовою належного функціонування внутрішнього ринку авіації та забезпечення стійкості інфраструктури. Розвиток інформаційних і комунікаційних технологій у Латвії та за її межами відбувається безпрецедентними темпами. У 2024 році Сейм ухвалив новий закон про національну кібербезпеку, який набув чинності 1 вересня 2024 року. Він суттєво оновив та розширив положення застарілого закону 2010 року, усунувши його недоліки та запровадивши суворі вимоги безпеки для державних органів, муніципалітетів, компаній та власників критичної інфраструктури. Закон також імплементує європейські стандарти щодо високого рівня безпеки мереж та інформаційних систем, передбачає створення Національного центру кібербезпеки та розширює коло суб'єктів, на яких поширюється його дія – загалом близько 2000 організацій.

Важливо наголосити, що нове законодавство передбачає значні санкції за недотримання вимог – до 10 млн євро. Це стосується ключових секторів суспільного інтересу: енергетики, транспорту, фінансової інфраструктури, охорони здоров'я та інших сфер. Відповідальність постачальників таких послуг полягає не лише у дотриманні стандартів кіберзахисту, але й у своєчасному інформуванні про інциденти. Адже масштабність, складність та частота кіберзагроз становлять реальну небезпеку для функціонування авіаційної галузі, можуть спричиняти фінансові втрати, підривати довіру громадян та завдавати значної шкоди економіці й суспільству Європейського Союзу. У цьому контексті міжнародна співпраця, зокрема між Латвією та Україною, а також активна участь наукової спільноти ХАІ, набуває особливого значення. Саме об'єднання зусиль науковців, інженерів та правників дозволяє формувати комплексні рішення, які зміцнюють авіаційну безпеку, забезпечують стійкість критичної інфраструктури та сприяють інтеграції України й Латвії у європейський простір безпеки.

Бажаю плідної дискусії та переконаний, що результати цієї конференції стануть вагомим внеском у розвиток міжнародних стандартів кіберзахисту та стійкості авіаційної галузі.

**СЛАВА УКРАЇНІ**!

https://doi.org/10.5281/zenodo.20496534

***Juļa LIDIJA,***
*Ph.D., Assistant Professor, Riga Stradins University,*
*Riga, Latvia,*
*e-mail: lidija.jula@rsu.lv,*
*ORCID: https://orcid.org/0000-0001-5139-4642*

***Selickis SILVESTRS, Bac.iur.***
*Graduate of Riga Stradins University,*
*Faculty of Social Sciences, Study Programme in Law,*
*Latvia. Bremen, Germany,*
*e-mail: selickis24@gmail.com*

***Putans ROMANS,***
*Dr.sc.admin., Associate Professor,*
*Riga Stradins University, Riga, Latvia,*
*e-mail: romans.putans@rsu.lv,*
*ORCID: https://orcid.org/0000-0003-0668-5728*

## АЛГОРИТМІЧНА ПЕРСОНАЛІЗАЦІЯ ЦІН ЯК ВИКЛИК ЦИФРОВІЙ БЕЗПЕЦІ, СПРАВЕДЛИВОСТІ ТА ЗАХИСТУ СПОЖИВАЧІВ В АВІАЦІЙНІЙ ГАЛУЗІ

У статті досліджується алгоритмічна персоналізація цін як виклик цифровій безпеці, справедливості та захисту споживачів в авіаційній галузі. Основна теза полягає в тому, що персоналізація цін у цифрових авіаційних послугах є не лише проблемою прав споживачів, а й проблемою цифрової стійкості та довіри в контексті критичної інфраструктури. Аналіз розмежовує динамічне ціноутворення та індивідуалізоване ціноутворення на основі профілювання, поведінкових даних і автоматизованого прийняття рішень, обґрунтовуючи потребу в сильніших гарантіях прозорості, відмови та справедливого управління даними.

**Ключові слова**: алгоритмічне ціноутворення; авіація; захист споживачів; цифрова безпека; справедливість; персональні дані; прозорість.

## ALGORITHMIC PRICE PERSONALIZATION AS A DIGITAL SECURITY, FAIRNESS AND CONSUMER PROTECTION CHALLENGE IN THE AVIATION SECTOR

The paper examines algorithmic price personalization as a digital security, fairness and consumer protection challenge in the aviation sector. Its central argument is that algorithmic price personalization in aviation digital services is not only a consumer rights issue, but also a problem of digital resilience and trust in the context of critical infrastructure. The analysis distinguishes traditional dynamic pricing from individualized pricing based on consumer profiling, behavioural data, location, device type and automated decision-making. It argues that formal transparency is necessary but insufficient on its own, and that stronger disclosure, opt-out mechanisms and fairness-oriented data governance are required.

**Keywords**: algorithmic pricing; aviation; consumer protection; digital security; fairness; personal data; transparency.

**Introduction**

The aviation sector has long relied on price flexibility, especially in the sale of air tickets, where prices may change according to demand, seasonality, remaining seat capacity, route popularity and the timing of purchase. Such dynamic pricing is not new and is usually justified by objective market conditions. However, the development of digital platforms, big data analytics and artificial intelligence creates a qualitatively different situation: prices may be adjusted not only on the basis of general market factors, but also on the basis of the digital profile of a specific consumer, including browsing history, location, device type, loyalty status or other behavioural data.

This distinction is central to the legal and policy analysis of algorithmic pricing in aviation. Dynamic pricing refers to price changes caused by market conditions applicable to consumers as a group. Algorithmic price personalization, by contrast, refers to individualized pricing based on data about a particular consumer and predictions of that consumer's willingness to pay. When the price of an aviation service becomes the outcome of consumer profiling rather than a transparent market signal, new risks arise for fairness, consumer autonomy and digital trust [10, p. 36-47].

The central argument of this paper is that algorithmic price personalization in aviation digital services is not only a consumer rights issue, but also a problem of digital resilience and trust in the context of critical infrastructure. In this context, aviation should not be treated as an ordinary e-commerce sector. It is closely connected to mobility, employment, family life, emergency travel and the functioning of critical infrastructure. For this reason, opaque and individualized pricing practices in aviation-related digital services may weaken not only consumer protection but also public confidence in data-driven infrastructure.

The aim of this paper is to analyse the digital security, fairness and consumer protection risks created by algorithmic price personalization in the aviation sector and to assess whether the current European Union transparency-based regulatory model is sufficient to address these risks. The research applies doctrinal legal analysis, grammatical, systemic and teleological interpretation of legal norms, and draws on empirical findings from a consumer survey concerning awareness, fairness perceptions and acceptance of personalized pricing.

**Algorithmic price personalization in aviation digital services**

Algorithmic price personalization may be defined as an automated pricing practice in which an identical or comparable service is offered at an individually adjusted price on the basis of consumer-specific data. In aviation, this may concern not only air tickets, but also baggage fees, seat selection, priority boarding, travel packages, insurance products, loyalty programme offers and services sold through intermediary booking platforms. The decisive feature is not the use of an algorithm as such, but the use of consumer profiling to differentiate prices offered to a specific consumer.

The aviation sector is particularly exposed to such practices because it operates through highly digitalised sales channels. Consumers search for routes, compare prices, log into loyalty accounts, use mobile applications and interact with booking platforms that can collect and process behavioural data in real time. Such data may reveal urgency, flexibility, purchasing power, travel habits or vulnerability. If these signals are used to adjust prices at the individual level, the consumer may be offered a price that reflects not only market demand but also the platform's assessment of the maximum price the consumer is willing to pay.

From a law-and-economics perspective, individualized price personalization may increase business efficiency and revenue optimization [3, p. 3270-3271]. Nevertheless, it also changes the function of price in the market [9, p. 410-411]. Price no longer operates as a comparable and externally observable signal, because different consumers may receive different prices for

comparable services on the basis of non-transparent criteria. This creates an informational imbalance: the trader knows more about the consumer than the consumer knows about the pricing process [1, p. 442-492; 13, p. 399-419; 2, p. 405-406].

**Consumer fairness, autonomy and trust**

The fairness dimension is particularly important in the aviation sector. Consumers may accept that an air ticket becomes more expensive when demand increases or departure approaches. They are less likely to accept that the price is higher because an algorithm has inferred urgency, income level, device type, location or repeated searching behaviour. In such cases, the issue is not merely whether the consumer was formally informed, but whether the consumer is treated fairly and can meaningfully understand the basis of the price offered [8, Arts. 20-21].

Empirical findings from the authors' broader study confirm that consumer attitudes toward algorithmic price personalization are predominantly critical. The empirical component of the study is based on an online consumer survey conducted between November 2025 and March 2026, including 174 respondents, using structured multiple-choice and Likert-scale questions to assess consumer awareness, perceived fairness, and acceptance of personalized pricing. The sample provides a confidence level of 95% with an estimated margin of error of approximately ±8.3 %, and the relationships between key variables were examined using non-parametric statistical methods, including Spearman's rank correlation analysis. Survey results showed that only 16 % stated that they clearly knew what algorithmic price personalization means, while 86 % had noticed different prices for the same product online. More than 80 % evaluated personalized pricing as unfair, and a majority associated such practices with a risk of discrimination [11]. These findings suggest that the legitimacy problem cannot be solved through formal disclosure alone.

Consumer acceptance is conditional. Respondents were more willing to accept personalization where they were clearly informed about it, where the personalization notice appeared next to the final price, where criteria could be viewed, and where an opt-out was available. However, even under such conditions, a significant share of respondents remained hesitant or opposed. This confirms that transparency is a necessary but insufficient regulatory tool: it may improve procedural legitimacy, but it does not by itself resolve substantive concerns about unfairness, unequal treatment or potential exploitation.

**Legal framework and regulatory gaps**

European Union law already recognises the possibility of personalized prices in digital markets. Article 6(1)(ea) of Directive 2011/83/EU requires traders to inform consumers where the price has been personalized on the basis of automated decision-making particularly in the context of distance contracts [6, Art. 6(1)(ea)]. This provision is an important starting point, but its protective capacity is limited [12, p. 16-17]. It primarily requires disclosure of the fact of personalization and does not necessarily require a meaningful explanation of the data categories, criteria or underlying logic that affected the final price.

The Unfair Commercial Practices Directive is also relevant because opaque pricing practices may materially distort the economic behaviour of the average consumer, especially where the consumer cannot understand why a price differs from the price offered to others [5, 639-640]. In aviation-related services, such opacity may be particularly problematic because consumers often face time pressure, limited route alternatives and complex price components. If a personalized price is presented as a neutral market price, the consumer may be unable to make a genuinely informed economic decision.

Data protection law provides a further layer of protection. Personalized pricing may rely on IP address, location, device data, search history, purchase history or loyalty programme data. Under the General Data Protection Regulation, personal data must be processed lawfully, fairly and

transparently. Articles 13, 14 and 15 establish information rights, while Article 22 may become relevant where automated decision-making, including profiling, produces legal or similarly significant effects on a person (the data subject), although its applicability to personalized pricing remains context-dependent [7, Art.22]. The Court of Justice of the European Union has also confirmed that even dynamic IP addresses may qualify as personal data where identification is reasonably possible [4].

Despite these legal instruments, the regulatory framework remains fragmented [12, p. 16-17; 2, p. 405-406]. Consumer law focuses mainly on information duties, data protection law focuses on lawful and transparent processing, and non-discrimination law addresses unequal treatment only under specific conditions. Algorithmic price personalization, however, combines all these dimensions. It may be formally disclosed, technically lawful but still perceived as unfair or manipulative if the consumer lacks meaningful control over the pricing process or cannot effectively assess how the price was determined.

**Digital resilience and critical infrastructure context**

Aviation is part of the broader critical infrastructure ecosystem. Its digital services depend on secure, reliable and trustworthy data processing systems. Pricing algorithms are usually discussed as commercial tools, but in aviation-related digital markets they also affect trust in infrastructure. If consumers suspect that booking platforms, airlines or ancillary service providers use opaque profiling to exploit urgency or vulnerability, trust in digital aviation services may decline.

The digital resilience perspective requires attention to more than cybersecurity in the narrow technical sense. It also includes the resilience of governance mechanisms, the reliability of data, the auditability of automated decisions and the ability of consumers and regulators to detect unfair outcomes. Incorrect, outdated or biased data may result in unjustified price differentiation. Insufficient algorithmic oversight may allow discriminatory or manipulative pricing models to remain unnoticed. In this respect, algorithmic price personalization becomes a governance-related risk for data-intensive aviation services.

Accordingly, aviation-related digital markets should be subject to higher transparency and accountability expectations than ordinary online retail. Consumers should be able to know whether a price is personalized, what categories of data were used, whether loyalty status, location, device type or previous search behaviour affected the price, and whether a non-personalized option is available. Such safeguards are especially important where aviation services are necessary for work, family obligations, urgent mobility or access to essential services.

**Recommendations**

Several regulatory and governance improvements follow from the analysis. First, disclosure obligations should be expanded from a simple notice that a price is personalized to a meaningful and accessible explanation of the categories of data and criteria used. The explanation need not reveal trade secrets or source code, but it should allow the consumer to understand the basis of personalization in practical terms.

Second, consumers should be given a real possibility to opt out of price personalization without losing access to the service. An opt-out mechanism that merely redirects the consumer to a less functional service or removes access to ordinary booking options would not constitute a meaningful effective choice. Third, supervisory authorities should develop guidance on algorithmic pricing in aviation and other data-intensive services, clarifying how consumer law and data protection law apply in practice.

Fourth, specific personalization criteria should be subject to stricter scrutiny. Pricing based on socio-economic indicators, location-based vulnerability, inferred behavioural characteristics, sensitive-data proxies or repeated search behaviour may raise particular concerns. Fifth, aviation

service providers and booking platforms should conduct internal fairness and data governance assessments for pricing algorithms, especially where automated systems affect access to essential mobility services.

**Conclusions**

Algorithmic price personalization in the aviation sector creates a complex challenge at the intersection of digital security, consumer protection, data protection and fairness. Dynamic pricing based on objective market factors may be economically justified and broadly acceptable. Individualized pricing based on consumer profiling requires stronger legal and governance safeguards because it may undermine transparency, equality of treatment and consumer trust.

The current EU regulatory model provides an initial transparency framework, but it remains insufficient where consumers cannot understand or verify how personalized prices are formed. Formal information about personalization does not necessarily ensure meaningful transparency, substantive fairness or real consumer autonomy. The empirical findings confirm that consumers perceive algorithmic price personalization critically and that acceptance depends on clear disclosure, opt-out possibilities and robust fairness safeguards.

Therefore, effective consumer protection in aviation digital services requires a shift from minimal disclosure to a more comprehensive governance-oriented model. Algorithmic price personalization should be transparent, controllable, proportionate and auditable. Only such an approach can preserve the balance between digital innovation in aviation, legitimate business interests and consumers' rights to a fair, secure and trustworthy digital environment. In the context of critical infrastructure, this is not only a matter of individual consumer protection, but also a matter of digital resilience and public trust.

## References


1. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442-492. https://doi.org/10.1257/jel.54.2.442

2. Borgesius, F. Z. (2020). Price discrimination, algorithmic decision-making, and European non-discrimination law. *European Business Law Review, 31*(3), 401-422. https://doi.org/10.54648/EULR2020017

3. Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review, 110*(10), 3267-3297. https://doi.org/10.1257/aer.20190623

4. Court of Justice of the European Union (2016). Judgment of 19 October 2016 in Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland. ECLI:EU:C:2016:779. [Accessed 28.04.2026]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582

5. Duivenvoorde, B. (2023). Consumer protection in the age of personalized marketing: Is EU law future-proof? *European Papers, 8*(2), 631-646. https://doi.org/10.15166/2499-8249/679

6. European Parliament and Council (2011). Directive 2011/83/EU on consumer rights. [Accessed 28.04.2026]. Available at: https://eur-lex.europa.eu/eli/dir/2011/83/oj

7. European Parliament and Council (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. [Accessed 28.04.2026]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

8. European Union (2016). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union, C 202,* 389-405. [Accessed 28.04.2026]. Available at: https://eur-lex.europa.eu/eli/treaty/char_2016/oj

9. Gautier, A., Ittoo, A., & Van Cleynenbreugel, P. (2020). AI algorithms, price discrimination and collusion: a technological, economic and legal perspective. *European Journal of Law and Economics, 50*(3), 405-435. https://doi.org/10.1007/s10657-020-09662-6

10. Grochowski, M., Jabłonowska, A., Lagioia, F., & Sartor, G. (2022). Algorithmic price discrimination and consumer protection: A digital arms race? *Technology and Regulation*, 2022, 36-47. https://doi.org/10.71265/kd9w2w17

11. Jula, L., Selickis, S., & Putans, R. (2026). Algorithmic Price Personalization in EU Digital Markets: Regulatory Design, Consumer Fairness and the Limits of Transparency. Manuscript submitted to *Journal Economics and Culture*.

12. Rott, P., Strycharz, J., & Alleweldt, F. (2022). Personalized pricing. European Parliament. [Accessed 28.04.2026]. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)734008

13. Varian, H. R. (2019). Artificial intelligence, economics, and industrial organization. In A. Agrawal, J. Gans, & A. Goldfarb (Eds.), The Economics of Artificial Intelligence: An agenda (pp. 399-419). Chicago: University of Chicago Press.

https://doi.org/10.5281/zenodo.20496634

***Vitālijs RAKSTIŅŠ***
*Lecturer, Faculty of Social Sciences,*
*Riga Stradins University, Riga, Republic of Latvia*
*e-mail: v.rakstins@gmail.com*

# SYSTEMATIC CHALLENGES IN ENHANCING CRITICAL INFRASTRUCTURE RESILIENCE

Over the past decade, the dominant logic of critical infrastructure protection has shifted from securing discrete physical assets to sustaining the functions that those assets enable. This research evaluates three institutional frameworks of this shift: the EU legislative framework anchored in the CER Directive (2022/2557) and the NIS2 Directive (2022/2555), NATO's seven baseline requirements for national civil preparedness adopted at the 2016 Warsaw Summit, and the total defense architectures of the Baltic and Nordic states, paying particular attention to Latvia's statutory framework for wartime service continuity. The core obstacle to effective resilience is the challenge of fragmented implementation, which is the persistent gap between formally complex legal obligations and the organizational depth, security culture, and interagency coordination required to make those obligations operationally meaningful, especially given that different international frameworks are substantially developed but fragmented.

**Keywords**: critical infrastructure, resilience, systematic challenges, CER Directive, NIS2 Directive, NATO, civil preparedness, total defense, Latvia, implementation.

## СИСТЕМНІ ВИКЛИКИ У ЗМІЦНЕННІ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Протягом останнього десятиліття домінуюча логіка захисту критичної інфраструктури змістилася від охорони окремих матеріальних об’єктів до забезпечення безперервності функцій, які ці об’єкти виконують. У цьому дослідженні оцінюються три інституційні рамки такого зсуву: законодавча база Європейського Союзу, закріплена в Директиві CER (2022/2557) та Директиві NIS2 (2022/2555); сім базових вимог НАТО щодо національної цивільної готовності, ухвалених на Варшавському саміті 2016 року; а також архітектури «тотальної оборони» країн Балтії та Північної Європи, з особливим акцентом на законодавчу базу Латвії щодо забезпечення безперервності функціонування у воєнний час. Ключовою перешкодою для ефективної стійкості є проблема фрагментованої імплементації – стійкий розрив між формально складними юридичними зобов’язаннями та необхідною організаційною глибиною, культурою безпеки й міжвідомчою координацією, які роблять ці зобов’язання операційно значущими. Це особливо актуально з огляду на те, що різні міжнародні рамки є суттєво розвиненими, але залишаються фрагментованими.

**Ключові слова**: критична інфраструктура, стійкість, системні виклики, директива CER, директива NIS2, НАТО, цивільна готовність, тотальна оборона, Латвія, імплементація.

## Introduction

Protection of critical infrastructure has not developed through steady accumulation but through periodic disruptions that forced practitioners and legislators to revise their core assumptions. The 2008 European Critical Infrastructure Directive (2008/114/EC) reflected an era in which the dominant concern was physical attack on specific installations. Organized around sectoral asset lists in energy and transport, and evaluated through physical security criteria, it still left inter-sectoral dependencies substantially unaddressed.

Three overlapping crises exposed that model's limitations. Russia's seizure of Crimea in 2014 demonstrated that energy supply disruptions and cyber operations, coordinated with conventional military pressure, could achieve political objectives without formal armed conflict. The COVID-19 pandemic then revealed that the more serious vulnerability was not any single sector but the cascade

effects between them: health systems, transport, energy, food supply, and communications proved mutually dependent in ways no sectoral continuity plan had modeled. Russia's full-scale invasion of Ukraine, which began in February 2022, confirmed the trajectory, as the deliberate targeting of power infrastructure, water systems, and communications networks became a sustained operational model (Balodis & Kepe, 2025). Each shift pointed to the same structural problem: the resilience of infrastructure as a physical object is secondary to the continuity of the functions it enables.

**The EU framework: CER and NIS2**

The CER Directive (2022/2557) establishes a framework covering hybrid threats, terrorism, sabotage, criminal infiltration, pandemics, and climate-related disruptions. Risk assessments conducted under the Directive must address cross-sectoral interdependencies (CER Directive, Art.5). Earlier directives did not require this. They treated each sector in isolation. This is a substantive departure from that siloed analysis. Designated critical entities bear obligations to implement resilience measures, develop and regularly test continuity plans, screen personnel in sensitive functions, and report significant disruptions to competent authorities within 24 hours.

The NIS2 Directive (2022/2555), adopted in parallel with CER, extends mandatory cybersecurity requirements across the same sectors. The NIS2 Directive (2022/2555), adopted in parallel with CER, extends mandatory cybersecurity requirements across the same sectors. The two instruments are explicitly cross-referenced and intended to function as a coordinated framework. NIS2 further requires essential entities to assess and manage cybersecurity risks in their supply chains — acknowledging that an operator's resilience is bounded by the weakest link among its suppliers.

**NATO's seven baseline requirements on resilience**

At the Warsaw Summit in July 2016, NATO's heads of state endorsed seven baseline requirements for national civil preparedness: continuity of government and critical government services; resilient energy supplies; capacity to manage uncontrolled population movement; resilient food and water resources; the ability to handle mass casualties; resilient civil communications systems; and resilient civil transportation systems (NATO, 2016). These requirements are framed as prerequisites for enablement of military operations. Contemporary military operations depend on civilian energy, transport, communications, and logistics networks that armed forces cannot independently replicate; degradation of those networks directly impairs NATO's operational capacity (CIMIC COE, 2025; NATO, 2024).

Subsequent summits extended the framework's scope. The 2021 Brussels Summit broadened the Resilience Commitment to cover supply chain diversification, infrastructure protection across domains including space and cyberspace, and resilience to the effects of emerging technologies. The 2022 Madrid Summit established common NATO resilience goals and transferred coordination responsibilities to a newly created Resilience Committee.

**Nordic Baltic approaches to total defence**

For the Nordic states, the post-2014 deterioration of the security environment did not prompt a new investment in national preparedness so much as accelerate one already underway. Sweden built its total defence structure in the 1950s and retained the institutional architecture through the Cold War's end, even as operational readiness declined. Finland is often mentioned as a reference model of total defence - nation never substantially dismantled its preparedness framework; it continues to operate under the concept of comprehensive security, a model that distributes responsibility across public authorities, businesses, municipalities, non-governmental organizations, and citizens within an integrated but functionally differentiated architecture (Finnish Comprehensive Security).

Latvia, Estonia, and Lithuania built their initial defence frameworks partly by drawing on Nordic models. Since Russia's aggression in 2014, all three have undertaken significant legal and organizational reforms to reintroduce total defense systems (Balodis & Kepe, 2025, DIIS 2025). Latvia's legislative framework is among the most explicitly function-centered in the EU. The National Security Law designates Category D as infrastructure whose destruction, operational degradation, or service discontinuation during a declared state of emergency or wartime would significantly endanger public and state security (National Security Law of Latvia, Art. 22.$^{2}$). This formulation goes beyond the CER Directive's requirements by establishing explicit legal obligations to sustain services under genuine wartime conditions, and by creating a mobilization exemption for workers whose continued

employment is necessary for essential service continuity. The practical implication is not intended to be just a plan on paper but rather a binding requirement to develop the capacity to keep essential functions running under degraded and hostile conditions.

**Analysis of challenges**

All three frameworks encounter the same fundamental constraint, a gap between binding requirements and what organizations can operationally deliver. Resource constraints are a contributing factor in some jurisdictions, but the more pervasive problem is structural. Responsibility for implementation is divided among various entities, including ministries, military planning chains, local governments, and private operators. Often, there are no cross-cutting coordination mechanisms or accountability frameworks in place to ensure that all responsible actors converge on a common operational outcome.

A second gap runs between civilian preparedness planning and military planning. NATO's baseline requirements explicitly address this by framing civil preparedness as a precondition for Alliance military effectiveness, but the institutional pathways for translating that strategic logic into coordinated planning at the national and subnational levels remain challenging in many member states. Civil emergency agencies and military planners often develop their respective continuity frameworks without sustained interaction, which means the civil infrastructure that military operations depend upon has not been stress-tested against the scenarios military planners are actually working with.

There's also a third problem that's even harder to deal with, and that's in the way resilience planning itself is set up. Scenario-based planning functions adequately for familiar, recurring disruptions. This planning method involves identifying likely or high-consequence threats, developing contingency plans against each, exercising those plans, and retaining the institutional knowledge to execute them. However, its inherent limitation surfaces when threats, not mentioned in the risks registers, appear. The Russian campaign against Ukrainian infrastructure demonstrated this with striking clarity: the combination of precision strikes, rolling blackouts, cyber operations, and information campaigns in adaptive sequences fell outside the scenario space of any civil continuity plan. Resilience engineering literature frames this as the problem of maintaining essential functions under conditions beyond the modeled scenario space. To address this, we need to have qualitatively different organizational capacities, such as personnel who can adapt when plans fail, backup systems that have been tested under realistic load, decision-makers who can make decisions without having all the information, and coordination protocols that can function when primary communications are unavailable.

**Conclusions**

The EU directives, NATO's baseline requirements, and the total defense frameworks of the Nordic and Baltic states collectively reflect a reorientation of critical infrastructure protection from securing physical objects to sustaining the functions those objects support. The legislative frameworks underpinning this shift carry enforceable obligations, which are designed to ensure that the goals of the initiative are met. Latvia's Category D infrastructure designation, which includes explicit wartime service continuity requirements and mobilization exemptions, illustrates how far that reorientation can be pressed into binding legal form.

The deficits are considered to be organizational rather than legal. The responsibility for implementation is spread across different institutions. These institutions often don't have the coordination mechanisms or shared planning culture needed to integrate their efforts to achieve a common operational outcome. Formal compliance diverges from functional preparedness in ways that existing accountability frameworks are poorly equipped to surface, and this discrepancy is something that must be addressed. Civilian and military planning continue to be organizationally isolated. To address these gaps, investment should be made in organizational practices rather than in further legislative elaboration. This means implementing exercises designed to test genuine operational dependencies rather than documented procedures, accountability mechanisms capable of distinguishing compliance from capability, structured civil-military planning integration at national and subnational levels, continuity training conducted under deliberately degraded conditions, and sustained public communication that embeds preparedness as a civic norm. The legislative

foundations are established, and the next step is to move forward with the implementation of the new policies.

## References


1. Balodis, M. & Kepe, M. (2025). Lessons from Latvia's Efforts to Keep Essential Services Running During a Crisis. Atlantic Council / RAND Corporation, May 2025. Available at: https://www.rand.org/pubs/commentary/2025/08/lessons-from-latvias-efforts-to-keep-essential-services.html

2. CIMIC Centre of Excellence (2025). CIMIC Handbook — Chapter 7: Resilience; 7.2 Seven Baseline Requirements. The Hague: CIMIC COE.

3. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, L 345/75.

4. DIIS — Danish Institute for International Studies (2025). Strengthening Civil Preparedness in the Baltic Sea Region. Copenhagen: DIIS.

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333/80.

6. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive). Official Journal of the European Union, L 333/164.

7. Finnish Comprehensive Security homepage https://turvallisuuskomitea.fi/en/comprehensive-security/ Latvia: National Security Law (Nacionālās drošības likums). Saeima of the Republic of Latvia.

8. NATO (2016). Warsaw Summit Communiqué. Brussels: NATO Public Diplomacy Division.

9. NATO (2024). Resilience, Civil Preparedness and Article 3. Brussels: NATO Public Diplomacy Division. Available at: https://www.nato.int/cps/en/natohq/topics_132722.htm

https://doi.org/10.5281/zenodo.20496663

***Світлана АНДРЕНКО,***
*помічниця ректора ректорату Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків, Україна*
*кандидатка юридичних наук*
*ORCID: https://orcid.org/0000-0002-2900-3120,*
*e-mail: sweta-a@ukr.net*

***Владислав ЄМЕЦЬ,***
*здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з права) Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://orcid.org/0009-0007-8195-9406,*
*e-mail: v.l.yemets@khai.edu*

## КОМПЛЕКСНА БЕЗПЕКА ЗАКЛАДІВ ВИЩОЇ ОСВІТИ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

У роботі акцентовано увагу на проблемах забезпечення безпеки закладів вищої освіти (ЗВО) України в умовах воєнного стану, коли університети, академії та інститути функціонують як об’єкти масового перебування людей і водночас стають потенційними цілями для обстрілів, диверсій та кібератак. Безпека ЗВО розглядається як багатокомпонентна система, що охоплює захист життя і здоров’я студентів та працівників, збереження майна, безпечну експлуатацію будівель і споруд, а також протидію сучасним викликам, включно з гібридними кіберзагрозами та ризиками для критичної інфраструктури. Підкреслено необхідність розробки комплексної програми безпеки, яка враховує реалії війни: облаштування укриттів і систем оповіщення, створення протоколів дій під час масованих атак, впровадження технологій кіберзахисту та забезпечення психосоціальної підтримки студентів і персоналу. Така програма має базуватися на положеннях чинного законодавства України та інтегрувати міжнародні стандарти безпеки освітнього середовища. Зроблено висновок про необхідність системного поєднання правових, організаційних та технічних інструментів для гарантування безперервності навчання й наукової діяльності навіть у кризових умовах війни.

**Ключові слова**: заклади вищої освіти, воєнний стан, безпека життєдіяльності, охорона праці, кіберзагрози, цивільний захист, освітнє середовище.

## COMPREHENSIVE SECURITY OF HIGHER EDUCATION INSTITUTIONS: LEGAL AND ORGANIZATIONAL ASPECTS

The paper examines the problems of ensuring the safety of higher education institutions in Ukraine as a multi-component system that encompasses the protection of students’ and staff members’ lives and health, preservation of property, safe operation of buildings and facilities, and counteraction to modern challenges, including cyber threats and wartime risks. The necessity of developing a comprehensive safety program for universities is emphasized, which should be based on the provisions of current Ukrainian legislation and take into account international standards. Particular attention is paid to fostering a safety culture among students and employees, implementing modern monitoring and cybersecurity technologies, organizing preventive measures and medical examinations, as well as coordinating actions with law enforcement agencies and civil protection services. The conclusion highlights the importance of a systemic approach that combines legal, organizational, and technical instruments to ensure the effective functioning of higher education institutions even under martial law and crisis conditions.

**Keywords**: higher education institutions, life safety, occupational safety, cyber threats, civil protection, educational environment, wartime security.

**Вступ**.

Заклади вищої освіти України (далі – ЗВО), такі як університети, академії та інститути, є об'єктами масового перебування людей і стратегічними вузлами інтелектуального потенціалу держави, що відповідно до Закону України «Про освіту» та Закону України «Про вищу освіту» зобов'язані забезпечувати безпечні та нешкідливі умови навчання, праці й проживання здобувачів освіти, співробітників і відвідувачів, а також гарантувати збереження майна та архітектурної цілісності будівель і споруд. У сучасних умовах, позначених тривалою воєнною агресією, масштабними руйнуваннями цивільної інфраструктури та постійним ризиком застосування ворогом балістичного озброєння, авіаційних ударів і безпілотних літальних апаратів, функція забезпечення безпеки у ЗВО трансформувалася з формального дотримання технічних регламентів у життєво необхідну стратегію виживання. Питання безпеки життєдіяльності в освітньому середовищі стали критично актуальними через необхідність протидії не лише класичним техногенним і природним ризикам, а й специфічним воєнним загрозам: від безпосередніх фізичних влучань у навчальні корпуси до мінної небезпеки та руйнування систем життєзабезпечення (енерго-, водо- та теплопостачання). Це зумовлює суворе дотримання положень Кодексу цивільного захисту України, який у 2022-2026 роках було значно деталізовано в частині вимог до облаштування надійних захисних споруд, створення безбар'єрних укриттів, систем екстреного оповіщення та розробки чітких протоколів реагування на надзвичайні ситуації воєнного характеру в місцях масового скупчення людей.

**Викладення основного матеріалу**.

Заклади вищої освіти надають освітні послуги, здійснюють науково–дослідну діяльність і використовують сучасне лабораторне обладнання, експлуатація якого пов'язана з вимогами охорони праці відповідно до Закону України «Про охорону праці». Водночас заклади освіти функціонують як складні господарські комплекси, що самостійно вирішують питання експлуатації будівель, роботи комунальних служб, систем вентиляції та енергопостачання, що в умовах воєнного стану потребує системного підходу до безпеки, який поєднує правові, організаційні та технічні інструменти. Аналіз небезпек для закладів вищої освіти дозволяє зробити висновок, що забезпечення їхньої безпеки складається з організації умов безпечної життєдіяльності співробітників, студентів і відвідувачів як у повсякденній діяльності, так і в надзвичайних ситуаціях, вирішення питань збереження майна та безпечної експлуатації споруд.

У науковій літературі проблеми безпеки ЗВО часто розглядаються вузько, акцентуючи увагу переважно на пожежній безпеці чи техніці безпеки, що не дозволяє комплексно вирішувати питання захисту від динамічних воєнних загроз, масованих обстрілів чи гібридних кібератак на критичну інфраструктуру університету. Відповідно до законодавства, першочерговим завданням є забезпечення учасників освітнього процесу знаннями у сфері безпеки життєдіяльності, що формує фундамент загальної культури безпеки.

Створення безпечних умов навчання у закладах вищої освіти охоплює багаторівневий комплекс заходів: по-перше, систематичне навчання керівників і працівників з питань охорони праці та цивільного захисту, яке має супроводжуватися регулярними практичними тренуваннями з евакуації та моделюванням складних воєнних кризових сценаріїв, включаючи алгоритми дій під час затяжних повітряних тривог або зникнення зв'язку; по-друге, атестація робочих місць за умовами праці, особливо у лабораторіях та дослідницьких центрах, де використовується високотехнологічне обладнання, джерела випромінювання чи небезпечні хімічні сполуки, що потребують особливого протоколу консервації у разі загрози влучання;

по-третє, організація безперервного виробничого контролю за дотриманням санітарно-гігієнічних норм у навчальних корпусах та гуртожитках, що в умовах війни включає моніторинг якості води та автономного функціонування систем життєзабезпечення; по-четверте, налагодження прозорої цифрової системи розслідування та обліку нещасних випадків, що дозволяє оперативно аналізувати ризики та коригувати безпекові протоколи відповідно до вимог чинного законодавства; по-п'яте, інтегроване забезпечення пожежної, радіаційної та хімічної безпеки через впровадження автоматизованих систем раннього виявлення загроз та розробку адаптивних планів евакуації, які враховують загрози балістичних ударів, диверсійних актів чи пошкодження систем енергоживлення; по-шосте, проведення поглиблених медичних оглядів та створення дієвих служб психосоціальної підтримки для профілактики професійного вигорання, збереження ментального здоров'я та подолання симптомів ПТСР у студентів і персоналу, що є критичним в умовах тривалого перебування у зоні бойових дій; по-сьоме, впровадження інтелектуальних систем кіберзахисту для убезпечення персональних даних та цифрових освітніх платформ від несанкціонованого втручання, що є частиною інформаційної безпеки держави; наостанок – комплексна модернізація та безпечна експлуатація будівель, що передбачає не лише оновлення застарілих інженерних мереж, а й обов'язкове зміцнення та інклюзивне облаштування споруд цивільного захисту (укриттів), які мають забезпечувати тривале та безпечне перебування великої кількості людей з доступом до засобів зв'язку та необхідних ресурсів.

**Висновки**.

Все викладене дозволяє зробити висновок, що безпека ЗВО має забезпечуватися на науковій основі через реалізацію комплексної програми, яка включатиме правові, організаційні та технічні заходи. Така програма має передбачати впровадження технологій кіберзахисту, системне навчання діям у надзвичайних ситуаціях воєнного характеру, формування культури безпеки та створення ефективних механізмів взаємодії з правоохоронними органами і службами цивільного захисту. Лише такий системний підхід здатен забезпечити стійке функціонування університетів, захист прав студентів і працівників та безпечний розвиток освітнього середовища навіть у кризових умовах.

**Список використаних джерел**

1. Верховна Рада України. Про освіту : Закон від 05.09.2017 № 2145–VIII. URL: https://zakon.rada.gov.ua/go/2145–19.

2. Верховна Рада України. Про вищу освіту : Закон від 01.07.2014 № 1556–VII. URL: https://zakon.rada.gov.ua/go/1556–18.

3. Верховна Рада України. Про охорону праці : Закон від 14.10.1992 № 2694–XII. URL: https://zakon.rada.gov.ua/go/2694–12.

4. Верховна Рада України. Кодекс цивільного захисту України : Закон від 02.10.2012 № 5403–VI. URL: https://zakon.rada.gov.ua/go/5403–17.

5. Президент України. Стратегія кібербезпеки України : Указ від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/go/447/2021.

6. Filipenko N., Spitsyna H., Andrieieva O. (2023) Security of higher educational institutions in Ukraine: today's realities. Забезпечення стійкості у складних умовах: збірник матеріалів доповідей. Харків, 2023. С. 19-22. DOI: https://doi.org/10.32620/BRCE.23.

https://doi.org/10.5281/zenodo.20496700

***Наталія БОНДАР,***
*кандидат юридичних наук,*
*завідувач кафедрою цивільно-правових дисциплін*
*та правового забезпечення підприємницької діяльності*
*ТОВ "Харківський університет", Харків, Україна*
*ORCID: https://orcid.org/0000-0002-7563-8493*
*e-mail: nataliiabondar28@gmail.com*

# КОРПОРАТИЗАЦІЯ ПІДПРИЄМСТВ АВІАЦІЙНОЇ ГАЛУЗІ В УКРАЇНІ: ПІДСТАВИ, ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ, РЕЗУЛЬТАТИ РЕАЛІЗАЦІЇ

У тезах досліджено корпоратизацію підприємств авіаційної галузі в Україні, її підстави, законодавче забезпечення та результати реалізації. Розкрито відмінність корпоратизації від приватизації, проаналізовано положення Закону України № 4196-IX щодо вибору організаційно-правової форми. Окреслено особливості корпоратизації стратегічних підприємств, їх роль у забезпеченні критичної інфраструктури та національної безпеки. Визначено основні результати реформи корпоративного управління, а також проблеми її впровадження. Обґрунтовано необхідність подальшого вдосконалення правового регулювання.

**Ключові слова***:* корпоратизація; державні підприємства; авіаційна галузь; корпоративне управління; акціонерне товариство; товариство з обмеженою відповідальністю; державна власність; критична інфраструктура; законодавство.

# CORPORATIZATION OF AVIATION INDUSTRY ENTERPRISES IN UKRAINE: GROUNDS, LEGAL FRAMEWORK, AND IMPLEMENTATION RESULTS

The theses examine the corporatization of aviation industry enterprises in Ukraine, its grounds, legal framework, and implementation results. The distinction between corporatization and privatization is clarified, and the provisions of Law of Ukraine No. 4196-IX regarding the choice of organizational and legal form are analyzed. The specific features of corporatization of strategic enterprises and their role in ensuring critical infrastructure and national security are outlined. The main outcomes of corporate governance reform, as well as challenges in its implementation, are identified. The necessity of further improvement of legal regulation is substantiated.

**Keywords***:* corporatization; state-owned enterprises; aviation industry; corporate governance; joint-stock company; limited liability company; state ownership; critical infrastructure; legislation

**Вступ.**

В умовах трансформації економіки України, воєнних викликів та необхідності забезпечення стійкості критичної інфраструктури особливого значення набуває реформування державного сектору. Одним із ключових інструментів такої трансформації є корпоратизація державних підприємств, яка передбачає зміну організаційно-правової форми та впровадження сучасних стандартів корпоративного управління. Для підприємств авіаційної галузі та об'єктів критичної інфраструктури ця реформа є не лише економічною, а й безпековою необхідністю. Реформа корпоративного управління державними підприємствами (ДП) в Україні триває з 1993 року.[6] У той же час в процесі реалізації цієї реформи, виникають питання, які потребують чіткого визначення, задля вірної правореалізації.

Як для науки, так і для правозастосування, важливо чітко усвідомлювати чітку різницю між корпоратизацією та іншими процесами реорганізації юридичних осіб, що відбуваються сьогодні у нашій державі.

Основна різниця між приватизацією та корпоратизацією полягає у зміні форми власності: приватизація передбачає перехід майна у приватні руки, тоді як корпоратизація залишає власником державу, але змінює структуру управління підприємством.[5]

Проведення корпоратизації державного унітарного підприємства в акціонерне товариство не є його приватизацією, а тому внесення майна до статутного фонду такого товариства не може розглядатися як підстава для зміни його форми власності. У зв'язку із цим державне майно, передане державою до статутного фонду державного унітарного підприємства, корпоратизованого в акціонерне товариство, 100% акцій статутного фонду якого залишаються у власності держави, до моменту завершення процедури приватизації є державною власністю.[9]

**Підстави корпоратизації підприємств в Україні.**

Корпоратизація державних підприємств обумовлена низкою економічних, правових та інституційних факторів. По-перше, значна частина державного сектору характеризується низькою ефективністю управління, що зумовлено застарілими підходами до організації діяльності. По-друге, існує потреба у підвищенні прозорості та підзвітності, що особливо актуально для стратегічних підприємств.

Важливим чинником є також інтеграція України до європейського економічного простору[1][1], яка передбачає адаптацію до стандартів корпоративного управління, зокрема рекомендацій міжнародних організацій. Для підприємств авіаційної галузі це має критичне значення, оскільки вони функціонують у висококонкурентному та технологічно складному середовищі.

Посилення корпоративного управління ДП залишається одним із ключових напрямів ширшої програми реформ України, включно з цілями європейської інтеграції, зобов'язаннями в межах міжнародних програм фінансової допомоги, а також пріоритетами відновлення та відбудови. [2]

**Законодавче забезпечення корпоратизації.**

Правове регулювання корпоратизації в Україні базується на нормах господарського та цивільного законодавства, а також спеціальних нормативно-правових актах, що визначають порядок реформування державних підприємств.

Одним з основних нормативних актів, що регулює процес корпоратизації державних та комунальних підприємств в Україні є Закон Про особливості регулювання діяльності юридичних осіб окремих організаційно-правових форм у перехідний період та об'єднань юридичних осіб від 9 січня 2025 року № 4196-IX [7] (далі по тексту Закону № 4196-IX), яким передбачена втрата чинності Господарського кодексу України.

Відповідно до ч. 2 ст. 14 цього Закону № 4196-IX у разі перетворення підприємства, єдиним учасником (засновником) якого є держава або територіальна громада (територіальні громади), уповноважений суб'єкт управління об'єктами державної власності або уповноважений орган місцевого самоврядування самостійно обирає організаційно-правову форму юридичної особи - правонаступника такого підприємства.

До таких форм належать:

[1] Інтеграція України до європейського економічного простору розпочата Угодою про партнерство та співробітництво від 14 червня 1994, що набула чинності 1 березня 1998 р. та повинна завершитися зі вступом України до ЄС

| | |
|---|---|
| державне комерційне підприємство<br>казенне підприємство | ➢ **АТ/ТОВ** 100 % акцій/часток у статутному капіталі якого належать **державі**<br>➢ **Державне некомерційне товариство** |
| комунальне комерційне підприємство | ➢ **АТ/ТОВ** 100 % акцій/часток у статутному капіталі якого належать **територіальній громаді**<br>➢ **комунальне некомерційне товариство** |
| спільне комунальне підприємство | ➢ **АТ/ТОВ** *(із збереженням пропорцій участі відповідних територіальних громад).*<br>➢ **комунальне некомерційне товариство** *(із збереженням пропорцій участі відповідних територіальних громад).* |

Порівняльна таблиця АТ та ТОВ [10]

| **Переваги АТ** | **Недоліки АТ** |
|---|---|
| ➢ для великих компаній з широкими можливостями залучення капіталу<br>➢ можливість залучення значних інвестицій (АТ може випускати акції та залучати великі суми капіталу)<br>➢ безперервність діяльності (зміна власників акцій не впливає на безперервність діяльності АТ);<br>➢ висока ліквідність акцій (обіг на фондовому ринку) | ➢ Складна система регулювання та звітності (підлягають суворішому регулюванню)<br>➢ Ризик втрати контролю (при збільшенні кількості акціонерів власники можуть втратити контроль над компанією)<br>➢ Додаткові витрати на управління та організацію (додаткові обов'язкові процедури – ведення реєстру акціонерів і т. ін.)<br>➢ Встановлено мінімальний розмір статутного фонду (капіталу) |
| **Переваги ТОВ** | **Недоліки ТОВ** |
| ➢ Обирають для малого та середнього бізнесу, де обмежена відповідальність є ключовим фактором;<br>➢ Обмежена відповідальність;<br>➢ Простота управління (ТОВ є менш складним, ніж в АТ, особливо для невеликих компаній);<br>➢ Можливість залучення інвесторів (може залучати інвестицій та кредити для розвитку);<br>➢ Менші витрати на створення та ведення (ТОВ обходиться дешевше ніж АТ) | ➢ Обмеження у залучені великих інвестицій<br>➢ Складність управління при збільшенні кількості учасників (може ускладнити процес прийняття рішень та управління) |

| | |
|---|---|
| ➢ Відсутній мінімальний розмір статутного капіталу | |

Ключовими елементами законодавчого забезпечення є:

- визначення правового статусу державних акціонерних товариств;
- розмежування функцій власника (держави) та органів управління;
- запровадження наглядових рад із незалежними членами;
- встановлення вимог до прозорості діяльності та фінансової звітності.

Окрему роль відіграють нормативні акти, що регламентують управління об'єктами державної власності, а також законодавство у сфері корпоративного управління. В умовах воєнного стану ці механізми доповнюються спеціальними інструментами державного контролю, що спрямовані на забезпечення безперервності функціонування критичної інфраструктури.

**Особливості корпоратизації підприємств авіаційної галузі.**

Підприємства авіаційної галузі належать до стратегічно важливих об'єктів економіки та безпеки держави. Їх корпоратизація має враховувати специфіку галузі, зокрема:

- високий рівень технологічної складності;
- значну капіталомісткість;
- залежність від міжнародних стандартів та ринків;
- критичну роль у забезпеченні обороноздатності.

У цьому контексті корпоратизація повинна поєднувати ринкові механізми управління з ефективним державним контролем. Особливо важливим є забезпечення балансу між економічною ефективністю та національною безпекою.

**Результати реалізації корпоратизації.**

З 2021 року Україна суттєво зміцнила систему корпоративного управління ДП, значною мірою наблизивши правову базу до Керівних принципів ОЕСР [4] з корпоративного управління державними підприємствами, попри обмеження воєнного часу. Починаючи з 2021 року, Україна здійснила масштабні законодавчі та політичні реформи для вдосконалення екосистеми ДП. У сукупності вони значно наближують законодавчу базу України до стандартів, закріплених у Керівних принципах ОЕСР з корпоративного управління на підприємствах державної форми власності (далі — «Керівні принципи ДП») Практична імплементація реформ в рамках всієї групи ДП залишається нерівномірною, а результати від посилення корпоративного управління істотно відрізняються між великими підприємствами та рештою ДП.

Станом на сьогодні корпоратизація в Україні має як позитивні результати, так і низку проблемних аспектів. [3]

До основних досягнень можна віднести:

- підвищення прозорості діяльності окремих державних підприємств;
- впровадження елементів сучасного корпоративного управління;
- зростання інвестиційної привабливості окремих компаній;
- покращення фінансових показників у ряді випадків.

Водночас існують суттєві виклики:

- неповна реалізація принципів корпоративного управління;
- збереження політичного впливу на діяльність підприємств;
- недостатній рівень професійності органів управління;
- ризики формального характеру реформ.

Для підприємств критичної інфраструктури додатковим викликом є необхідність функціонування в умовах підвищених ризиків, пов'язаних із воєнними діями.

**Перспективи розвитку.**

У найближчі роки очікується активізація процесів корпоратизації, зокрема у стратегічних галузях. Основними напрямами розвитку є:

- удосконалення законодавчої бази;
- посилення ролі незалежних наглядових рад;
- цифровізація управління державними підприємствами;
- залучення міжнародних партнерів до реформування.

Особливу увагу слід приділити забезпеченню стійкості підприємств авіаційної галузі, що передбачає інтеграцію принципів сталого розвитку, ризик-менеджменту та безпекових стандартів.

**Виключення.**

Реформування (перетворення) оборонної промисловості та залізничного транспорту загального користування в Україні здійснюється відповідно до спеціального законодавства[8], тобто дія Закону України Про особливості регулювання діяльності юридичних осіб окремих організаційно-правових форм у перехідний період та об'єднань юридичних осіб Закон України від 9 січня 2025 р. № 4196-IX на ці сфери не розповсюджується.

**Висновки.**

Корпоратизація підприємств в Україні є важливим інструментом підвищення ефективності державного сектору та забезпечення стійкості критичної інфраструктури. Вона створює передумови для інтеграції у міжнародний економічний простір, залучення інвестицій та підвищення конкурентоспроможності.

Водночас успішність реалізації цієї реформи залежить від якості законодавчого забезпечення, ефективності інституцій та рівня політичної волі. Для підприємств авіаційної галузі корпоратизація має здійснюватися з урахуванням стратегічного значення галузі та необхідності забезпечення національної безпеки.

**Список використаних джерел:**


1. Угода про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами від 14 червня 1994 URL: https://zakon.rada.gov.ua/laws/show/998_012/ed19940614#Text (дата звернення 16.04.2026)
2. Огляд ОЕСР щодо корпоративного управління державними підприємствами в Україні, 2026 С.5 URL: https://www.oecd.org/content/dam/oecd/en/publications/support-materials/2026/04/oecd-review-of-the-corporate-governance-of-state-owned-enterprises-in-ukraine-2026_6e0b273c/Ukraine-SOE-Review-highlights-UKR.pdf (дата звернення 16.04.2026)
3. Огляд ОЕСР щодо корпоративного управління державними підприємствами в Україні, 2026 URL: https://www.oecd.org/content/dam/oecd/en/publications/support-materials/2026/04/oecd-review-of-the-corporate-governance-of-state-owned-enterprises-in-ukraine-2026_6e0b273c/Ukraine-SOE-Review-highlights-UKR.pdf (дата звернення 16.04.2026)
4. ОЕСР - Organisation for Economic Co-operation and Development - https://www.oecd.org/uk/publications/2024_8d61003c-uk.html (дата звернення 16.04.2026)
5. Правова позиція викладена в Постанові Великої Палати Верховного Суду від 3.04.2024 у справі №917/1212/21 URL: https://reyestr.court.gov.ua/Review/118297147 (дата звернення 16.04.2026)
6. Про корпоратизацію підприємств Указ Президента України N 210/93 від15 червня 1993 року URL: https://zakon.rada.gov.ua/laws/show/210/93#Text (дата звернення 16.04.2026)

7. Про особливості регулювання діяльності юридичних осіб окремих організаційно-правових форм у перехідний період та об'єднань юридичних осіб Закон України від 9 січня 2025 р. № 4196-IX URL: https://zakon.rada.gov.ua/laws/show/4196-20?find=1&text=%D1%81%D0%B0%D0%BC%D0%BE%D1%81%D1%82%D1%96%D0%B9%D0%BD%D0%BE#w1_1

8. Про особливості реформування підприємств оборонно-промислового комплексу державної форми власності. Закон України № 1630-IX від 13 липня 2021 р https://zakon.rada.gov.ua/laws/show/1630-20#Text; (дата звернення 16.04.2026) Про особливості утворення акціонерного товариства залізничного транспорту загального користування Закон України № 4442-VI від 23 лютого 2012 р. https://zakon.rada.gov.ua/laws/show/4442-17#Text (дата звернення 16.04.2026)

9. Чим корпоратизація відрізняється від приватизації, нагадала ВП ВС 07.01.2025 Закон і бізнес
URL: https://zib.com.ua/ua/164940.html#:~:text=%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B8%D1%85%20%D1%83%D0%BD%D1%96%D1%82%D0%B0%D1%80%D0%BD%D0%B8%D1%85%20%D0%BF%D1%96%D0%B4%D0%BF%D1%80%D0%B8%D1%94%D0%BC%D1%81%D1%82%D0%B2%20%D1%87%D0%B5%D1%80%D0%B5%D0%B7%20%D1%97%D1%85%20%D0%BF%D0%B5%D1%80%D0%B5%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F,%D1%82%D0%BE%D0%B2%D0%B0%D1%80%D0%B8%D1%81%D1%82%D0%B2%D0%B0%20%D1%94%20%D0%BB%D0%B8%D1%88%D0%B5%20%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D1%83%D0%BC%D0%BE%D0%B2%D0%BE%D1%8E%20%D0%B4%D0%BB%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%B0%D0%BB%D1%8C%D1%88%D0%BE%D1%97%20%D0%BF%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%97 (дата звернення 16.04.2026)

10. Щербакова Н., «Скасування Господарського кодексу» Вебінар від 14.08.2025 р. https://www.google.com/search?q=%D0%B2%D1%96%D0%B4%D0%BC%D1%96%D0%BD%D0%B0+%D0%B3%D0%BE%D1%81%D0%BF%D0%BE%D0%B4%D0%B0%D1%80%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE+%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D1%83%2C+%D1%89%D0%B5+%D0%BF%D1%80%D0%BE%D0%B4%D0%BE%D0%B2%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F+%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%83+%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%97&oq=%D0%B2%D1%96%D0%B4%D0%BC%D1%96%D0%BD%D0%B0+%D0%B3%D0%BE%D1%81%D0%BF%D0%BE%D0%B4%D0%B0%D1%80%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE+%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D1%83%2C+%D1%89%D0%B5+%D0%BF%D1%80%D0%BE%D0%B4%D0%BE%D0%B2%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F+%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%83+%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%97&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCjM1Njg4ajBqMTWoAgiwAgHxBbaxEEa5eNL-&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:c4d676f6,vid:thNA5DAhcmI,st:0 (дата звернення 16.04.2026)

https://doi.org/10.5281/zenodo.20496722

***Алла ГОРДЕЮК,***
*кандидатка юридичних наук, доцентка, професор «ХАІ»*
*доцентка кафедри права Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://*orcid.org/0000-0001-7423-3673
*e-meil:a.hordeiuk@khai.edu*

***Руслан ДЕМУРА,***
*аспірант кафедри комп'ютерних систем, мереж і кібербезпеки*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://orcid.org/0009-0003-2248-2565*
*e-mail:r.i.demura@csn.khai.edu*

## ПРАВОВИЙ АСПЕКТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

У даній роботі висвітлюється питання правової регламентації забезпечення кібербезпеки цивільної авіації на міжнародному (в тому числі регіональному) та національному рівнях. Зазначено на Чиказьку конвенцію як базовий міжнародний нормативний акт у сфері цивільної авіації, котрий встановлює керівні положення щодо забезпечення безпечного функціонування цивільної авіації та слугує правовим підґрунтям для діяльності Міжнародної організації цивільної авіації. Зазначено, що ця організація є платформою для нормотворчості і суттєвим результатом її діяльності є доопрацювання Додатку 17 «Авіаційна безпека» Стандартів та рекомендованих практик (SARPs) та додання нового Стандарту, що рекомендує державам розробляти і впроваджувати заходи захисту критичних інформаційно-комунікаційних систем та даних цивільної авіації від кібератак. При цьому зауважено на рекомендаційний характер положень SARPS, що тягне за собою проблему необов’язкового їх дотримання та створює суттєву прогалину в системі забезпечення кібербезпеки на глобальному рівні. Також охарактеризовано багаторівневу нормативну архітектуру забезпечення кібербезпеки в авіаційній галузі на рівні ЄС, зокрема зазначено на нову Директиву (ЄС) 2022/2555 (NIS 2) з кібербезпеки, яка поширює єдину правову рамку кібербезпеки, зокрема на авіаційний сектор, встановлює вимоги до управління ризиками та обов'язкового звітування про інциденти. Вказано на як очевидну законодавчу прогалину – відсутність норм про кібербезпеку цивільної авіації у Повітряному кодексі України та на доцільність внесення до нього відповідних змін з метою гармонізації національного авіаційного права з правом ЄС. У кримінально-правовому аспекті стосовно міжнародного кримінального переслідування кібератак на авіацію зазначено на відсутність правової регламентації у зв’язку з несанкціонованим втручанням у функціонування авіаційних систем. Зроблено висновки про те, що правове забезпечення кібербезпеки цивільної авіації перебуває на сьогодні у стані активного формування і про те, що цей процес у силу його актуальності потребує постійного контролю з боку міжнародного авіаційного співтовариства.

**Ключові слова:** авіаційна галузь, цивільна авіація, кібербезпека, кібератака, правова регламентація

## LEGAL ASPECTS OF CYBERSECURITY IN CIVIL AVIATION

This paper examines the legal framework governing cybersecurity in civil aviation at the international, regional, and national levels. The Chicago Convention is identified as the fundamental

international legal instrument in the field of civil aviation, establishing the guiding principles for the safe operation of civil aviation and serving as the legal basis for the activities of the International Civil Aviation Organization. The paper notes that this organization acts as a platform for rule-making, and that one of the significant outcomes of its activities is the revision of Annex 17 “Aviation Security” to the Standards and Recommended Practices (SARPs), as well as the introduction of a new Standard recommending that States develop and implement measures to protect critical civil aviation information and communication systems and data from cyberattacks. At the same time, attention is drawn to the non-binding nature of the SARPs provisions, which creates the problem of inconsistent compliance and constitutes a significant gap in the global cybersecurity framework.

The paper also characterizes the multi-level regulatory architecture of cybersecurity in the aviation sector at the EU level, with particular attention to Directive (EU) 2022/2555 (NIS 2), which extends a common cybersecurity framework to, inter alia, the aviation sector and establishes requirements for risk management and mandatory incident reporting. The paper identifies an obvious legislative gap, namely the absence of provisions on civil aviation cybersecurity in the Air Code of Ukraine, and substantiates the expediency of introducing relevant amendments in order to harmonize national aviation law with EU law. From the perspective of criminal law and international criminal prosecution of cyberattacks targeting aviation, the paper points to the absence of specific legal regulation concerning unauthorized interference with the operation of aviation systems. It is concluded that the legal framework for civil aviation cybersecurity is currently undergoing active development and that, given its importance, this process requires constant attention from the international aviation community.

**Keywords:** aviation industry, civil aviation, cybersecurity, cyberattack, legal regulation.

**Вступ**.

Увага до тематики з правового забезпечення кібербезпеки цивільної авіації зумовлена глобальною цифровізацією цієї галузі – від автоматизованих систем управління повітряним рухом (АТМ) до бортових авіоніки та наземної інфраструктури. Такі стрімкі зміни суттєво розширили поверхню кібератак на об’єкти критичної інфраструктури та актуалізували потребу у вдосконалені правової регламентації щодо створення дієвих механізмів убезпечення авіаційних кібертехнологій.

**Виклад основного матеріалу.**

Базовим міжнародно-правовим інструментом для авіаційної галузі на сьогодні залишається Чиказька конвенція про міжнародну цивільну авіацію 1944 року (Чиказька конвенція), яка хоча й не містить прямих норм щодо кіберзахисту, але слугує конституційною основою для діяльності Міжнародної організації цивільної авіації (International Civil Aviation Organization, далі – ІКАО ). У відповідь на нові загрози, 41-а сесія Асамблеї ІКАО у 2022 р. ухвалила Резолюцію A41-19 «Addressing Cybersecurity in Civil Aviation», що прийшла на зміну резолюціям A39-19 (2016) та A40-10 (2019) та закликала держави впроваджувати Стратегію кібербезпеки цивільної авіації, засновану на семи стовпах: міжнародна співпраця, управління, ефективне законодавство, кібербезпекова політика, обмін інформацією, управління інцидентами та розбудова потенціалу [1]. Ключовим нормативним досягненням стало включення до Додатку 17 «Авіаційна безпека» SARPs до Чиказької конвенції Стандарту 4.9.1, що рекомендує державам розробляти і впроваджувати заходи захисту критичних інформаційно-комунікаційних систем та даних цивільної авіації від кібератак [2]. Попри це, правова природа SARPs не є юридично обов'язковою у класичному розумінні міжнародного права, що породжує правозастосовну проблему дотримання: держава може нотифікувати

різницю між своїм законодавством і стандартом, а не бути юридично зобов'язаною усунути її. Це становить суттєву прогалину в системі забезпечення кібербезпеки на глобальному рівні.

На регіональному рівні, зокрема на рівні ЄС сформовано багаторівневу нормативну архітектуру забезпечення кібербезпеки в авіаційній галузі. Так, Директива ЄС 2022/2555 (NIS 2) з кібербезпеки набула чинності 16 січня 2023 р. та замінила Директиву ЄС (NIS 1) з 18 жовтня 2024 р. Вона поширює єдину правову рамку кібербезпеки, зокрема на транспортний та авіаційний сектори, встановлює вимоги до управління ризиками та обов'язкового звітування про інциденти [3]. Водночас Імплементаційний Регламент ЄС 2023/203 (EASA Part-IS) як законодавчий акт з інформаційної безпеки в авіаційній галузі, запровадив авіаційно-специфічні вимоги до систем управління інформаційною безпекою (ISMS) для організацій, що підпадають під сертифікацію EASA (організацій з технічного обслуговування, авіаційних навчальних центрів тощо). Принципово важливим є те, що відповідність NIS 2 не означає автоматичної відповідності Part-IS: ці два нормативні акти мають різний предметний охват та цілі, і EASA наразі опрацьовує механізм взаємозаліку [4]. Для України, яка взяла курс на євроінтеграцію та імплементацію *acquis communautaire*, це означає необхідність двоколійного виконання авіаційного законодавства ЄС в рамках Угоди про асоціацію та адаптації до NIS 2 у сфері критичної інформаційної інфраструктури.

Правову основу кібербезпеки в Україні складає Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, який визначає критичну інформаційну інфраструктуру (КІІ) та встановлює систему суб'єктів кібербезпеки на чолі з Національним координаційним центром кібербезпеки при РНБО [5]. Авіаційна інфраструктура підпадає під транспортний сектор КІІ. Постанова КМУ від 19.06.2019 № 519 затвердила загальні вимоги до кіберзахисту об'єктів КІІ, що гармонізовані зі стандартами ЄС, НАТО та NIST (Національний інститут стандартів і технологій США – федеральне агентство, що розробляє технічні стандарти, методики вимірювань та рекомендації у сфері кібербезпеки). [6]. Разом з тим Повітряний кодекс України не містить спеціальних норм щодо кібербезпеки, що є очевидною законодавчою прогалиною. Вбачається доцільним внесення змін до Повітряного кодексу з метою закріплення: обов'язку авіаційних операторів мати сертифіковану ISMS, правового режиму кіберінциденту в авіації та відповідальності за його незвітування. Такі зміни відповідали б Standard 4.9.1 Annex 17 та вимогам Part-IS і сприяли б гармонізації з правом ЄС.

Щодо кримінально-правового виміру та міжнародного кримінального переслідування кібератак на авіацію, то слід зазначити, що Конвенція про боротьбу з незаконними актами відносно міжнародної цивільної авіації (Пекінська конвенція) від 2010 р. (Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation) та Пекінський протокол від 2010 р., що доповнив Гаазьку конвенцію про боротьбу з незаконним захопленням повітряних суден 1970 р., розширили склади злочинів у сфері авіаційної безпеки, охопивши кібератаки на бортові системи управління [1]. Асамблея ІКАО 41а від 2022 р. закликала держави ратифікувати ці документи саме як інструменти боротьби з кіберзагрозами цивільній авіації. Також Конвенція Ради Європи про кіберзлочинність 2001 р. (Будапештська конвенція), ратифікована Україною у 2005 р., закладає загальні кримінально-правові стандарти щодо несанкціонованого втручання в комп'ютерні системи [7]. Проте жодний з цих документів не містить спеціальних норм щодо авіаційних систем організації повітряного руху (ATM), авіоніки або систем управління аеропортом. Це свідчить про наявність lacuna legis (правової прогалини) у міжнародному кримінальному праві, яка потребує заповнення або через розробку спеціального протоколу до Будапештської конвенції, або через відповідні положення у майбутніх актах ІКАО.

Слід зазначити, що транскордонний характер кіберзагроз авіації породжує комплекс правових проблем: колізії юрисдикцій, складнощі атрибуції нападу конкретному суб'єкту та відповідальності держав за дії підконтрольних їм угруповань. Стаття 1 Чиказької конвенції закріплює повний і виключний суверенітет держави над її повітряним простором, що могло б слугувати основою для юрисдикційних претензій у разі кібератаки на авіаційні системи в межах державної юрисдикції. Водночас «Стратегія кібербезпеки ІКАО» прямо передбачає, що координація кібербезпеки авіації повинна виходити за межі цивільної авіації та охоплювати взаємодію з національними/міжнародними органами кібербезпеки, правоохоронними структурами та військовими [8]. Це ставить питання розмежування між цивільно-правовим режимом ІКАО та режимом міжнародної відповідальності держав за кіберопераціями. За відсутності обов'язкових норм про атрибуцію кібератак у повітряному праві перспективним є застосування Tallinn Manual 2.0 від 2017 р. як доктринального інструменту тлумачення норм міжнародного права щодо кібероперацій проти критичної інфраструктури, включаючи авіаційну. Для України як держави, що перебуває в стані збройного конфлікту, питання атрибуції та відповідальності за кібератаки проти аеронавігаційної інфраструктури набуває практичного виміру.

**Висновки**.

Таким чином, у підсумку за наведеною вище аналітикою, можемо зауважити, що система міжнародно-правового забезпечення кібербезпеки цивільної авіації на сучасному етапі перебуває у стані активного формування. Її розвиток характеризується поліцентричністю джерел правового регулювання – від рекомендаційних актів ІКАО до юридично обов’язкових актів права Європейського Союзу, що зумовлює як нормативну багаторівневість, так і певну фрагментарність відповідного регулювання. З огляду на особливу значущість кіберзахисту для безпечного функціонування цивільної авіації цей процес потребує постійної уваги й координації з боку міжнародного авіаційного співтовариства.

До ключових правових прогалин у досліджуваній сфері доцільно віднести: по-перше, необов’язковий характер стандартів і рекомендованої практики ІКАО щодо кіберзахисту; по-друге, відсутність спеціальних норм щодо кіберінцидентів у сфері цивільної авіації в Повітряному кодексі України; по-третє, наявність прогалини у міжнародному кримінальному праві стосовно кваліфікації та переслідування кібератак на авіаційні системи.

Для України як держави-кандидата на членство в Європейському Союзі першочерговим завданням є імплементація та належна адаптація вимог Директиви (ЄС) 2022/2555 (NIS 2) і нормативних положень EASA Part-IS до національного законодавства з урахуванням специфіки авіаційного сектору. Саме такий підхід сприятиме посиленню правових засад кібербезпеки цивільної авіації та подальшій гармонізації національного авіаційного права з правом ЄС.

**Список використаних джерел:**

1. ICAO Assembly Resolution A41-19: Addressing Cybersecurity in Civil Aviation. 2022. URL: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/A41-19.pdf (дата звернення: 22.03.2026).

2. Annex 17 to the Convention on International Civil Aviation – Aviation Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference/ 12th ed., Amendment 18. Montreal : ICAO, 2022. URL: https://www.icao.int/aviation-security-policy-section/Annex17 (дата звернення: 22.03.2026).

3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation

(EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // Official Journal of the European Union. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 22.03.2026).

4. Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety // Official Journal of the European Union. 2023. L 31. URL: https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj (дата звернення: 22.03.2026).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 22.03.2026).

6. Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF (дата звернення: 22.03.2026).

7. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001, ратифікована Законом України № 2824-IV від 07.09.2005 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/go/994_575 (дата звернення: 22.03.2026).

8. Aviation Cybersecurity Strategy [Електронний ресурс]. – Montreal : International Civil Aviation Organization, 2019. URL: https://www.icao.int/sites/default/files/Meetings/a42/Documents/AVIATION-CYBERSECURITY-STRATEGY.EN_.pdf (дата звернення: 22.03.2026).

9. Svanadze V. Кібербезпека в цивільній авіації та існуючі виклики // Юридичний вісник «Повітряне і космічне право». 2020. Т. 4, № 57. С. 27–33. DOI: 10.18372/2307-9061.57.15039.

10. Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention, 2010) [Електронний ресурс]. ICAO Doc 9960. URL: https://www.icao.int/sites/default/files/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf (дата звернення: 22.03.2026).

https://doi.org/10.5281/zenodo.20496751

***Світлана ГУЦУ,***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: https://0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті досліджено інформаційну безпеку як ключову складову правового забезпечення кіберзахисту критичної інфраструктури в Україні в умовах воєнної агресії. Проаналізовано динаміку зростання кіберінцидентів та їх спрямованість на державні системи й об'єкти критичної інфраструктури. Розкрито зміст інформаційної безпеки як ширшої правової категорії порівняно з кібербезпекою. Виявлено проблеми фрагментарності законодавства, колізії між принципами відкритості інформації та вимогами безпеки, а також ризики відкритих реєстрів. Обґрунтовано необхідність удосконалення правового регулювання та гармонізації із європейськими стандартами.

**Ключові слова:** інформаційна безпека, кібербезпека, критична інфраструктура, захист інформації, міжнародні стандарти кіберзахисту.

# INFORMATION SECURITY AS A COMPONENT OF THE LEGAL FRAMEWORK FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE

**Abstract:** The article examines information security as a key component of the legal framework for ensuring the cybersecurity of critical infrastructure in Ukraine under conditions of armed aggression. It analyzes the dynamics of increasing cyber incidents and their targeting of state systems and critical infrastructure facilities. The study reveals the concept of information security as a broader legal category compared to cybersecurity. It identifies problems of legislative fragmentation, conflicts between the principles of information openness and security requirements, as well as risks associated with open public registers. The necessity of improving legal regulation and harmonizing it with European standards is substantiated.

**Keywords:** information security, cybersecurity, critical infrastructure, information protection, international cybersecurity standards.

**Вступ**.

В умовах збройної агресії проти України питання забезпечення кібербезпеки набувають особливої актуальності, оскільки об'єкти критичної інфраструктури стають пріоритетними цілями для кібератак. В останні три роки в Україні спостерігається різке та системне зростання їх кількості, а значна частина спрямована на державні органи та об'єкти критичної інфраструктури. За даними урядової команди реагування на кіберінциденти CERT-UA, у 2023 році було зафіксовано близько 2541 кіберінцидент, у 2024 році – 4315 інцидентів, що становить зростання майже на 70% [1].

**Виклад основного матеріалу**.

У 2025 році тенденція до ескалації кіберзагроз збереглася: кількість опрацьованих інцидентів сягнула приблизно 5927, що на 37% більше порівняно з 2024 роком [2]. Частина атак безпосередньо пов'язана з об'єктами критичної інфраструктури, зокрема енергетичним сектором, системами державного управління та сферою безпеки.

Статистичні дані також свідчать про високий рівень концентрації атак на ключові сектори. Найбільш ураженими залишаються місцеві органи влади, урядові структури, сектор безпеки та оборони, а також енергетична інфраструктура, що підтверджує їхню роль як пріоритетних цілей у кібервійні . Окремі дослідження фіксують, що у попередні роки значна частина інцидентів вже мала цілеспрямований характер щодо державних органів та критичних систем життєзабезпечення .

Загалом аналіз даних CERT-UA свідчить про сталість тенденції до щорічного зростання кіберінцидентів, а також про їхній системний характер у контексті воєнної агресії. Це підтверджує, що кіберпростір є одним із ключових театрів гібридного протистояння, а критична інфраструктура — одним із головних об'єктів кіберзагроз в Україні.

У цьому контексті інформаційна безпека виступає ключовим елементом правового забезпечення кіберзахисту, оскільки саме інформаційні ресурси, інформаційно-комунікаційні системи та дані є основою функціонування критично важливих сфер держави.

У сучасній правовій доктрині інформаційна безпека розглядається як стан захищеності інформаційного простору, за якого забезпечується цілісність, конфіденційність та доступність інформації. Водночас кібербезпека є більш вузьким поняттям і охоплює захист інформаційних систем від кіберзагроз. Таким чином, інформаційна безпека виступає ширшою категорією, яка включає як технічні, так і правові механізми захисту інформації, формуючи основу для ефективного кіберзахисту.

Нормативно-правове забезпечення інформаційної безпеки в Україні базується на низці законодавчих актів, зокрема Закон України «Про критичну інфраструктуру» [3], Закон України «Про основні засади забезпечення кібербезпеки України» [4], Закон України «Про інформацію» [5], Закон України «Про захист інформації в інформаційно-комунікаційних системах» [6]. Зазначені акти визначають правові та організаційні засади захисту інформації, регулюють діяльність суб'єктів забезпечення кібербезпеки, а також встановлюють вимоги до функціонування інформаційно-комунікаційних систем.

Важливе значення у формуванні сучасних підходів до забезпечення інформаційної безпеки критичної інфраструктури мають міжнародні стандарти та правові рамки, які визначають мінімальні вимоги до кіберзахисту та управління ризиками. Ключову роль у цьому контексті відіграють акти Європейського Союзу, зокрема Директива NIS Directive [7], яка встановлює обов'язки держав-членів щодо забезпечення високого спільного рівня кібербезпеки мережевих та інформаційних систем. Директива передбачає запровадження національних стратегій кібербезпеки, системи управління ризиками, а також механізмів обов'язкового повідомлення про кіберінциденти для операторів критичних послуг.

Додатково суттєвий вплив на формування правових підходів до захисту інформації має Загальний регламент захисту даних GDPR [8], який закріплює принципи законності, мінімізації даних та їх належного захисту. У контексті критичної інфраструктури його значення полягає у встановленні високих стандартів безпеки персональних та службових даних, що обробляються в інформаційних системах, які можуть бути частиною критичних сервісів. Це безпосередньо впливає на побудову правових механізмів захисту інформаційної безпеки в державному секторі та сфері публічних послуг.

На глобальному рівні важливу аналітичну та рекомендаційну функцію виконує Міжнародний союз електрозв'язку (ITU), який у своїх глобальних індексах кібербезпеки

оцінює рівень розвитку правових, організаційних і технічних заходів у державах. Крім того, агентство ENISA розробляє регулярні звіти про кіберзагрози та методології оцінки ризиків, які використовуються для формування політики ЄС у сфері захисту критичної інфраструктури. Ці підходи сприяють уніфікації стандартів кіберзахисту та поступовій гармонізації національних правових систем із міжнародними вимогами.

Особливе значення інформаційна безпека має у сфері функціонування об'єктів критичної інфраструктури, до яких належать підприємства та установи, що забезпечують життєво важливі потреби населення і держави. Порушення їхньої діяльності внаслідок кібератак або витоку інформації може спричинити значні соціально-економічні та безпекові наслідки. Основними загрозами у цій сфері є несанкціонований доступ до інформації, втручання в роботу інформаційних систем, поширення шкідливого програмного забезпечення, а також інформаційно-психологічний вплив.

Незважаючи на сформовану нормативну базу у сфері інформаційної та кібербезпеки, правове регулювання у сфері захисту критичної інфраструктури залишається недостатньо системним та узгодженим. Це насамперед проявляється у фрагментарності законодавства, тобто відсутності єдиного кодифікованого акта, який би комплексно врегульовував усі аспекти інформаційної безпеки та кіберзахисту.

Наприклад, правові норми, що регулюють одну й ту саму сферу, розпорошені між різними законами: питання загальної інформаційної безпеки частково регулюються Законом України «Про інформацію», технічний та організаційний кіберзахист – Законом України «Про основні засади забезпечення кібербезпеки України», захист інформації в системах – Законом України «Про захист інформації в інформаційно-комунікаційних системах», а правовий режим об'єктів критичної інфраструктури – Законом України «Про критичну інфраструктуру». У результаті виникає ситуація, коли одна й та сама подія (наприклад, кібератака на державний реєстр або енергетичну систему) може одночасно підпадати під різні правові режими, але жоден із них не дає повного алгоритму дій. Наприклад:

– Закон «Про кібербезпеку» визначає загальні суб'єкти реагування (CERT-UA, СБУ, НКЦК), але не встановлює детальної процедури координації під час масованої атаки;

– Закон «Про критичну інфраструктуру» визначає категорії об'єктів, але не деталізує вимоги до їх інформаційного захисту;

– Закон «Про інформацію» встановлює принципи відкритості, але не містить чітких критеріїв обмеження доступу до технічної інформації про системи КІ.

Як приклад практичної колізії можна навести ситуації під час кібератак на енергетичні системи або державні реєстри (2022–2024 роки), коли органи влади були змушені одночасно обмежувати доступ до технічної інформації про інфраструктуру з міркувань безпеки та виконувати вимоги законодавства про публічність і прозорість діяльності [9].

Ще одним проявом фрагментарності є відсутність єдиних стандартів класифікації інцидентів: різні органи (СБУ, Держспецзв'язку, адміністратори систем) можуть по-різному кваліфікувати одну й ту саму подію – як «кібератаку», «інцидент інформаційної безпеки» або «порушення цілісності системи», що ускладнює статистику, облік і правове реагування.

Таким чином, фрагментарність законодавства проявляється не лише у великій кількості нормативних актів, але й у відсутності єдиного понятійного апарату, узгоджених процедур реагування та комплексного правового механізму захисту критичної інфраструктури.

Окремої уваги потребує колізія між принципом відкритості інформації та вимогами інформаційної безпеки, яка особливо загострюється у сфері захисту критичної інфраструктури. Її практичний зміст полягає в тому, що державні органи одночасно

зобов'язані забезпечувати прозорість своєї діяльності та гарантувати недопущення розкриття відомостей, які можуть бути використані для здійснення кіберзагроз.

Так, відповідно до законодавства про доступ до публічної інформації, громадськість має право отримувати інформацію про діяльність органів влади, включно з даними про функціонування державних систем, використання бюджетних коштів, реалізацію проєктів цифровізації тощо. Однак у випадку критичної інфраструктури значна частина такої інформації має подвійний характер: вона є водночас публічно значущою і потенційно небезпечною для розкриття.

Наприклад, запити щодо структури державних інформаційних систем (зокрема реєстрів, енергетичних або транспортних платформ) теоретично можуть підпадати під право на доступ до публічної інформації. Водночас розкриття технічних деталей – таких як архітектура системи, маршрутизація даних, конфігурація серверів, механізми резервного копіювання або відомості про вразливості – створює прямі ризики для їхньої кібербезпеки. Саме ці дані можуть бути використані для планування кібератак або несанкціонованого втручання.

Також окремим аспектом зазначеної колізії є ризики, пов'язані з надмірною відкритістю державних інформаційних ресурсів, зокрема Єдиного державного реєстру судових рішень та інших відкритих електронних реєстрів. Хоча їх функціонування ґрунтується на принципі доступності та прозорості правосуддя й діяльності держави, у сучасних умовах цифровізації та гібридних загроз така відкритість може створювати додаткові ризики інформаційної безпеки. Зокрема, у Єдиному державному реєстрі судових рішень у відкритому доступі містяться великі масиви даних, які формально знеособлені, однак у сукупності можуть бути використані для аналітичної обробки. Йдеться про можливість автоматизованого збору інформації щодо:

– структури виробничих процесів підприємств енергетики, транспорту, комунального господарства;

– договірних відносин із підрядниками, включно з IT- та сервісними компаніями;

– технологічних спорів, аварій, збоїв у роботі обладнання або систем;

– фінансових і логістичних моделей функціонування підприємств;

– інформації про використання конкретного програмного забезпечення або обладнання.

У разі системного аналізу таких даних можливе формування детальної картини функціонування об'єкта критичної інфраструктури, що виходить за межі публічної мети розкриття інформації. У поєднанні з іншими відкритими джерелами це створює ризики проведення OSINT-розвідки, яка може бути використана для виявлення слабких місць у виробничих або енергетичних процесах, критичних вузлів інфраструктури, залежності від окремих постачальників або програмних рішень, потенційних точок для кібер- або фізичних атак.

Особливої уваги потребує те, що значна частина таких відомостей потрапляє у відкритий доступ не безпосередньо, а опосередковано – через судові спори (наприклад, щодо аварій, контрактів, стягнення збитків чи порушення господарських зобов'язань). У результаті публічні рішення судів можуть містити фрагменти технічної або виробничої інформації, яка в сукупності формує чутливий профіль об'єкта критичної інфраструктури.

Таким чином, виникає ситуація, коли правова вимога відкритості судових рішень і державних реєстрів фактично вступає у конкуренцію з потребами захисту критичної

інфраструктури, оскільки агрегована інформація про господарську діяльність підприємств може бути використана для підвищення ефективності кіберзагроз або інших форм впливу.

З іншого боку, повне обмеження доступу до такої інформації також є проблемним, оскільки воно може суперечити принципам відкритості діяльності органів публічної влади та ускладнювати громадський контроль, особливо у сферах, де використовуються значні бюджетні кошти (наприклад, у процесах цифровізації державних послуг чи розвитку реєстрів).

Додатково колізійність проявляється у практиці реагування на кібератаки. Під час інцидентів державні органи, як правило, оприлюднюють лише загальну інформацію про факт атаки та її наслідки (наприклад, тимчасову недоступність сервісів), але утримуються від розкриття технічних причин, способів проникнення або виявлених уразливостей. Це пояснюється необхідністю недопущення повторних атак, однак з точки зору принципу відкритості така інформаційна обмеженість може сприйматися як недостатня прозорість. Відсутність законодавчо чітко визначених критеріїв розмежування між «суспільно необхідною відкритістю» та «інформацією, критичною для безпеки систем», призводить до неоднорідної практики: в одних випадках органи влади надмірно обмежують доступ до інформації, посилаючись на безпеку, а в інших – допускають розкриття даних, які потенційно можуть бути використані для кіберзагроз. Це створює правову невизначеність і ускладнює баланс між прозорістю та захистом критичної інфраструктури.

**Висновки**.

Удосконалення правового забезпечення інформаційної безпеки має здійснюватися шляхом гармонізації національного законодавства із європейськими стандартами, розвитку комплексного підходу до захисту інформації, а також посилення відповідальності за правопорушення у сфері кібербезпеки. Важливим напрямом є також підвищення рівня кіберграмотності та правової культури як серед працівників об’єктів критичної інфраструктури, так і серед населення загалом.

**Список використаних джерел:**

1. Державна служба спеціального зв’язку та захисту інформації України. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 24.04.2026).

2. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37% // Ukr-Communications. URL: https://www.ukr-com.net/cert-ua-u-2025-rotsi-opratsiuvala-mayzhe-6000-kiberintsydentiv-kilkist-vorozhykh-atak-zrosla-na-37/ (дата звернення: 24.04.2026).

3. Закон України «Про критичну інфраструктуру». Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1882-20

4. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

5. Закон України «Про інформацію». Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

6. Закон України «Про захист інформації в інформаційно-комунікаційних системах». – Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

7. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across

the Union (NIS Directive). – Official Journal of the European Union, L 194, 19.07.2016, p. 1–30. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148.

8. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

9. Масштабна кібератака на державні реєстри. Чому це сталося та як вберегти інші системи – пояснюють фахівці з кібербезпеки // AIN.UA. 20.12.2024. URL: https://ain.ua/2024/12/20/masstabna-kiberataka-na-derzavni-poiasniuiut-faxivci-z-kiberbezpeki/ (дата звернення: 24.04.2026).

https://doi.org/10.5281/zenodo.20496781

***Руслан ДЕМУРА,***
*аспірант кафедри комп'ютерних систем, мереж і кібербезпеки*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»,*
*ORCID: https://orcid.org/0009-0003-2248-2565*
*e-mail: r.i.demura@csn.khai.edu*

**Науковий керівник**:
***Наталія ФІЛІПЕНКО,***
*докторка юридичних наук, професорка,*
*професорка кафедри права Гуманітарного-правового факультету*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*
*ORCID: http://orcid.org/0000-0001-9469-3650*
*e-mail: n.filipenko@khai.edu*

**Науковий керівник**:
***Вячеслав ХАРЧЕНКО,***
*член-кореспондент НАН України,*
*доктор технічних наук, професор,*
*завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*
*ORCID: https://orcid.org/0000-0001-5352-077X*
*e-mail: v.kharchenko@csn.khai.edu*

## ЦИФРОВІ ДОКАЗИ В КОНТЕКСТІ СУЧАСНОЇ СУДОВОЇ ЕКСПЕРТИЗИ

У науковій роботі проведено комплексний аналіз гносеологічних та процесуальних викликів, пов'язаних із використанням цифрових доказів у сучасній судово-експертній практиці України. Актуальність дослідження зумовлена тотальною цифровізацією суспільних відносин та необхідністю захисту об’єктів критичної інфраструктури, зокрема авіаційної галузі, від гібридних кіберзагроз. Автор наголошує, що на відміну від традиційних речових доказів, цифрові дані є нематеріальними та потребують спеціалізованого програмного інтерпретатора для їх сприйняття судом, що робить експертне знання ключовою ланкою в процесі доказування.

Основна увага приділена подоланню нормативної колізії між формою та змістом у правозастосуванні. Обґрунтовано необхідність розрізнення понять «електронний документ» та «електронний доказ». Спираючись на актуальну практику Верховного Суду 2021–2026 років, доведено, що відсутність кваліфікованого електронного підпису не може бути безумовною підставою для відхилення даних із месенджерів (Viber, Telegram) чи систем Jira та GitLab, якщо можливо встановити їх походження та цілісність. У контексті форензики підкреслено пріоритет функціонального розуміння «оригіналу», де побітова копія (mirror image) визнається ідентичною первинному носію за умови верифікації криптографічними хеш-функціями (SHA-256) згідно зі стандартом ДСТУ ISO/IEC 27037:2017.

Розглянуто проблему «ланцюга володіння» (Chain of Custody), особливо в контексті розслідування авіаційних подій та кіберінцидентів. Автор акцентує на вразливості цифрових слідів до невидимої модифікації та ризику ефекту «чорної скриньки», коли суд некритично делегує епістемологічну функцію алгоритмам. Окремий акцент зроблено на прихованому вимірі метаданих ($MFT, EXIF) та використанні OSINT-джерел як інструментів виявлення фальсифікацій.

Проаналізовано сучасні виклики щодо дотримання балансу між інтересами правосуддя та правом на приватність (ст. 8 ЄКПЛ). На основі прецеденту ЄСПЛ 2025 року у справі *Černý and Others v. the Czech Republic* обґрунтовано необхідність впровадження в Україні процедури фільтрації (sifting procedure) для захисту адвокатської таємниці на цифрових носіях. Крім того, досліджено вплив штучного інтелекту через тріаду: ШІ як актив, засіб захисту та інструмент атаки (зокрема, deepfake), що потребує розробки нових судово-експертних методик.

У висновках запропоновано конкретні кроки de lege ferenda: законодавче закріплення стандартів ISO щодо збирання доказів, ратифікацію Другого додаткового протоколу до Будапештської конвенції для транскордонного доступу до хмарних даних, а також створення спеціалізованого регламенту взаємодії між CERT-UA та органами досудового розслідування. Наголошено на важливості запровадження спеціалізації «IT-форензика» для суддів та експертів як передумови кіберстійкості держави.

**Ключові слова:** цифрові докази, судова експертиза, кібербезпека, критична інфраструктура, метадані, ланцюг володіння, штучний інтелект, deepfake, авіаційна галузь, ЄСПЛ.

## DIGITAL EVIDENCE IN THE CONTEXT OF MODERN FORENSIC SCIENCE

This research paper provides a comprehensive analysis of the epistemological and procedural challenges associated with the use of digital evidence in modern Ukrainian forensic practice. The relevance of the study is driven by the total digitalization of social relations and the urgent need to protect critical infrastructure, particularly in the aviation sector, from hybrid cyber threats. The author emphasizes that, unlike traditional physical evidence, digital data is intangible and requires specialized software interpreters for judicial perception, positioning expert knowledge as a key link in the evidentiary process.

The main focus is placed on overcoming the normative conflict between form and substance in legal application. The necessity of distinguishing between the concepts of an "electronic document" and "electronic evidence" is substantiated. Drawing on the current practice of the Supreme Court for 2021–2026, it is proven that the absence of a qualified electronic signature should not be an absolute ground for rejecting data from messengers (Viber, Telegram) or systems such as Jira and GitLab, provided their origin and integrity can be established. In the context of forensics, the priority of a functional understanding of the "original" is highlighted, where a bit-to-bit copy (mirror image) is recognized as identical to the primary medium, subject to verification by cryptographic hash functions (SHA-256) in accordance with the DSTU ISO/IEC 27037:2017 standard.

The problem of the "Chain of Custody" is examined, especially in the context of aircraft accident investigations and cyber incidents. The author highlights the vulnerability of digital traces to invisible modification and the risk of the "black box" effect, where the court uncritically delegates its epistemological function to algorithms. Special emphasis is placed on the hidden dimension of metadata ($MFT, EXIF) and the use of OSINT sources as tools for detecting falsifications.

Modern challenges regarding the balance between the interests of justice and the right to privacy (Article 8 of the ECHR) are analyzed. Based on the 2025 ECHR precedent in *Černý and Others v. the Czech Republic*, the necessity of implementing a sifting procedure in Ukraine to protect attorney-client privilege on digital media is substantiated. Furthermore, the impact of artificial intelligence is explored through the triad of AI as an asset, a means of defense, and an instrument of attack (specifically deepfakes), necessitating the development of new forensic methodologies.

In the conclusions, specific *de lege ferenda* steps are proposed: the legislative consolidation of ISO standards regarding evidence collection, the ratification of the Second Additional Protocol to the Budapest Convention for cross-border access to cloud data, and the creation of a specialized cooperation regulatory framework between CERT-UA and pre-trial investigation bodies. The importance of introducing an "IT Forensics" specialization for judges and experts is emphasized as a prerequisite for the state's cyber resilience.

**Keywords:** digital evidence, forensic science, cybersecurity, critical infrastructure, metadata, chain of custody, artificial intelligence, deepfake, aviation industry, ECHR.

**Вступ**.

Цифровізація суспільних відносин докорінно змінила не лише способи комунікації та збереження інформації, а й саму архітектуру доказування у судовому процесі. Сьогодні фактичні дані, релевантні для справи, дедалі частіше існують не у формі традиційного письмового чи речового доказу, а у вигляді електронних повідомлень, метаданих, логів серверів, дампів оперативної пам'яті та хмарних архівів. Ця тенденція набуває особливого виміру у сфері функціонування об'єктів критичної інфраструктури, насамперед авіаційної галузі, де навігаційні системи, бортові самописці, системи управління повітряним рухом та телекомунікаційні мережі генерують масиви цифрових даних, які становлять незамінне джерело доказів як у справах про авіаційні події, так і у розслідуваннях кіберінцидентів.

Українське процесуальне законодавство імплементувало цю категорію: Цивільний процесуальний кодекс України (ст. 100) [1], Господарський процесуальний кодекс України (ст. 96) [2] та Кодекс адміністративного судочинства України (ст. 99) [3] прямо визначають електронні докази як інформацію в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи. Зазначені зміни набули чинності у редакції процесуальних кодексів від 15 грудня 2017 року та відтоді поступово наповнюються судовою практикою Верховного Суду.

Утім, на відміну від традиційного документа, цифровий доказ є нематеріальним і ніколи не є «самоочевидним» — його пізнання стикається з гносеологічним бар'єром: суддя не здатний безпосередньо сприймати бінарний код без спеціалізованого програмного інтерпретатора. Саме тому, відповідно до Закону України «Про судову експертизу» [4] та ст. 242 КПК України [5], у значній кількості випадків саме експертне знання забезпечує процесуально належну інтерпретацію цифрових даних, надаючи цифровому сліду процесуального статусу доказу у правовому полі.

Особливої актуальності ця проблематика набуває в контексті кіберзагроз для критичної інфраструктури. Стратегія кібербезпеки України на 2021–2025 роки, затверджена Указом Президента України № 447/2021 [6], прямо акцентує необхідність підвищення рівня знань слідчих та суддів у сфері збирання й дослідження цифрових (електронних) доказів як передумову ефективного розслідування кіберзлочинів проти об'єктів критичної інфраструктури.

З огляду на викладене, **метою роботи** є комплексний аналіз ключових гносеологічних і процесуальних викликів, пов'язаних із використанням цифрових доказів у сучасній судово-експертній практиці, а також визначення перспективних напрямів адаптації українського законодавства до міжнародних стандартів та практики ЄСПЛ.

Сучасна доктрина та практика роботи з цифровими доказами формуються на перетині процесуального права, технічної криміналістики (Digital Forensics) та теорії прав людини [7; 8; 9]. Науковий аналіз дозволяє виокремити п'ять фундаментальних проблем.

***1. Нормативна колізія форми та змісту.***

В українському правозастосуванні триває подолання формалістського змішування понять «електронного документа» та «електронного доказу». Закон України «Про електронні документи та електронний документообіг» [10] встановлює нормативні вимоги до форми електронного документа: відповідно до ст. 6 накладанням електронного підпису завершується створення електронного документа, а згідно зі ст. 7 оригіналом вважається електронний примірник з обов'язковими реквізитами, у тому числі з електронним підписом автора. Однак процесуальне поняття електронного доказу є значно ширшим: воно охоплює вебсайти, текстові та мультимедійні повідомлення, метадані, бази даних та інші дані в електронній формі, які за своєю природою можуть не мати ознак сформованого за правилами діловодства документа.

Верховний Суд у своїй практиці послідовно виходить із допустимості використання неформалізованих цифрових даних як доказів, зокрема листування у месенджерах (Telegram,

Viber), а також інформації з електронних систем (Jira, GitLab) за умови можливості встановлення їх походження та змісту [11; 12]. Зокрема, постановою Касаційного цивільного суду у складі Верховного Суду від 09.01.2026 у справі № 751/4083/24 визнано, що повідомлення, надіслане через месенджер Viber, може оцінюватися судом як належний доказ ознайомлення працівника з наказом про призупинення трудового договору за умови встановлення обставин його направлення та отримання. Відсутність кваліфікованого електронного підпису сама по собі не зумовлює недопустимість такого доказу.

Водночас у кримінальному провадженні цифрові дані не виокремлені у самостійну процесуальну категорію «електронних доказів», а набувають доказового значення через інститути документів (ст. 99 КПК України), речових доказів (ст. 100 КПК України), протоколів слідчих (розшукових) дій та висновку експерта [5]. У зв'язку з цим у судово-експертній практиці дослідження цифрових носіїв і даних здійснюється, зокрема, в межах комп'ютерно-технічних експертиз (на підставі Інструкції про призначення та проведення судових експертиз та експертних досліджень [14], затвердженої наказом Мін'юсту від 08.10.1998 № 53/5), які відіграють ключову роль у встановленні автентичності, цілісності та походження цифрової інформації.

У цифровому середовищі поняття оригіналу потребує функціонального, а не лише матеріального розуміння, оскільки форензично створена побітова (bit-to-bit) копія може вважатися ідентичною щодо інформаційного змісту первинному носію за умови належної верифікації з використанням сучасних криптографічних хеш-функцій (зокрема SHA-256; використання MD5 у сучасній практиці має обмежений характер і потребує обережної оцінки). Стандартна методологія такої верифікації закріплена у прийнятому в Україні ДСТУ ISO/IEC 27037:2017 [15].

***2. Проблема ланцюга володіння (Chain of Custody) та ефект «чорної скриньки».***

Цифрові докази надзвичайно вразливі до невидимої модифікації. Будь-яке незафіксоване втручання — навіть технічно «невинне» увімкнення комп'ютера слідчим без використання апаратного блокіратора запису (Write-blocker) — призводить до зміни системних файлів та неминучої зміни хеш-суми. Згідно зі ст. 87 КПК України [5], недопустимими є докази, отримані внаслідок істотного порушення прав та свобод людини. У цьому контексті неналежне вилучення або документування цифрових даних може поставити під сумнів достовірність, цілісність і, залежно від характеру порушення, допустимість доказу.

Тут правове мислення стикається із загрозою надмірної «технократизації»: суд змушений делегувати епістемологічну функцію експерту, некритично довіряючи алгоритмам. Це зумовлює нагальну необхідність більш широкого впровадження та уніфікованого застосування положень ДСТУ ISO/IEC 27037:2017 [15] щодо документування кожного кроку поводження з доказом. В авіаційній сфері ця проблема має свою специфіку: дані бортових реєстраторів (FDR та CVR) функціонують у спеціальному режимі розслідування авіаційних подій, де питання доступу та використання інформації (у контексті Додатка 13 до Чиказької конвенції 1944 р. [16]) поєднують доказове значення з вимогами безпеки польотів та конфіденційності.

Особливої уваги заслуговує проблема хмарних доказів. Другий додатковий протокол до Будапештської конвенції про кіберзлочинність (CETS № 224) [17], який підписаний Україною та очікує на ратифікацію, передбачає механізми прискореного транскордонного розкриття електронних доказів. Це критично важливо для розслідування кіберінцидентів на об'єктах критичної інфраструктури, дані яких часто зберігаються у хмарних середовищах інших юрисдикцій.

***3. Прихований вимір метаданих та OSINT-джерела.***

Для судового експерта технічна оболонка файлу (метадані EXIF, часові мітки створення та модифікації, геолокація) часто має вищу доказову вагу, ніж його видимий зміст. Саме метадані фіксують контекст походження або вказують на сліди фальсифікації (наприклад, timestomping — навмисну зміну часових міток, яка виявляється експертами через глибокий аналіз системної таблиці файлів, як-от $MFT). Рекомендація Комітету Міністрів

Ради Європи CM/Rec(2019)3 [18] акцентує на ризиках маніпулювання електронними слідами та необхідності їх ретельного документування.

Окремим дискусійним питанням є доказова цінність відкритих даних (OSINT). Матеріали із соціальних мереж, публічних баз та супутникові знімки дедалі частіше використовуються у провадженнях, однак критерії їх допустимості та форензичної верифікації потребують подальшого доктринального осмислення та конкретизації у судовій практиці.

***4. Межі втручання у приватність та захист адвокатської таємниці.***

Експертиза цифрових пристроїв постійно балансує між інтересами правосуддя та гарантіями ст. 8 Конвенції про захист прав людини і основоположних свобод (ЄКПЛ). Рубіжним прецедентом у цій сфері стало рішення Великої палати Європейського суду з прав людини від 18 грудня 2025 року у справі Černý and Others v. the Czech Republic [19].

Під час обшуку правоохоронці вилучили смартфон підозрюваного, здійснили повне криміналістичне копіювання (mirror imaging) пристрою та долучили до справи переписку з п’ятьма адвокатами захисту. ЄСПЛ констатував порушення Конвенції, наголосивши, що захист адвокатської таємниці поширюється не лише на пристрої адвоката, а й на електронну переписку, що зберігається на пристроях клієнта [19]. Зазначене рішення підштовхує держави до запровадження чітких і передбачуваних процедур фільтрації (sifting procedure) привілейованих даних при вилученні та копіюванні цифрових носіїв. Відтак порушення процедурної чистоти при вилученні та копіюванні цифрових носіїв може поставити під сумнів доказову цінність отриманих матеріалів, що кореспондує з підходами, відомими у порівняльному праві як доктрина «плодів отруєного дерева».

***5. Виклики штучного інтелекту та deepfake-доказів.***

Нагальним викликом стає верифікація доказів, згенерованих або модифікованих засобами ШІ. Варто зазначити, що аспект штучного інтелекту в цьому контексті необхідно розглядати системно, враховуючи тріаду взаємозв'язку ШІ та кібербезпеки: ШІ як актив, що захищається; ШІ як засіб підсилення захисту активів; та ШІ як засіб, що підсилює атаку на актив [20]. Технології deepfake, виступаючи саме як інструмент підсилення атаки, здатні продукувати медіафайли з надвисоким ступенем реалізму. Рамкова конвенція Ради Європи про штучний інтелект (ухвалена 17 травня 2024 р., CETS № 225) [21] формує загальний міжнародно-правовий фон щодо прозорості, підзвітності та управління ризиками ШІ-систем. Однак вона не є спеціальним актом і не містить прямих процесуальних правил верифікації deepfake-доказів у суді. На національному рівні питання судово-експертного підтвердження автентичності таких матеріалів залишається нормативно неврегульованим.

Окрім того, Закон України «Про основні засади забезпечення кібербезпеки України» [22] встановлює загальні правові засади захисту об’єктів критичної інформаційної інфраструктури. Водночас чинне законодавство не містить спеціалізованого процесуального механізму, який би комплексно регулював особливості збирання, фіксації та використання цифрових доказів під час розслідування кіберінцидентів на таких об’єктах.

Як свідчить науковий аналіз, це зумовлює наявність доктринальної проблеми, що полягає у відсутності уніфікованого процесуального порядку трансформації технічних матеріалів, отриманих у ході реагування на кіберінциденти (зокрема, первинної фіксації цифрових слідів фахівцями CERT-UA), у процесуально допустимі докази для органів досудового розслідування.

**Висновки**

У сучасній судовій експертизі цифровий доказ постає як фундаментальний виклик традиційній юридичній епістемології. Правосуддя працює не з «чистим фактом», а з його алгоритмічною репрезентацією. Для об’єктів критичної інфраструктури, зокрема авіаційної галузі, ця проблема набуває особливої гостроти через складність систем генерування даних та їх міжнародно-правовий статус.

Головним критерієм надійності цифрового доказу є не формалізована оболонка (КЕП), а математична цілісність (хеш-сума) та бездоганний ланцюг збереження (Chain of Custody). З огляду на це, перспективним напрямом (de lege ferenda) вбачається законодавче закріплення вимог ДСТУ ISO/IEC 27037:2017 [15] як обов’язкового алгоритму дій для органів досудового

розслідування, що слугуватиме мінімальним стандартом належної практики поводження з цифровими доказами.

Рішення ЄСПЛ у справі Černý and Others v. the Czech Republic (2025 р.) формує важливий конвенційний орієнтир щодо захисту привілейованої комунікації в цифровому середовищі. Українське законодавство потребує невідкладного доповнення нормами про обов'язкову процедуру фільтрації привілейованих даних за участі незалежного судді або спеціаліста.

Ефективна протидія кіберзагрозам вимагає системних кроків: (а) ухвалення спеціального процесуального регламенту взаємодії CERT-UA та слідчих органів; (б) ратифікації Другого додаткового протоколу [17] до Будапештської конвенції [23] (CETS № 224) задля оперативного транскордонного доступу до електронних доказів; (в) запровадження спеціалізації «IT-форензика» у системі підготовки експертів та суддів; (г) розробки судово-експертних методик верифікації цифрових доказів з обов'язковим урахуванням тріади ШІ (ШІ як актив, засіб захисту та інструмент атаки) [20]. Виконання цих умов забезпечить належну правову стійкість критичної інфраструктури в умовах сучасних гібридних загроз.

**Список використаних джерел:**


1. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV.
2. Господарський процесуальний кодекс України: Закон України від 06.11.1991 № 1798-XII.
3. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 № 2747-IV.
4. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII.
5. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI.
6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021.
7. Гора І. В. та ін. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: монографія / за заг. ред. В. А. Колесника. Київ: 7БЦ, 2024. 484 с.
8. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. Науковий вісник Ужгородського НУ. Серія: Право. 2024. Вип. 85. Ч. 4. С. 71–75.
9. Рабко Т. Електронні докази. Поняття та загальні вимоги щодо оформлення (ст. 96 ГПК України, ст. 99 КАС України, ст. 100 ЦПК України). Вища школа адвокатури НААУ, 2024.
10. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV.
11. Постанова Верховного Суду у складі Касаційного господарського суду від 19.01.2021 у справі № 922/51/20.
12. Постанова Верховного Суду у складі Касаційного господарського суду від 15.07.2022 у справі № 910/5408/21.
13. Постанова Верховного Суду у складі Касаційного цивільного суду від 09.01.2026 у справі № 751/4083/24. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/133182740 (дата звернення: 15.04.2026).
14. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затверджена наказом Міністерства юстиції України від 08.10.1998 № 53/5.
15. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT).
16. Конвенція про міжнародну цивільну авіацію (Чиказька конвенція) 1944 р. Додаток 13 «Розслідування авіаційних подій і інцидентів».
17. Другий додатковий протокол до Конвенції про кіберзлочинність щодо розширеної співпраці та розкриття електронних доказів (CETS № 224).

18. Recommendation CM/Rec(2019)3 of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, 30.01.2019.

19. Рішення Європейського суду з прав людини у справі Černý and Others v. the Czech Republic від 18.12.2025 (заяви № 37514/20, 37525/20, 37533/20, 37546/20 та 37555/20).

20. Veprytska O., Kharchenko V., Illiashenko O. Cybersecurity and Artificial Intelligence: Triad-Based Analysis and Attacks Review. Cybernetics and Information Technologies. 2025. Vol. 25, No 3. URL: https://cit.iict.bas.bg/CIT-2025/v-25-3/10341-Volume25_Issue_3-10_paper.pdf.

21. Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права (CETS № 225) від 17.05.2024.

22. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII.

23. Конвенція Ради Європи про кіберзлочинність (CETS № 185) від 23.11.2001 (ратифікована Законом України від 07.09.2005 № 2824-IV).

https://doi.org/10.5281/zenodo.20496921

***Єлизавета ДОРОШ,***
*студентка 2 курсу група 726ю,*
*гуманітарного-правового факультету*
*Національного аерокосмічного університету*
*м. Харків, Україна*
*e-mail: y.y.dorosh @student.khai.edu,*

**Науковий керівник**:
***Світлана ГУЦУ,***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: http://orcid.org/0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

# ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ТРАНСФОРМАЦІЮ ТРУДОВИХ ПРАВ У КОНТЕКСТІ ЧЕТВЕРТОГО ПОКОЛІННЯ ПРАВ ЛЮДИНИ

У статті досліджено вплив штучного інтелекту на трансформацію трудових прав у контексті формування четвертого покоління прав людини. Проаналізовано особливості алгоритмічного управління працею, а також ризики порушення принципів недискримінації, приватності та права на працю. Обґрунтовано необхідність закріплення нових цифрових трудових прав, зокрема права на алгоритмічну прозорість, пояснення автоматизованих рішень і людське втручання. Розглянуто міжнародно-правові підходи до регулювання застосування штучного інтелекту у сфері праці. Зроблено висновок про потребу модернізації трудового законодавства з урахуванням викликів цифровізації та пріоритету прав людини.

**Ключові слова.** штучний інтелект, трудові права, четверте покоління прав людини, цифрові права, алгоритмічне управління, захист персональних даних, цифровий контроль працівників.

# THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE TRANSFORMATION OF LABOR RIGHTS IN THE CONTEXT OF THE FOURTH GENERATION OF HUMAN RIGHTS

The article examines the impact of artificial intelligence on the transformation of labor rights within the framework of the emerging fourth generation of human rights. It analyzes the features of algorithmic management in labor relations and identifies risks related to discrimination, privacy violations, and the restriction of the right to work. The study substantiates the need to establish new digital labor rights, including the right to algorithmic transparency, explanation of automated decisions, and human oversight. International legal approaches to AI regulation in employment are also considered. The paper concludes that labor legislation requires modernization to address digital challenges and ensure the primacy of human rights.

**Keywords.** artificial intelligence, labor rights, fourth generation of human rights, digital rights, algorithmic management, personal data protection, employee digital monitoring.

**Вступ**.

Стрімка інтенсифікація розвитку технологій штучного інтелекту зумовлює глибинну трансформацію суспільних відносин, що особливо виразно проявляється у сфері праці. Інтеграція алгоритмічних систем у процеси добору персоналу, оцінювання ефективності працівників, прийняття управлінських рішень щодо умов праці та припинення трудових правовідносин свідчить про поступове формування нової моделі – алгоритмічно опосередкованого управління працею. Водночас чинне трудове законодавство не містить системних правових механізмів, спрямованих на врегулювання взаємодії працівника з такими системами, що зумовлює виникнення ризиків порушення принципу недискримінації, надмірного втручання у приватне життя та фактичного звуження змісту права на працю. У цьому контексті актуалізується необхідність осмислення штучного інтелекту крізь призму еволюції прав людини, зокрема в межах концепції четвертого покоління прав, а також визначення його ролі у формуванні нових правових гарантій у сфері праці [1].

**Ступінь наукової розробленості проблеми**.

Сучасна правова доктрина характеризується активізацією наукового дискурсу щодо цифрових прав людини як складової четвертого покоління прав. Серед українських науковців, які здійснюють дослідження впливу цифровізації та штучного інтелекту на трудові правовідносини, слід відзначити Н.А. Азьмук, О.В. Баранова, С.Ф. Гуцу, А.М. Колота, Є.О. Харитонова, А.Ф. Щербатюк та інших. У їхніх працях закладено теоретико-методологічні основи дослідження трансформації змісту прав людини в умовах цифровізації, зокрема щодо захисту персональних даних, забезпечення алгоритмічної прозорості та етичних засад застосування штучного інтелекту. Так, Гуцу С.Ф. зазначає, що: «Впровадження цифрових технологій і залучення штучного інтелекту в трудові відносини в першу чергу змушує замислитись над проблемою нерівності і дискримінації у сфері праці. Наявність або відсутність доступу до технологій сформує нові форми нерівності як у сполученні «працівник-працівник», так і «працівник-робот (ШІ)» [2].

**Виклад основного матеріалу**.

Концепція поколінь прав людини відображає історичну еволюцію уявлень про зміст, обсяг і механізми забезпечення прав особи. Четверте покоління прав формується під впливом цифровізації суспільства та охоплює права, пов’язані з функціонуванням інформаційно-комунікаційних технологій, зокрема право на цифрову ідентичність, захист персональних даних, інформаційну безпеку та алгоритмічну справедливість. У цьому вимірі штучний інтелект постає не лише як технологічний інструмент, а як системний фактор, що безпосередньо впливає на зміст і способи реалізації прав людини. У сфері трудових правовідносин це проявляється у формуванні нових моделей організації праці, насамперед алгоритмічного управління, за якого значна частина управлінських функцій делегується системам, що не мають правосуб’єктності, проте здійснюють визначальний вплив на реалізацію трудових прав.

Однією з проблем у цьому контексті є забезпечення прозорості алгоритмічних рішень. Працівник, як правило, позбавлений доступу до інформації про логіку функціонування систем штучного інтелекту, що істотно ускладнює реалізацію права на захист та ефективне оскарження рішень роботодавця. Це зумовлює необхідність нормативного закріплення права на алгоритмічну прозорість як самостійної складової трудових прав, що передбачає можливість отримання зрозумілого пояснення критеріїв, які вплинули на прийняття відповідного рішення[3]. Поряд із цим, застосування штучного інтелекту породжує ризики дискримінації, обумовлені використанням упереджених даних або некоректно налаштованих алгоритмів. У зв’язку з цим виникає потреба у формуванні нових правових механізмів

забезпечення рівності у сфері праці, зокрема шляхом запровадження обов'язкових процедур перевірки алгоритмічних систем на предмет недискримінаційності та пропорційності їх рішень. Врегулювання зазначених проблем можливе лише за умови формування комплексного правового механізму, який поєднує матеріально-правові гарантії прав працівника із чіткими процедурними інструментами їх реалізації.

У цьому контексті обґрунтованим є нормативне закріплення права працівника на пояснення рішень, прийнятих із використанням систем штучного інтелекту. Зміст такого права полягає у забезпеченні доступу не до технічної архітектури алгоритму, а до інформації про ключові фактори та критерії, що вплинули на результат[4]. Це створює передумови для ефективної реалізації права на захист та судового оскарження. Водночас необхідним є встановлення обов'язку роботодавця здійснювати попередній і періодичний незалежний аудит алгоритмічних систем з метою виявлення дискримінаційних або непропорційних рішень. Важливим елементом такого підходу має стати законодавче обмеження використання виключно автоматизованих рішень щодо істотних умов трудових правовідносин, що забезпечує збереження вирішальної ролі людини у процесі управління працею.

Окремого значення набуває забезпечення права на приватність працівника в умовах цифрового контролю. Впровадження принципу пропорційності такого контролю передбачає, що застосування засобів моніторингу можливе лише за наявності об'єктивної виробничої необхідності та за умови відсутності менш інвазивних альтернатив. При цьому роботодавець зобов'язаний забезпечити прозорість обробки персональних даних, зокрема шляхом інформування працівника про обсяг, мету та строки їх використання [5]. Доцільним є також встановлення чітких меж здійснення цифрового контролю, включаючи заборону його застосування поза межами робочого часу, що сприятиме дотриманню балансу між професійною діяльністю та особистим життям. З урахуванням зазначеного обґрунтованим є виокремлення нової категорії цифрових трудових прав людини, які охоплюють право на алгоритмічну прозорість, право на людське втручання у процес прийняття рішень, право на захист від цифрової дискримінації та право на професійну адаптацію в умовах автоматизації [6]. Такі права мають розглядатися як невід'ємна складова четвертого покоління прав людини та потребують належного нормативного закріплення.

Міжнародно-правове регулювання застосування штучного інтелекту у сфері праці формується через систему актів універсального та регіонального характеру, які закріплюють підхід до впровадження цифрових технологій. Зокрема, у Рекомендації ЮНЕСКО щодо етики штучного інтелекту 2021 року визначено базові принципи прозорості, підзвітності та недискримінації, що безпосередньо спрямовані на забезпечення прав працівників в умовах алгоритмічного управління [7]. Резолюції Організації Об'єднаних Націй та аналітичні доповіді, присвячені впливу штучного інтелекту на ринок праці, акцентують на необхідності дотримання прав людини у процесі цифровізації зайнятості та попередженні зростання соціальної нерівності [8]. Важливе значення мають акти Міжнародної організації праці, які формують підхід до інтеграції штучного інтелекту у сферу праці на основі принципу «людина під контролем», гарантування гідної праці та недопущення алгоритмічної дискримінації. На регіональному рівні право Європейського Союзу закріплює більш деталізовані механізми: Акт про штучний інтелект встановлює ризик-орієнтоване регулювання та відносить системи, що використовуються у трудових відносинах, до категорії високого ризику, передбачаючи обов'язковість прозорості, оцінки ризиків і людського контролю; Директива щодо платформної праці закріплює право працівника на перегляд автоматизованих рішень та обмежує їх виключне застосування; водночас акти у сфері кібербезпеки забезпечують захист персональних даних працівників. У сукупності зазначені міжнародні акти формують

комплексну нормативну основу, спрямовану на забезпечення балансу між технологічним розвитком і гарантіями трудових прав, що підтверджує становлення нових цифрових трудових прав як складової четвертого покоління прав людини.

**Висновки.** Штучний інтелект виступає одним із ключових чинників трансформації трудових правовідносин та формування четвертого покоління прав людини. Його впровадження створює як нові можливості для підвищення ефективності праці, так і комплексні ризики для реалізації прав працівників. Чинне трудове законодавство не повною мірою відповідає викликам цифрової епохи, що зумовлює необхідність його системної модернізації. Обґрунтовано доцільність формування концепції цифрових трудових прав людини як складової сучасної правової доктрини. Подальший розвиток правового регулювання має базуватися на принципі пріоритету людини у взаємодії з технологіями штучного інтелекту та передбачати впровадження комплексних гарантій, зокрема права на пояснення алгоритмічних рішень, обов'язкового аудиту систем штучного інтелекту, обмеження повністю автоматизованих рішень у трудових правовідносинах і дотримання принципу пропорційності цифрового контролю. Це забезпечить належний баланс між інтересами роботодавця та ефективним захистом прав працівника в умовах цифровізації.

**Список використаних джерел:**


1. Довгаль Б., Михайліна Т. Цифрові права людини четвертого покоління крізь призму трансгуманізму // Підприємництво, господарство і право. 2021. № 1. С. 171-175. URL: https://pgp-journal.kiev.ua/archive/2021/1/31.pdf.
2. Гуцу С.Ф. Упровадження штучного інтелекту в трудові відносини: перспективи правового регулювання // Вісник НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 2 (50) 2021. С. 87-92 URL: https://visnyk-psp.kpi.ua/article/view/242876/316922.
3. Гуцу С. Ф. Павликівський В. І. Алгоритмічне управління працею: інтеграція ШІ у трудове законодавство та практику соціального діалогу // Наукові перспективи: журнал. 2026. Серія Право. № 3(69). С. 909-918. DOI: https://doi.org/10.52058/2708-7530-2026-3(69).
4. Денисенко К.В., Борко І.С., Косов О.М, Проблеми захисту прав людини в умовах цифровізації суспільства // Науковий вісник Ужгородського національного університету. Серія ПРАВО. Випуск 77: частина 1. С. 90-94. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/16-1.pdf.
5. Бутинська Р. Я. Штучний інтелект у сфері праці: проблеми та перспективи правового регулювання/ Р. Я. Бутинська//Аналітичне-порівняльне правознавство/ редкол.: Ю. М. Бисага (голов. ред.), В. В. Заборовський, Д. М. Бєлов, С. Б. Булеца та ін.; ДВНЗ «УжНУ» – Ужгород, 2024. – №2. – С. 301-308. URL http://journal-app.uzhnu.edu.ua/article/view/303268/295356
6. Швець В. В., Пархоменко Н. М. Штучний інтелект у трудових правовідносинах: проблеми правового регулювання // Eastern European Law Journal. 2025. №130. С. 165-173. URL: https://easternlaw.com.ua/wp-content/uploads/2025/01/shvets_parkhomenko_130.pdf
7. UNESCO. Recommendation on the Ethics of Artificial Intelligence: Key Facts [Електронний ресурс]. URL: https://unesco.org.uk/resources/unesco-recommendation-on-the-ethics-of-artificial-intelligence-key-facts.
8. Національний інститут стратегічних досліджень. Основні підсумки тижня високого рівня 80-ї сесії Генеральної Асамблеї ООН [Електронний ресурс]. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/osnovni-pidsumky-tyzhnya-vysokoho-rivnya-80-yi-sesiyi.

https://doi.org/10.5281/zenodo.20496963

***Назарій ЖУРБА,***
*здобувач другого (магістерського) рівня*
*вищої освіти кафедри права*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*e-mail: n.v.zhurba@student.khai.edu*

**Науковий керівник**:
***Віталій ПАВЛИКІВСЬКИЙ,***
*доктор юридичних наук, професор*
*завідувач кафедри права Національного аерокосмічного*
*університету «Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://orcid.org/0000-0002-1190-9303*
*e-mail: v.pavlykivskyi@khai.edu*

## РІШЕННЯ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ЯК ДЖЕРЕЛО КРИМІНАЛЬНОГО ПРАВА УКРАЇНИ: ОБҐРУНТОВАНІСТЬ ЗАСТОСУВАННЯ, ПРИКЛАДИ ТА АКТУАЛЬНА ПРОБЛЕМАТИКА

У роботі досліджено рішення ЄСПЛ як джерело кримінального права України на прикладі правового регулювання довічного позбавлення волі. Окрему увагу приділено співвідношенню міжнародних стандартів, Конституції України, чинного Кримінального кодексу України, зокрема статей 81 і 82, а також практиці Конституційного Суду України 2021–2023 років. Показано, що рішення ЄСПЛ у справах, пов’язаних із довічним позбавленням волі, стали важливим чинником зміни національного законодавства та судової практики, оскільки закріпили вимогу наявності реальної перспективи звільнення для засуджених. У роботі проаналізовано еволюцію українського підходу до довічного позбавлення волі, механізми його заміни або пом’якшення, а також значення каяття, виправлення і перегляду покарання. Окремий порівняльний блок присвячено підходам США та Німеччини до регулювання довічного ув’язнення. Зроблено висновок, що сучасне українське кримінальне право поступово наближається до європейської моделі, у якій довічне позбавлення волі не може бути покаранням без надії на перегляд.

**Ключові слова:** ЄСПЛ, довічне позбавлення волі, Кримінальний кодекс України, стаття 81, стаття 82, Конституційний Суд України, джерела права, право на надію.

## JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS AS A SOURCE OF UKRAINIAN CRIMINAL LAW: JUSTIFICATION OF APPLICATION, EXAMPLES, AND CURRENT ISSUES

This paper examines ECtHR judgments as a source of Ukrainian criminal law, focusing on the legal regulation of life imprisonment. Special attention is given to the relationship between international human rights standards, the Constitution of Ukraine, the current Criminal Code of Ukraine, especially Articles 81 and 82, and the case law of the Constitutional Court of Ukraine in 2021–2023. The study shows that ECtHR judgments in cases concerning life imprisonment became an important factor in reshaping both legislation and judicial practice in Ukraine, as they established the requirement of a realistic prospect of release for life-sentenced prisoners. The paper analyzes the evolution of Ukraine’s approach to life imprisonment, the mechanisms for replacing or reducing such

punishment, and the role of remorse, rehabilitation, and sentence review. A comparative section addresses the approaches of the United States and Germany to life imprisonment regulation. The study concludes that modern Ukrainian criminal law is gradually moving toward the European model, under which life imprisonment cannot be a punishment without hope of review.

**Keywords:** ECtHR, life imprisonment, Criminal Code of Ukraine, Article 81, Article 82, Constitutional Court of Ukraine, sources of law, right to hope.

**Вступ**.

Україна має широку, за структурою, систему джерел кримінального права, яка будується не лише на Кримінальному кодексі, а й а міжнародних договорах і практиці судів, як і на Конституції, що забезпечує реальне застосування норм. Без винятків, в основу системи закладено принцип верховенства права, який чітко закріплено у статті 8 Конституції України, який означає, що закон має не просто існувати формально, а бути справедливим, передбачуваним і таким, що реально захищає людину від свавілля держави. Саме тому в кримінальному праві України не можна обмежуватися лише буквальним текстом кодексу, якщо його застосування суперечить конституційним засадам або стандартам Конвенції [1].

**Викладення основного матеріалу**.

Окреме місце в цій системі посідає практика Європейського суду з прав людини. Україна як сторона Конвенції зобов'язана виконувати рішення ЄСПЛ, а також упроваджувати європейські стандарти в національне законодавство і судочинство. Це означає, що рішення ЄСПЛ не є просто рекомендаціями для українських судів. Вони стають орієнтиром, без урахування якого неможливо правильно тлумачити права людини у сфері кримінальної юстиції. Особливо це помітно у справах, де йдеться про довічне позбавлення волі, адже там Суд аналізує не лише законність покарання, а й наявність у засудженого реальної перспективи звільнення.

Важливим елементом у поданій тематиці постає Закон України "Про виконання рішень та застосування практики Європейського суду з прав людини" що був ухвалений у 2006 році. Хоча Україна ратифікувала Конвенцію ще у 1997 році, проте механізм її практичного застосування ґрунтувався більше на загальних нормах міжнародного права, конституційних положеннях та був фрагментарним. Вже після прийняття цього нормативного акту змінюється дві вагомі речі: рішення ЄСПЛ у справах проти України стали прямо обов'язковими до виконання державою відповідно до статті 46 Конвенції; суди України отримали законодавчу основу для застосування практики ЄСПЛ при розгляді справ. Таким чином почався процес становлення рішень ЄСПЛ як складової частини національного правозастосування, що вже у 2012 році після нової редакції набуло усталеної нормативної основи для застосування в Україні. Остання редакція чинна і сьогодні, проте система реалізації стала більш розгалуженою: виконання рішень забезпечується не лише цим законом, а й іншими підзаконними актами, бюджетними та інституційними механізмами та практикою органів державної влади [2]. Тому, дослідження питання застосування рішень ЄСПЛ як джерела права є важливим не лише для розуміння чинного кримінального законодавства України, а й для оцінки того, як міжнародні стандарти впливають на національне право. Тема дозволяє простежити еволюцію підходу до довічного позбавлення волі, порівняти практику до і після рішень КСУ, а також показати, чому рішення ЄСПЛ сьогодні є необхідним елементом правильного застосування кримінального права України.

Довічне позбавлення волі в Україні є найсуворішим видом основного покарання і може застосовується лише за особливо тяжкі злочини у випадках, прямо передбачених Кримінальним кодексом. Зміст цього кримінального покарання полягає не просто в тривалому

триманні особи в установі виконання покарань, а в максимально тривалому обмеженні свободи, яке за своєю суттю ставить питання про межі гуманності такого виду покарання. Тому, довічне позбавлення волі завжди балансує на межі між інтересом держави до безпеки суспільства та правом людини на повагу до особистої гідності. У чинному Кримінальному кодексі важливе значення мають стаття 64, яка визначає загальні засади довічного позбавлення волі, а також статті 81 і 82, які регулюють механізми умовно-дострокового звільнення та заміни покарання більш м'яким [3]. В період до 2021 року, ці норми фактично не працювали для довічно засуджених у повному обсязі, і це створювало проблему "покарання без перспективи". Проте все ж, довічне позбавлення волі в Україні не скасовує інших інститутів, зокрема помилування Президентом, яке завжди було винятковим, дискретним і залежним від розсуду влади, тому не могло замінити системного механізму перегляду покарання.

У США довічне позбавлення волі має дуже різні моделі в залежності від штату: наявне умовно-дострокове звільнення через тривалий строк, або ж існує "life without parole", тобто фактично без шансу на вихід. Німеччина вважає довічне покарання теж найсуворішим, але його виконання пов'язане з можливістю судового перегляду після мінімального строку відбування, що краще узгоджується з європейським стандартом "права на надію". У практиці ЄСПЛ критично ставиться не до довічного покарання, а до ситуацій, коли для засудженого немає реалістичної процедури перегляду або звільнення [8; 9]. Для України це важливо з двох причин: порівняння показує, що європейська модель не заперечує суворого покарання, але вимагає прозорого механізму оцінки виправлення; досвід США демонструє, що надмірна жорсткість без перегляду часто веде до критики з боку правозахисних стандартів і ставить питання про гуманність системи. Тому проводячи паралелі, можна зрозуміти, що наша "нова модель" рухається у напрямку німецько-європейського підходу, а не американської моделі «ізоляції».

Тема рішень Європейського суду з прав людини, через призму довічного позбавлення волі сьогодні є однією з найчутливіших у кримінальному праві України, тому що вона стосується не тільки покарання за найтяжчі злочини, а й межі втручання держави в людську гідність. В умовах сьогодення цю проблему вже неможливо розглядати лише через норми Кримінального кодексу, адже на неї безпосередньо впливають рішення ЄСПЛ і позиція Конституційного Суду України. Саме тому аналіз довічного позбавлення волі є водночас і дослідженням джерел права, і перевіркою того, наскільки українська правова система відповідає європейським стандартам.

Судова практика ЄСПЛ щодо довічного позбавлення волі в Україні стала вирішальним каталізатором подальших змін. У справі, першій частині за 2015 рік Petukhov v. Ukraine, ЄСПЛ розглядав скаргу заявника, якого було засудженого до довічного позбавлення волі за особливо тяжкі злочини. ЄСПЛ дійшов висновку, що українська система не забезпечувала реального механізму перегляду покарання і не давала засудженому практичної перспективи звільнення, що визнавалось як порушення статті 3 Конвенції, яка забороняє нелюдське або таке, що принижує гідність, поводження [5]. Вже у справі Petukhov v. Ukraine (No. 2), яка розпочалася у 2019 році та отримала своє завершення у 2025 році, ЄСПЛ підтвердив, що проблема має системний характер і потребує не лише індивідуального захисту, а й загальних законодавчих змін [6]. В цей період, для України це означало, що довічне позбавлення волі в його попередньому вигляді не відповідало європейським стандартам, оскільки засуджений не міг розраховувати на зрозумілий та ефективний перегляд свого становища. Практика ЄСПЛ ключовим висвітлює те, що не скасування довічного покарання як такого, а вимога, щоб воно мало можливість бути переглянутим і не перетворювалося на "покарання без надії". Така логіка стала основою для подальшого втручання Конституційного Суду України та змін до

кодексу. Актуальність теми посилилася після того, як Конституційний Суд України у рішенні № 6-р(II)/2021 визнав неконституційними частину першу статті 81 та частину першу статті 82 КК України в тій частині, у якій вони не дозволяли застосовувати ці механізми до осіб, засуджених до довічного позбавлення волі — це саме ті зміни, які вплинули на подальший хід розвитку теми довічного позбавлення волі. Суд фактично наголосив, що цей вид покарання може існувати лише тоді, коли засуджений має реальну законодавчу перспективу звільнення або заміни покарання більш м'яким. Це означає, що покарання не повинно перетворюватися на остаточне виключення людини з правового простору без надії на перегляд її становища [4].

Самі ж рішення КС України у період 2021-23 років фактично змінили ту ж саму логіку підходу до довічного позбавлення волі. От у 2023 році КСУ звернувся до цієї теми, але вже з іншого боку — через права на особисте і сімейне життя засуджених. Це рішення показало, що після 2021 року питання довічного покарання не вичерпалося лише проблемою звільнення. Конституційний Суд підкреслив, що і після засудження особа не втрачає всіх конституційних прав, а держава повинна забезпечити мінімальні стандарти людської гідності, сімейних зв'язків і правового статусу. Таким чином, у 2021 році КСУ відкрив питання перспективи звільнення, а у 2023 році розширив рамку, показавши, що довічне покарання не може зводитися до повної ізоляції людини від правового та соціального життя.

З практичної точки зору це означає, що довічне покарання більше не може сприйматися як остаточне та абсолютно незмінне. Чинна редакція статті 82 КК уже передбачає, що покарання у виді довічного позбавлення волі може бути замінено позбавленням волі на строк від п'ятнадцяти до двадцяти років за умови, що засуджений відбув не менше п'ятнадцяти років. Це дуже важливо, бо саме наявність такого механізму робить покарання сумісним із європейським підходом до "права на надію".

Відповідно, довічне позбавлення волі не може більше сприйматися як абсолютне та незмінне. Сьогодні, чинна редакція статті 82 Кримінального кодексу передбачає, що такий вид покарання може бути замінено позбавленням волі на строк від п'ятнадцяти до двадцяти років. Проте, лише за умови, шо засуджений вже відбув не менше п'ятнадцяти років, і це доволі важливо, адже наявність такого механізму робить покарання сумісним із європейським підходом [3]. Тому, вже сучасна модель більш зорієнтована на оцінку виправлення поведінки, каяття та небезпеки повторного вчинення злочину. Це і є принциповою новелою: найтяжчий злочинець не може бути позбавлений права на переоцінку свого становища, хоч і визнаємо, зо держава також не відмовляється від суворості покарання.

Проєкт нового Кримінального кодексу зберіг довічне позбавлення волі як вид покарання, але подав його у більш системній та сучасній структурі, як довічне ув'язнення. Передбачені вікові цензи та можливість та ресоціалізацію, за відповідних умов, передбачених статтею 3.5.8. [7]. Саме ця "нова модель", спровокована судовими прецедентами, закладена в основу проєкту. Відповідно, ідея повного скасування такої форми покарання як довічне позбавлення волі не є базовою для кодифікації в Україні, проте акцент робиться саме на поєднанні передбаченості, суворості та можливості перегляду. Практично, це означає оцінку поведінки засудженого, ступеня небезпеки суспільству, каяття та його виправлення.

**Висновки**.

В підсумку, головний висновок полягає в тому, що довічне позбавлення волі в Україні більше не розглядається як покарання без правової перспективи після рішення КСУ № 6-р(II)/2021 та подальшого розвитку практики. Держава зобов'язується запроваджувати засудженому можливості до оскарження, відстоювання гідності та можливості на виправлення.[4] Наша модель пройшла шлях від суто карального підходу до більш гуманістичного, і продовжує рух далі, з огляду на новелізацію законодавства та положення

проєкту нового Кримінального кодексу. А з практики, можна зафіксувати, що раніше довічно засуджені фактично залежали лише від помилування, то нині в законі з'явився механізм заміни невідбутої частини покарання та можливість оцінки виправлення особи.

Беззаперечно, не варто применшувати значення практики ЄСПЛ, адже саме рішення у справах, як от Petukhov v. Ukraine та Petukhov v. Ukraine (No. 2) показують, що довічне позбавлення волі без реальної перспективи звільнення суперечить статті 3 Конвенції. І саме це стало не просто міжнародним сигналом, а прямим поштовхом до зміни національного законодавства і конституційного тлумачення [5; 6]. Це вплинуло і на рішення Конституційного Суду України, як каталізатор, та у 2021–2023 роках фактично закріпило нову правову модель, за якої довічне позбавлення волі стало можливим за умови наявності механізму перегляду, коли засуджена особа не втрачає всіх прав після вироку. Це зблизило українське право з європейськими стандартами та підтвердило, що практика ЄСПЛ є реально діючим джерелом правових підходів в Україні.

Навіть порівнюючи ситуацію з іншими країнами, розуміємо, що Україна рухається у напрямку європейської, а не надмірно жорсткої моделі довічного покарання, де досвід Німеччини підтверджує важливість судового перегляду і права на надію. Тому, розвиток українського кримінального законодавства спрямовується не на посилення ізоляції, а на вдосконалення механізмів перевірки виправлення, каяття, реінтеграції та безпечності особи для суспільства. Це, у свою чергу, підтверджує, що ті рішення ЄСПЛ стають не просто порадою необов'язковою до виконання, а каталізатором, який провокує зміни, та у фіналі стає прецедентом, певним юридичним стандартом, який ми і вважаємо за надійне джерело права в Українському законодавстві.

**Список використаних джерел:**


1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР станом на 2026 р. (Дата звернення 24.04.2026)
2. Закон України "Про виконання рішень та застосування практики ЄСПЛ" від 02.12.2012 № 3477-IV станом на 2026 р. (Дата звернення 24.04.2026)
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III : станом на 2026 р. (Дата звернення 24.04.2026)
4. Рішення Конституційного Суду України № 6-р(II)/2021 у справі за конституційними скаргами щодо відповідності Конституції України положень частини першої статті 81, частини першої статті 82 Кримінального кодексу України від 16.09.2021. (Дата звернення 24.04.2026)
5. Petukhov v. Ukraine : judgment of the European Court of Human Rights, application no. 41216/13, 12 March 2019. (Дата звернення 24.04.2026)
6. Petukhov v. Ukraine (No. 2) : judgment of the European Court of Human Rights, application no. 41216/13, 12 March 2019. (Дата звернення 24.04.2026) (Дата звернення 24.04.2026)
7. Проєкт нового Кримінального кодексу України. (Дата звернення 24.04.2026)
8. Life imprisonment and Article 3 of the ECHR. Considerations on compatibility and future development by Juliana Sveinsdottir, 2021. URL: https://www.diva-portal.org/smash/get/diva2:1567228/FULLTEXT01.pdf (Дата звернення 24.04.2026)
9. German and American Prosecutions: An Approach to Statistical Comparison by Floyd Feeney, 1998. URL: https://bjs.ojp.gov/content/pub/pdf/gap.pdf (Дата звернення 24.04.2026)

https://doi.org/10.5281/zenodo.20497037

***Ірина КАЗАНЧУК,***
*кандидат юридичних наук, професор,*
*доцент кафедри адміністративного права та процесу Навчально-наукового інституту № 3 Харківського національного університету внутрішніх справ*
*ORCID: http://orcid.org/0000-0003-4269-2749*

# ПРОБЛЕМНІ АСПЕКТИ ПРАВОВОГО ЗАСТОСУВАННЯ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ В УМОВАХ ВОЄННИХ ДІЙ В УКРАЇНИ

У роботі досліджено сучасний стан нормативно-правового забезпечення застосування безпілотних авіаційних систем (БпАС) у діяльності Національної поліції України. Показано, що до 2022 року використання дронів мало переважно експериментальний характер, проте в умовах воєнного стану вони стали ключовим інструментом превентивної, пошуково-рятувальної, контр-терористичної та документарної діяльності. Виявлено, що чинна правова база є фрагментарною та не забезпечує комплексного регулювання, що створює ризики порушення прав людини та ускладнює процесуальне використання матеріалів, отриманих за допомогою БпАС. Запропоновано напрями вдосконалення законодавства: доповнення Закону України «Про Національну поліцію» окремою статтею про застосування БпАС, внесення змін до Повітряного кодексу України, ухвалення спеціального відомчого порядку застосування дронів поліцією та уточнення положень КУпАП. Реалізація цих заходів сприятиме підвищенню ефективності правоохоронної діяльності та гармонізації авіаційного законодавства України з нормами ЄС.

**Ключові слова**: безпілотні авіаційні системи, Національна поліція України, воєнний стан, нормативно-правове забезпечення, права людини, Повітряний кодекс України, адміністративне провадження, євроінтеграція.

# PROBLEMATIC ASPECTS OF THE LEGAL APPLICATION OF UNMANNED AERIAL SYSTEMS BY THE UNITS OF THE NATIONAL POLICE OF UKRAINE UNDER WARTIME CONDITIONS

This paper examines the current state of the legal framework governing the use of unmanned aerial systems (UAS) by the National Police of Ukraine. It demonstrates that until 2022, drones were employed mainly in an experimental capacity, whereas under martial law they have become a crucial tool for preventive, search-and-rescue, counter-terrorism, and documentation activities. The study reveals that the existing legal framework is fragmented and fails to provide comprehensive regulation, which creates risks of human rights violations and complicates the procedural use of materials obtained through UAS. The paper proposes directions for legislative improvement, including the introduction of a dedicated article in the Law of Ukraine “On the National Police” regulating UAS application, amendments to the Air Code of Ukraine, adoption of a specific ministerial order on police drone operations, and clarification of provisions in the Code of Administrative Offenses. Implementation of these measures will enhance the effectiveness of law enforcement activities and support the harmonization of Ukraine’s aviation legislation with European Union standards.

**Keywords**: unmanned aerial systems (UAS), National Police of Ukraine, martial law, legal framework, human rights, Air Code of Ukraine, administrative proceedings, European integration.

**Вступ**.

Якщо до 2022 року застосування безпілотних авіаційних систем (надалі – БпАС) у роботі Національній поліції України здійснювалось переважно в експериментальному режимі (в основному під час огляду місць ДТП, пошукових операцій), то в умовах військових дії в Україні БпАС стали невід'ємним інструментом превентивної, пошуково-рятувальної, контр-терористичної та документарно-фіксаційної діяльності українських поліцейських. Так, за даними щорічного звіту Національної поліції України за 2025 рік, тільки тактичних розвідувальних дронів виконано понад 1 400 польотів за рік, а від початку повномасштабного вторгнення — понад 9,3 тис. [1]. На сьогодні підрозділи поліції використовують дрони у пошуку зниклих осіб, фіксації наслідків ворожих ракетних та дронових влучань, документуванні воєнних злочинів, протимінній діяльності, виявленні і фіксації екологічних правопорушень, чи під час евакуації населення з прифронтових територій [2]. Наприкінці 2025 року зафіксовано перші спроби використання БпЛА для скоєння тяжких злочинів, що вимагає вдосконалення контролю [1]. Отже, сучасні технології дозволяють значно підвищити ефективність роботи поліцейських в умовах воєнних дій в країні. Втім, відсутність комплексного правового забезпечення застосування БпАС створює серйозні ризики порушення прав людини, зокрема, використання дронів задля спостереження (моніторингу) місцевості і фіксації правопорушень у режимі реального часу (над територією приватних помешкань). Не слід забувати і про те, що недосконалість правової бази ускладнює процесуальне використання матеріалів, отриманих за допомогою БпАС, та, в решті решт, перешкоджає виконанню Україною євроінтеграційних зобов'язань щодо гармонізації авіаційного законодавства з нормами права Європейського Союзу.

Звісно, під час дії воєнного стану зміст повноважень поліції, визначених статтею 23 Закону України «Про Національну поліцію», був значно розширений [3], що, з одного боку, часто призводить до обмежень деяких прав і свобод громадян, а з іншого – поліція стає не лише гарантом підтримання публічної безпеки і порядку в суспільстві, а й активним учасником заходів забезпечення національної безпеки, що зумовлює своєчасне реагування на усі виклики і загрози, пов’язані з війною. А тому проблема створення належної правової бази застосування БпАС в діяльності поліції стає особливо актуальною.

**Викладення основного матеріалу**.

Чинне нормативно-правове забезпечення системи застосування БпАС Національною поліцією України є фрагментарним і включає в себе в основному: конституційні норми, які визначають співвідношення поліцейських повноважень і прав людини; норми Закону України «Про Національну поліцію», які визначають повноваження поліції щодо застосування технічних засобів [3]; норми Закону України «Про захист персональних даних»; Повітряний кодекс України від 19 травня 2011 р. № 3393-VI, який закріплює визначення безпілотного повітряного судна (стаття 1), регламентує використання повітряного простору (стаття 21), вимоги до авіаційного персоналу (стаття 27) та встановлює базис для державної реєстрації [4]; Положення про використання повітряного простору України, затверджене постановою Кабінету Міністрів України від 6 грудня 2017 р. № 954, яке деталізує режими польотів; Наказ МВС України від 18 грудня 2018 р. № 1026 «Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису», який залишається єдиним відомчим актом, що прямо легітимізує застосування БпЛА в Національній поліції [5], тощо. Принципово важливим кроком стало прийняття Закону України «Про внесення змін до деяких законодавчих актів України щодо застосування правоохоронними органами безпілотних повітряних суден та протидії їх незаконному використанню» від 13.07.2023 р. №

3232-IX, яким доповнено перелік повноважень поліції щодо застосування БпАС та протидії їх незаконному використанню [6]. Проте спеціальної глави або розділу про засади застосування БпАС у Законі України «Про Національну поліцію» досі не має, що залишає значну частину питань (висота польоту, тривалість, принципи мінімізації даних, обов'язкові процедури оцінювання впливу) поза прямим законодавчим регулюванням.

Можна констатувати, що враховуючи специфіку повноважень структурних підрозділів Національної поліції, використання в їх діяльності системи БпАС в умовах воєнного стану має певні проблемні аспекти, що включають в себе: правові колізії та прогалини у чинному законодавстві, ризики порушення прав і свобод громадян. Отже, удосконалення законодавчої бази, підвищення професійного рівня працівників, впровадження інноваційних технологій в правоохоронній діяльності – це ті заходи, які у комплексі дозволять діяти поліції не тільки законно, але й професійно і результативно у складні для країни часи.

В результаті чого напрямки вдосконалення нормативно-правового забезпечення системи застосування БпАС Національною поліцією повинні включати комплекс правових, організаційних і технічних заходів, а також внесення конкретних змін до чинного законодавства України, а саме:

*По-перше,* слід доповнити положення Закону України «Про Національну поліцію» окремою статтею за назвою «Підстави та порядок застосування безпілотних авіаційних систем», в якій пропонується: надати поняття «безпілотні авіаційні системи», класифікацію їх видів за рівнем ризику (низький, середній, високий), визначити вичерпний перелік напрямків застосування (превентивна діяльність, пошуково-рятувальні операції, реагування на ДТП, документування правопорушень, контр-терористична діяльність), обов'язковість процедури оцінювання впливу на захист персональних даних (DPIA) та оцінювання впливу на основоположні права (FRIA) для операцій з елементами штучного інтелекту, закріпити щорічні публічні звіти про застосування БпАС, обов’язковість контролю за правомірністю використання дронів та відповідальності осіб.

*По-друге*, внесення змін до Повітряного кодексу України, передбачивши в ньому окремий розділ «Особливості польотів безпілотних повітряних суден правоохоронних органів». Розділ має закріпити: статус поліцейських БпПС як державних повітряних суден відповідно до європейських норм і стандартів; спеціальний дозвільний порядок для державних польотів; реєстр БпПС правоохоронних органів; кваліфікаційні вимоги до дистанційних пілотів-поліцейських; порядок взаємодії та координації дій Національної поліції з Державіаслужбою України, Генеральним штабом Збройних сил України та органами протиповітряної оборони в умовах воєнного стану.

*По-третє,* затвердження спеціального відомчого нормативного документа - наказу МВС України «Про затвердження Порядку застосування безпілотних авіаційних систем Національною поліцією України», який повинен містити, зокрема, такі положення: категорії БпАС поліції, технічні вимоги до обладнання; сертифікацію дистанційних пілотів; підготовка до польоту; виконання польоту; документування результатів; зберігання та використання даних; контроль і аудит; особливості застосування в умовах правового режиму воєнного стану.

*По-четверте*, внесення змін до Кодексу України про адміністративні правопорушення. Так, стаття 251 КУпАП має бути доповнена окремим положенням про те, що матеріали, отримані за допомогою БпАС, при дотриманні встановленого законом порядку прирівнюються до показань атестованих технічних приладів і мають доказову силу в адміністративному провадженні. Крім того, стаття 14-1 КУпАП має бути уточнена щодо можливості автоматичної фіксації правопорушень за допомогою сертифікованих БпАС поліції.

**Висновки**.

Сучасне використання безпілотних авіаційних систем у діяльності Національної поліції України демонструє їхню ефективність у воєнних умовах, проте водночас виявляє значні прогалини у правовому регулюванні, що створює ризики для прав людини та ускладнює процесуальне використання отриманих матеріалів; тому першочерговим завданням є створення цілісної нормативної бази, яка забезпечить баланс між потребами безпеки та дотриманням правових стандартів, а також сприятиме гармонізації українського законодавства з європейськими нормами.

**Список використаних джерел:**


1. Звіт Національної поліції України про результати роботи у 2025 році. URL: https://npu.gov.ua/static-objects/npu/sites/1/zvit-npu-2025.pdf
2. Бандурка О. М., Науменко С. М., Шевченко Т. В. Нормативно-правове регулювання експлуатації безпілотних авіаційних комплексів при виконанні завдань Національної поліції України. *Вісник Кримінологічної асоціації України*. 2024. № 1 (31). С. 336–353. DOI: https://doi.org/10.32631/vca.2024.1.28.
3. Про Національну поліцію : Закон України від 02 липня 2015 р. № 580-VIII. *Офіційний веб-сайт Верховної Ради України* «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/580-19
4. Повітряний кодекс України від 19.05.2011 № 3393-VI. *Відомості Верховної Ради України*. 2011. № 48–49. Ст. 536. URL: https://zakon.rada.gov.ua/laws/show/3393-17.
5. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : наказ МВС України від 18.12.2018 № 1026. Зареєстровано в Мінюсті 11.01.2019 за № 28/32999. URL: https://zakon.rada.gov.ua/laws/show/z0028-19.
6. Про внесення змін до деяких законодавчих актів України щодо застосування правоохоронними органами безпілотних повітряних суден та протидії їх незаконному використанню : Закон України від 13.07.2023 № 3232-IX. URL: https://zakon.rada.gov.ua/laws/show/3232-20.

https://doi.org/10.5281/zenodo.20497066

***Наталія КАПУСТНИК,***
*кандидатка юридичних наук,*
*асистентка кафедри права*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID: https://orcid.org/0009-0009-5327-9192*
*e-mail:n.kapustnyk@khai.edu*

# ЦИВІЛЬНО-ПРАВОВІ МЕХАНІЗМИ ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ОБ'ЄКТАМ АВІАЦІЙНОЇ ІНФРАСТРУКТУРИ ВНАСЛІДОК ВОЄННИХ ДІЙ: ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ ТА МІЖНАРОДНИЙ ДОСВІД

У тезах досліджуються проблемні аспекти цивільно-правової відповідальності за пошкодження авіаційної інфраструктури в умовах збройної агресії. Аналізується чинне законодавство України щодо фіксації та оцінки збитків. Особлива увага приділяється міжнародним механізмам репарацій та можливості використання досвіду компенсаційних комісій ООН. Обґрунтовується необхідність створення спеціального правового режиму відшкодування для об'єктів критичної інфраструктури, що враховує складність оцінки упущеної вигоди та непрямих збитків у високотехнологічній авіаційній галузі.

**Ключові слова:** авіаційна інфраструктура, цивільно-правове відшкодування, воєнні дії, критична інфраструктура, збитки, міжнародні стандарти.

# CIVIL LAW MECHANISMS FOR REPARATION OF DAMAGE CAUSED TO AVIATION INFRASTRUCTURE OBJECTS AS A RESULT OF MILITARY ACTIONS: PROBLEMS OF LAW ENFORCEMENT AND INTERNATIONAL EXPERIENCE

The abstract examines the problematic aspects of civil liability for damage to aviation infrastructure in the context of armed aggression. The current legislation of Ukraine regarding the recording and assessment of damages is analyzed. Special attention is paid to international reparation mechanisms and the possibility of using the experience of UN compensation commissions. The necessity of creating a special legal regime of compensation for critical infrastructure objects is substantiated, taking into account the complexity of assessing lost profits and indirect damages in the high-tech aviation industry.

**Keywords:** aviation infrastructure, civil compensation, military actions, critical infrastructure, damages, international standards.

**Вступ**.

Сучасна військова агресія проти України продемонструвала критичну вразливість авіаційного сектору, який є стратегічно важливим елементом національної безпеки та ключовим фактором інтеграції держави у світовий економічний простір. Відповідно до Закону України «Про критичну інфраструктуру» критична інфраструктура визначається як сукупність об’єктів, систем і послуг, що мають важливе значення для національної безпеки, економіки та життєдіяльності населення [4]. Згідно з Порядком віднесення об’єктів до критичної інфраструктури, затвердженим постановою Кабінету Міністрів України № 1109 від 09 жовтня 2020 року, та додатків до нього, послуги з управління повітряним рухом, авіаперевезення (робота авіаційного транспорту), забезпечення роботи аеропортів та допоміжного обладнання, що розташоване в аеропортах віднесені до секторів критичної інфраструктури [2]. Таким чином, об’єкти авіаційної діяльності, віднесені до життєво важливих систем, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Знищення або суттєве пошкодження міжнародних аеропортів (зокрема «Антонов» у Гостомелі, «Херсон», «Харків», «Дніпро»), руйнування злітно-посадкових смуг,

аеронавігаційного обладнання, ангарних комплексів та самих повітряних суден потребує не просто капітального будівництва, а складної процедури ресертифікації всього обладнання згідно з жорсткими регламентами ICAO (International Civil Aviation Organization) та EASA (European Union Aviation Safety Agency). Все це ставить перед правовою системою надскладне завдання: забезпечення справедливого та повного відшкодування завданої шкоди. Застосування традиційних цивільно-правових механізмів в умовах збройного конфлікту стикається з низкою концептуальних та практичних перепон, що потребує глибокого аналізу як національного законодавства, так і міжнародного досвіду.

**Викладення основного матеріалу**.

Для уніфікації процесу юридичної фіксації збитків для подальшого стягнення репарацій Міністерство розвитку громад, територій та інфраструктури України ухвалило Наказ від 24 березня 2023 року № 182, яким затверджено відповідну Методику визначення шкоди та збитків, завданих інфраструктурі транспорту, інфраструктурі електронних комунікаційних мереж та об’єктів поштового зв’язку внаслідок збройної агресії Російської Федерації [3]. Хоча документ охоплює різні види транспорту та зв'язку, авіаційна інфраструктура (аеродроми, аеродромні об'єкти, аеронавігаційне обладнання тощо) посідає в ньому одне з ключових місць через надзвичайно високу вартість активів та складність їх відновлення. Методика встановлює комплексний підхід, який дозволяє рахувати не лише пряму шкоду, але й непрямі втрати підприємств цивільної авіації. Формула оцінки включає три основні компоненти:

- Розмір реальних збитків: вартість повністю знищеного або пошкодженого майна аеропортів та авіакомпаній (вартість руйнувань фізичних об'єктів).

- Упущена вигода: доходи, які аеропорти, авіакомпанії та провайдери аеронавігаційного обслуговування могли б реально отримати за звичайних обставин, якби їхня робота не була паралізована війною та закриттям повітряного простору.

- Потреби у витратах на відновлення: кошти, необхідні для демонтажу зруйнованих конструкцій, розробки нової проектної документації, закупівлі сучасного обладнання та безпосереднього будівництва (відновлення функціональності інфраструктури).

Затвердження вищезазначеного Наказу стало критично важливим кроком у переході до суворої юридичної та економічної площини констатації руйнувань. Без єдиної, визнаної державою Методики, оцінки різних експертів могли б суттєво відрізнятися, що послабило б позиції України у міжнародних трибуналах. Сьогодні цей документ дає змогу операторам аеропортів та державі консолідовано та аргументовано формувати претензії до держави-агресора, створюючи надійне підґрунтя для майбутньої відбудови та модернізації авіаційної галузі за рахунок репарацій. Проте, все це лише фіксація завданої шкоди, основна проблема полягає у механізмах відшкодування.

Авіаційна інфраструктура є складним комплексом, що включає як нерухоме майно (аеродроми, термінали, злітно-посадкові смуги), так і високотехнологічне рухоме майно (радіолокаційні системи, світлосигнальне обладнання, засоби зв'язку). З точки зору цивільного права, шкода, завдана цим об'єктам, включає не лише реальні збитки (вартість знищеного майна та витрати на його відновлення), але й колосальну упущену вигоду (неотримані доходи від аеропортових зборів, наземного обслуговування, оренди площ тощо). Згідно зі статтею 1166 Цивільного кодексу України майнова шкода, завдана неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або юридичної особи, а також шкода, завдана майну, відшкодовується в повному обсязі особою, яка її завдала [8]. Однак, у випадку воєнних дій суб'єктом відповідальності виступає іноземна держава, що докорінно змінює традиційний підхід до відповідальності за завдану шкоду.

Головною проблемою правозастосування на національному рівні є концепція судового імунітету. Відповідно до статті 79 Закону України «Про міжнародне приватне право» пред'явлення позову до іноземної держави та забезпечення позову допускається лише за згодою компетентних органів цієї держави, якщо інше не передбачено міжнародним договором або законом України [5]. Зрозуміло, що Російська Федерація такої згоди не надає. Проте в межах формування нової концепції безпеки спостерігається тенденція до обмеження

«абсолютного» імунітету. Тут доцільно аргументувати, що дії, спрямовані на цілеспрямоване знищення критичної інфраструктури є міжнародними злочинами, що позбавляє агресора права на судовий імунітет. Судова практика України продемонструвала еволюційний підхід до вирішення цієї колізії. Верховний Суд у своїй постанові від 14 квітня 2022 року у справі № 308/9708/19 сформував правову позицію щодо ігнорування судового імунітету Російської Федерації, спираючись на доктрину «деліктного винятку» [1]. Ця доктрина, що є частиною звичаєвого міжнародного права, передбачає, що іноземна держава не користується імунітетом у справах про відшкодування шкоди, завданої смертю, тілесним ушкодженням або пошкодженням майна, якщо така шкода завдана на території держави суду. Незважаючи на це прогресивне рішення, яке дозволяє українським власникам авіаційної інфраструктури отримувати позитивні рішення національних судів проти Російської Федерації, проблема полягає у виконанні таких рішень. Оскільки активи Російської Федерації на території України переважно вже націоналізовані або конфісковані, виконання рішень потребує пошуку майна держави-агресора в іноземних юрисдикціях, де іноземні суди можуть не визнати скасування судового імунітету українськими судами.

З огляду на обмеженість національних інструментів, критичного значення набуває міжнародний досвід. Найбільш показовим є досвід Компенсаційної комісії ООН (UNCC), створеної після вторгнення Іраку в Кувейт (1190-1991 рр.) [7]. Цей квазісудовий орган було створено для забезпечення справедливості та виплати репарацій, тому розглядав претензії щодо відшкодування збитків (включно зі шкодою інфраструктурі) і здійснював виплати зі спеціального фонду, який наповнювався за рахунок відсотків від експорту іракської нафти. Для деталізації процедур Керівна рада UNCC приймала рішення, які встановлювали чіткі критерії для оцінки та задоволення позовів. Комісія розробила сувору систему класифікації претензій, в тому числі для збитків, що були завдані критичній інфраструктурі. Для України критично важливим є запозичення досвіду класифікації категорій претензій, задоволених цією комісією для інфраструктурних об’єктів.

Важливим кроком у забезпеченні міжнародного стандарту відшкодування стало створення Міжнародного реєстру збитків (Register of Damage for Ukraine) у Гаазі. За ініціативи України, Європейського Союзу та ще 42 країн, під егідою Ради Європи в Гаазі було створено Міжнародний реєстр збитків [6]. Це офіційна система збору заяв про матеріальні втрати, завдані війною Російської Федерації проти України, для майбутніх виплат за рахунок заморожених активів агресора. Для власників об'єктів авіаційної інфраструктури це означає необхідність ретельної фіксації збитків: проведення будівельно-технічних, економічних та товарознавчих експертиз, збір супутникових знімків, актів руйнувань, аудиторських звітів щодо упущеної вигоди.

З огляду на викладене, необхідно зазначити, що в умовах війни стандарти фіксування збитків, що згодом можна буде використовувати в якості доказів, вимагають легітимізації новітніх методів:

- використання супутникових знімків високої роздільної здатності як основного доказу руйнувань у зонах, де фізичний доступ експертів обмежений;
- цифрові звіти: визнання актів ДСНС та електронних реєстрів руйнувань належними доказами без додаткової верифікації в окремих випадках;
- комплексна експертиза: поєднання класичної будівельної експертизи з висновками авіаційних фахівців щодо втрати цілісності систем навігації.

Специфіка авіації вимагає залучення міжнародних експертів (наприклад, оцінювачів ICAO) для підтвердження вартості специфічного обладнання, аналогів якому може не бути на внутрішньому ринку.

**Висновки**.

Підсумовуючи, слід зазначити, що забезпечення стійкості авіаційної галузі в умовах збройної агресії потребує комплексної модернізації цивільно-правових механізмів відшкодування шкоди. Чинне законодавство України не повною мірою враховує специфіку завдання збитків об’єктам критичної інфраструктури, зокрема складність оцінки упущеної вигоди та непрямих втрат. Існує необхідність законодавчого закріплення статусу цифрових

доказів, а також адаптації національних підходів до оцінки шкоди з урахуванням міжнародних стандартів і практик. Гармонізація національного законодавства зі стандартами ICAO та EASA сприятиме інтеграції України у міжнародний авіаційний простір та підвищенню рівня безпеки. Особливого значення в цьому напрямі набуває використання міжнародного досвіду, зокрема механізмів компенсаційних комісій та сучасних інструментів фіксації збитків. Водночас фактичне стягнення коштів можливе лише через консолідований Міжнародний компенсаційний механізм, який має включати Комісію з розгляду заяв та Компенсаційний фонд, наповнення якого повинно здійснюватися за рахунок суверенних активів центробанку Російської Федерації, заморожених у країнах-партнерах.

**Список використаних джерел:**


1. Постанова Верховного Суду від 14 квітня 2022 року у справі № 308/9708/19. URL: https://reyestr.court.gov.ua/Review/104086064 (дата звернення: 15.04.2026).
2. Постанова Кабінету Міністрів України від 09 жовтня 2020 року № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020 (дата звернення: 13.04.2026).
3. Про затвердження Методики визначення розміру шкоди та збитків, завданих інфраструктурі транспорту, інфраструктурі електронних комунікаційних мереж та об'єктів поштового зв'язку внаслідок збройної агресії Російської Федерації: Наказ Міністерства розвитку громад, територій та інфраструктури України від 24.03.2023 р. № 182. URL: https://zakon.rada.gov.ua/laws/show/z0733-23 (дата звернення: 13.04.2026).
4. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 13.04.2026).
5. Про міжнародне приватне право: Закон України від 23.06.2005 р. № 2709-IV. URL: https://zakon.rada.gov.ua/laws/show/2709-15 (дата звернення: 15.04.2026).
6. Резолюція CM/Res(2023)3 про встановлення Розширеної часткової угоди про Реєстр збитків, завданих агресією Російської Федерації проти України від 12 травня 2023 року, URL: https://zakon.rada.gov.ua/laws/show/961_001-23 (дата звернення: 15.04.2026).
7. Резолюція Ради Безпеки ООН № 692 від 20 травня 1991 року. URL: https://digitallibrary.un.org/record/113598?v=pdf (дата звернення: 15.04.2026).
8. Цивільний кодекс України від 16.01.2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 13.04.2026).

https://doi.org/10.5281/zenodo.20497120

***Руслана КІЦЕНКО,***
*здобувачка фахової передвищої освіти*
*4 курс, Одеський фаховий коледж економіки, права*
*та готельно-ресторанного бізнесу, м. Одеса, Україна*
*ORCID: https://orcid.org/0009-0005-9828-1676*
*e-mail: unicorncapri2@ukr.net*

**Науковий керівник**:
***Марина ПАТРІЛЕВИЧ,***
*спеціаліст вищої категорії, викладач правознавчих дисциплін,*
*голова циклової комісії правознавчих та соціально-економічних дисциплін*
*Одеського фахового коледжу економіки, права та готельно-ресторанного бізнесу,*
*м. Одеса, Україна*

# ВИКОНАВЧЕ ПРОВАДЖЕННЯ В УМОВАХ ЦИФРОВИХ РИЗИКІВ: ЗАХИСТ ДАНИХ ТА АВТОМАТИЗАЦІЯ ПРОЦЕДУР

У тезах досліджується виконавче провадження в умовах цифровізації з акцентом на захист персональних даних та автоматизацію процедур. Розглядаються основні цифрові ризики, зокрема кіберзагрози, технічні збої та проблеми синхронізації державних реєстрів, що впливають на ефективність виконання судових рішень. Аналізуються практичні приклади з української правозастосовної практики. Визначено переваги впровадження автоматизованих систем, а також необхідність удосконалення правового регулювання у сфері інформаційної безпеки виконавчого провадження. Обґрунтовується важливість балансу між цифровою ефективністю та захистом прав учасників процесу.

**Ключові слова:** виконавче провадження, цифровізація, кібербезпека, персональні дані, автоматизація, судові рішення, правове регулювання.

# ENFORCEMENT PROCEEDINGS IN CONDITIONS OF DIGITAL RISKS: DATA PROTECTION AND AUTOMATION OF PROCEDURES

The paper examines enforcement proceedings under digital transformation with a focus on data protection and procedural automation. It analyzes key digital risks, including cyber threats, technical failures, and data synchronization issues within state registers that affect the efficiency of court decision enforcement. Practical examples from Ukrainian legal practice are considered. The study highlights the benefits of automated systems while emphasizing the need to improve legal regulation in the field of information security in enforcement proceedings. The importance of balancing digital efficiency and the protection of participants' rights is substantiated.

**Keywords:** enforcement proceedings, digitalization, cybersecurity, personal data protection, automation, court decisions, legal regulation.

**Вступ**.

Сучасний етап розвитку правової системи характеризується стрімкою цифровізацією суспільних відносин, що суттєво впливає на всі стадії судового процесу, включно з

виконавчим провадженням. Перехід до електронного документообігу, використання автоматизованих реєстрів, інтеграція державних баз даних та впровадження цифрових сервісів у сфері примусового виконання судових рішень — все це істотно підвищує ефективність правозастосування, однак одночасно створюються нові ризики, пов'язані з кібербезпекою та захистом персональних даних.

**Викладення основного матеріалу**.

Виконавче провадження як завершальна стадія судового захисту прав і свобод особи має особливе значення, оскільки саме на цьому етапі відбувається фактична реалізація судових рішень. Його ефективність безпосередньо впливає на рівень довіри громадян до судової системи та держави загалом. В умовах цифрової трансформації ця сфера дедалі більше залежить від інформаційних технологій, які забезпечують швидкість, прозорість та доступність виконавчих процедур. Разом із тим активне впровадження автоматизованих систем у діяльність органів виконавчої служби супроводжується низкою цифрових ризиків. Серед них особливе місце займають загрози несанкціонованого доступу до інформаційних систем, витоку персональних даних боржників і стягувачів, кібератаки на державні реєстри, а також технічні збої, які можуть призвести до порушення строків або порядку виконання судових рішень.

Окремої уваги потребує питання правового регулювання захисту даних у виконавчому провадженні. У цьому контексті важливе значення мають як національні нормативно-правові акти, що регулюють діяльність органів державної виконавчої служби та приватних виконавців, так і міжнародні стандарти у сфері захисту персональних даних і кібербезпеки. Водночас цифровізація відкриває значні можливості для оптимізації виконавчого провадження. Автоматизація рутинних процедур, електронний обмін документами між судами, виконавцями та банківськими установами, а також використання аналітичних систем дозволяють суттєво скоротити строки виконання рішень і зменшити людський фактор, що часто є джерелом помилок або зловживань.

Практична реалізація виконавчого провадження в умовах цифровізації в Україні сьогодні значною мірою здійснюється через автоматизовані системи, зокрема Єдиний реєстр боржників, автоматизовану систему виконавчого провадження (АСВП), електронну взаємодію з банками та державними органами. Ці інструменти значно підвищили швидкість виконання судових рішень, однак одночасно виявили низку практичних проблем, пов'язаних із цифровими ризиками.

Закон України «Про виконавче провадження» від 02.06.2016 № 1404-VIII дає таке визначення у ст. 9: Єдиний реєстр боржників - це систематизована база даних про боржників, що є складовою автоматизованої системи виконавчого провадження та ведеться з метою оприлюднення в режимі реального часу інформації про невиконані майнові зобов'язання боржників та запобігання відчуженню боржниками майна [1].

Одним із найпоширеніших прикладів є ситуації з арештом банківських рахунків через автоматизовану систему. У практиці виконавчої служби трапляються випадки, коли арешт накладається на рахунки осіб, які вже погасили заборгованість, але інформація про це не була своєчасно оновлена в системі. Це — проблема несинхронізованості даних між виконавцями, банками та державними реєстрами, що безпосередньо шкодить правильній реалізації прав, інтересів та свобод громадян.

Ще одним актуальним кейсом є використання Єдиного реєстру боржників. Потрапляння до цього реєстру часто автоматично блокує певні фінансові операції та ускладнює доступ до банківських послуг. На практиці трапляються ситуації, коли особу не виключають із реєстру навіть після закінчення виконавчого провадження через технічні або

адміністративні затримки. Це дійсно створює ризики порушення права власності та ділової репутації.

Важливо також звернути увагу на кіберризики. У 2023–2025 роках в Україні фіксувалися випадки кібератак на державні реєстри та інформаційні системи органів влади. Наймасштабнішою з них була кібератака, що відбулася 19 грудня 2024, внаслідок якої близько 60 різних реєстрів виявились недоступними. Було тимчасово призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції України. Атаки зазнали також Автоматизовна система виконавчого провадження, Єдиний реєстр боржників та Єдиний реєстр приватних виконавців України [3].

У контексті виконавчого провадження це може призвести до тимчасової втрати доступу до матеріалів справ, спотворення даних або затримки виконання судових рішень. Наприклад, у разі технічного збою АСВП виконавець фактично позбавлений можливості оперативно накладати арешти чи знімати обмеження.

Окремо слід розглянути проблему захисту персональних даних. Виконавче провадження передбачає обробку великого обсягу чутливої інформації: фінансовий стан боржників, банківські рахунки, місце роботи, майнові активи. У разі недостатнього рівня захисту інформаційних систем існує ризик витоку даних, що може бути використано третіми особами для шахрайства або тиску на учасників провадження.

Водночас цифровізація демонструє і позитивні практичні результати. Наприклад, автоматичне списання коштів із рахунків боржників через банківські системи значно скоротило строки виконання рішень порівняно з традиційною паперовою процедурою. Також електронний обмін даними між судами та виконавцями дозволяє уникнути затримок, пов’язаних із поштовою доставкою документів.

Ще одним позитивним кейсом є впровадження автоматичного розподілу виконавчих проваджень між державними виконавцями, що зменшує ризик корупційних зловживань та забезпечує більш рівномірне навантаження. Однак навіть ця система залежить від стабільності програмного забезпечення та якості захисту серверів.

Отже, до позитивних результатів цифровізації у даній сфері можна віднести:

- пришвидшення виконання судових рішень за рахунок автоматизованих процедур;
- зменшення впливу людського фактора та ризику корупційних зловживань;
- підвищення прозорості виконавчого провадження через електронні реєстри;
- спрощення обміну інформацією між судами, виконавцями та банками;
- покращення доступу сторін до інформації про стан виконавчого провадження.

Однією з найперспективніших можливостей є використання алгоритмів ШІ для обробки великої кількості виконавчих справ і виявлення закономірностей у поведінці боржників. Такі алгоритми здатні аналізувати історію виконання рішень, фінансовий стан боржників, їхню судову історію, активність у державних реєстрах і на основі цього формувати рейтинги ризиків невиконання. Це дозволяє виконавцям оперативно приймати рішення щодо пріоритетності справ, визначати найбільш ефективні шляхи впливу на боржника та знижувати навантаження на людський ресурс [2, с. 188].

Проведене дослідження виконавчого провадження в умовах цифрових ризиків дозволяє зробити висновок, що сучасна система примусового виконання судових рішень перебуває на етапі активної трансформації під впливом інформаційних технологій. Цифровізація суттєво підвищує ефективність виконавчих процедур, забезпечує їх оперативність, прозорість та зменшує вплив людського фактора, що традиційно був джерелом затримок і зловживань.

Водночас впровадження автоматизованих систем, електронних реєстрів та міжвідомчого обміну даними формує нові виклики, пов’язані з кібербезпекою та захистом персональної інформації. Разом із тим цифрові інструменти демонструють високий потенціал для вдосконалення системи виконання рішень. Автоматизація процесів, електронна взаємодія між органами влади та банківськими установами, а також використання єдиних реєстрів дозволяють значно скоротити строки виконання судових рішень і підвищити ефективність правозастосування.

**Висновки**.

Отже, можна дійти висновку, що подальший розвиток виконавчого провадження має базуватися на балансі між цифровою ефективністю та належним рівнем інформаційної безпеки. Необхідним є удосконалення нормативно-правового регулювання, впровадження сучасних стандартів кіберзахисту та підвищення надійності автоматизованих систем. Цифровізація виконавчого провадження зможе повною мірою забезпечити захист прав громадян і ефективність виконання судових рішень внаслідок ліквідування її недоліків.

**Список використаних джерел:**

1. Про виконавче провадження : Закон України від 02.06.2016 № 1404-VIII : станом на 11 берез. 2026 р. URL: https://surl.li/ligjpi (дата звернення: 09.04.2026).
2. Сокол М. Цифровізація виконавчого провадження: перспективи впровадження інтелектуальних технологій у сфері публічного управління. Право та державне управління. 2021. № 4. С. 185–190. URL: https://surl.li/kzollh (дата звернення: 09.04.2026).
3. Увага! Масштабна кібератака на державні реєстри! - Асоціація приватних виконавців України. Асоціація приватних виконавців України. URL: https://surl.li/lfjxti (дата звернення: 09.04.2026).

https://doi.org/10.5281/zenodo.20497143

***Віталій КОЛОМІЄЦЬ,***
*здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з права) 2 курсу кафедри права Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків, Україна*
ORCID: https://orcid.org/0009-0006-6539-5105
e-mail: kvk@i.ua

**Науковий керівник**:
***Віталій ПАВЛИКІВСЬКИЙ,***
*доктор юридичних наук, професор завідувач кафедри права Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків, Україна*
ORCID: https://orcid.org/0000-0002-1190-9303
e-mail: v.pavlykivskyi@khai.edu

# ПРОБЛЕМИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ПРОТИДІЇ СЕКСУАЛЬНІЙ ЕКСПЛУАТАЦІЇ ТА СЕКСУАЛЬНОМУ НАСИЛЬСТВУ ЩОДО ДІТЕЙ В УКРАЇНІ

У тезах досліджено сучасний стан кримінально-правової протидії сексуальній експлуатації та сексуальному насильству щодо дітей в Україні в контексті імплементації міжнародних стандартів. Проаналізовано зміни, внесені Законом України № 1256-IX, та визначено їх значення для посилення захисту дітей. Виявлено низку проблем чинного законодавства, зокрема недоліки конструкції окремих кримінально-правових норм і неповноту криміналізації окремих форм експлуатації. Обґрунтовано необхідність розширення складів кримінальних правопорушень, пов'язаних із використанням дітей у створенні матеріалів сексуального характеру, а також удосконалення відповідальності за організацію проституції. Окрему увагу приділено проблемі відсутності криміналізації користування сексуальними послугами дітей віком від 16 до 18 років. Запропоновано напрями вдосконалення законодавства та уніфікації термінології відповідно до міжнародних стандартів.

**Ключові слова:** сексуальна експлуатація дітей; сексуальне насильство; кримінальна відповідальність; дитяча проституція; матеріали сексуального насильства; кримінальне законодавство.

# PROBLEMS AND DIRECTIONS FOR IMPROVING CRIMINAL-LEGAL ACTION TO COMBAT SEXUAL EXPLOITATION AND SEXUAL VIOLENCE AGAINST CHILDREN IN UKRAINE

The theses examine the current state of criminal law counteraction to sexual exploitation and sexual abuse of children in Ukraine in the context of implementing international standards. The amendments introduced by Law of Ukraine No. 1256-IX are analyzed, and their significance for strengthening child protection is determined. A number of shortcomings in the current legislation are

identified, including deficiencies in the structure of certain criminal law provisions and incomplete criminalization of specific forms of exploitation. The necessity of expanding criminal offenses related to the use of children in the production of sexually exploitative materials and improving liability for the organization of prostitution is substantiated. Particular attention is paid to the lack of criminalization of the use of sexual services of children aged 16 to 18. Directions for improving legislation and harmonizing terminology in line with international standards are proposed.

**Keywords:** sexual exploitation of children; sexual abuse; criminal liability; child prostitution; child sexual abuse material; criminal law.

**Вступ**.

У сучасних умовах глобалізації та стрімкого розвитку інформаційно-телекомунікаційних технологій проблема сексуальної експлуатації та сексуального насильства щодо дітей набуває особливої актуальності. У Стратегії Європейського Союзу щодо більш ефективної боротьби із сексуальним насильством стосовно дітей наголошується, що світ фактично «програє битву» цьому явищу [1]. Вказане обумовлює необхідність постійного вдосконалення національних механізмів протидії, зокрема кримінально-правових.

**Викладення основного матеріалу**.

Україна, як держава-учасниця Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції), ратифікованої у 2012 році, взяла на себе зобов'язання щодо приведення національного законодавства у відповідність до міжнародних стандартів [3]. Водночас у першому звіті Ланцаротського комітету від 4 грудня 2015 року було констатовано наявність суттєвих недоліків у правовому регулюванні зазначеної сфери в Україні.

Важливим кроком на шляху усунення виявлених прогалин стало прийняття Закону України № 1256-IX від 18 лютого 2021 року, яким імплементовано положення Ланцаротської конвенції та внесено комплексні зміни до кримінального та кримінального процесуального законодавства [2].

Зазначеним законом, зокрема, було:

- запроваджено принцип захисту особи у разі невстановлення її віку за наявності підстав вважати її дитиною;
- удосконалено механізми профілактики та захисту дітей, у тому числі через обмеження доступу до роботи з дітьми осіб, засуджених за відповідні злочини;
- передбачено додаткові гарантії захисту прав дитини у кримінальному провадженні;
- розширено коло кримінально караних діянь у сфері сексуальної експлуатації дітей;
- встановлено відповідальність не лише за виготовлення та розповсюдження, але й за споживання матеріалів сексуального характеру за участю дітей.

Особливої уваги заслуговує криміналізація у ст. 301-1 КК України одержання доступу до матеріалів, що містять сексуальне насильство над дітьми, їх придбання та зберігання навіть за відсутності мети збуту. Такий підхід відповідає сучасним міжнародним тенденціям, спрямованим на зменшення попиту як ключового чинника існування відповідного ринку.

Водночас аналіз чинного кримінального законодавства та практики його застосування свідчить про наявність низки суттєвих проблем.

По-перше, спостерігається невідповідність між назвами та змістом окремих кримінально-правових норм. Зокрема, статті 301 та 301-1 КК України формально регламентують обіг порнографічних матеріалів, однак фактично охоплюють також діяння, пов'язані з примушуванням до участі у їх створенні. При цьому об'єктом посягання виступає

не лише суспільна мораль, а й особа дитини, що свідчить про змішаний характер відповідних складів злочинів.

Така конструкція норм суперечить принципам юридичної техніки, ускладнює кваліфікацію кримінальних правопорушень та перешкоджає притягненню винних до відповідальності за сукупністю злочинів. У результаті обмежуються можливості індивідуалізації покарання.

По-друге, чинне законодавство передбачає відповідальність переважно за примушування дитини до участі у створенні відповідної продукції. Водночас поза межами криміналізації залишаються інші поширені способи втягнення, такі як обман, шантаж, використання уразливого стану, матеріальної або іншої залежності, а також довіри чи авторитету. Це не відповідає реальним формам злочинної поведінки та знижує ефективність кримінально-правового впливу.

У зв'язку з цим доцільним є:

- виокремлення в окрему статтю відповідальності за використання дитини у створенні матеріалів сексуального характеру;
- розширення об'єктивної сторони такого складу злочину шляхом включення альтернативних способів вчинення;
- диференціація кримінальної відповідальності залежно від віку потерпілої особи (малолітня чи неповнолітня).

По-третє, проблемним є нормативне регулювання відповідальності за організацію проституції. Зокрема, ч. 1 ст. 302 КК України передбачає відповідальність за створення або утримання місць розпусти без обов'язкової наявності корисливого мотиву, що ставить під сумнів достатній рівень суспільної небезпечності таких діянь [5, с. 17].

Водночас відповідні дії часто перетинаються зі складом сутенерства, передбаченим ст. 303 КК України, що створює ризики неправильної кваліфікації та необґрунтованого пом'якшення кримінальної відповідальності [4, с. 4-5].

У цьому контексті обґрунтованими видаються такі напрями вдосконалення:

- декриміналізація некорисливого звідництва;
- об'єднання норм щодо організації проституції в межах однієї статті;
- чітка диференціація відповідальності залежно від способів вчинення злочину, зокрема із виділенням насильства як кваліфікуючої ознаки.

По-четверте, суттєвою прогалиною є відсутність кримінальної відповідальності за користування сексуальними послугами дітей віком від 16 до 18 років. Незважаючи на те, що саме ця вікова категорія найбільш часто залучається до проституції, відповідні дії залишаються поза межами криміналізації.

Такий стан речей не відповідає міжнародним стандартам, зокрема положенням Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії.

У зв'язку з цим доцільно передбачити в КК України окрему норму, яка встановлюватиме відповідальність за користування дитячою проституцією незалежно від віку дитини (до 18 років). Запровадження такої заборони сприятиме зниженню попиту та, відповідно, скороченню масштабів експлуатації дітей.

Окремим напрямом удосконалення є уніфікація термінології. На міжнародному рівні дедалі частіше піддається критиці використання терміна «дитяча порнографія», оскільки він може створювати хибне уявлення про добровільність участі дитини. Натомість пропонується використовувати термін «матеріали, що містять сексуальне насильство над дітьми», який більш точно відображає сутність відповідних діянь.

Узагальнюючи викладене, слід зазначити, що незважаючи на значний прогрес у гармонізації кримінального законодавства України з міжнародними стандартами, система протидії сексуальній експлуатації та сексуальному насильству щодо дітей потребує подальшого вдосконалення. Основними напрямами такого вдосконалення є:

- усунення суперечностей у конструкції кримінально-правових норм;
- розширення кола криміналізованих форм експлуатації дітей;
- криміналізація попиту на сексуальні послуги дітей;
- оптимізація норм щодо організації проституції;
- уніфікація термінології відповідно до міжнародних стандартів.

**Висновки**.

Реалізація зазначених заходів сприятиме підвищенню ефективності кримінально-правового захисту дітей, забезпеченню їхніх прав та свобод, а також виконанню міжнародних зобов'язань України.

**Список використаних джерел:**

1. EU strategy for a more effective fight against child sexual abuse. Brussels, 24.7.2020 COM(2020) 607 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0607 (дата звернення: 3.04.2026 р.).

2. Закон України «Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції)» № 1256-IX від 18.02.2021 р. URL: https://zakon.rada.gov.ua/laws/show/1256-20#n38 (дата звернення: 3.04.2026 р.).

3. Конвенція Ради Європи «Про захист дітей від сексуальної експлуатації та сексуального насильства» від 25 жовтня 2007 р. м. Ланцароте. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/994_927#Text (дата звернення: 3.04.2026 р.).

4. Плотнікова А. В. Кримінальна відповідальність за організацію заняття проституцією: автореф. дис. ... канд. юрид. наук: спец. 12.00.08 - кримінальне право та кримінологія; кримінально-виконавче право. Національна академія прокуратури України. Київ, 2010. 20 с.

5. Розслідування торгівлі дітьми: навч.-практ. посіб. Київ, 2011. 240 с.

https://doi.org/10.5281/zenodo.20497325

***Дмитро КОНДРАТОВ,***
*кандидат юридичних наук, доцент,*
*помічник проректора з науково-педагогічної*
*роботи та міжнародних зв'язків*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID: https://orcid.org/0000-0001-5426-4878*
*e-mail: d.kondratov@khai.edu*

***Костянтин ШЕВЕЛЕВ,***
*кандидат юридичних наук,*
*провідний фахівець відділу внутрішнього аудиту*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID: http://orcid.org/0000-0002-3501-5021*
*e-mail: shevelevk982@gmail.com*

# ДО ПИТАННЯ ДЕРЖАВНОГО КОНТРОЛЮ БЕЗПЕКОВОГО ПРОСТОРУ ЗАКЛАДІВ ОСВІТИ

Розглянуто окремі проблемні питання законодавчого регулювання державного контролю в частині приведення приміщень захисних споруд (безпекового простору) закладів освіти, які функціонують в умовах воєнного стану, до умов, що відповідають вимогам чинного законодавства України про освіту, цивільний захист, ліцензування тощо.

Авторами обґрунтовано необхідність модернізації правового базису функціонування безпекового простору закладів освіти. Констатовано, що за відсутності системних вимог до безпеки та ефективного зовнішнього контролю виникає детермінована загроза зниження якості освітніх послуг, а також загроза життю та здоров'ю людей, які можуть перебувати у захисних спорудах закладів освіти. Виявлено пряму кореляцію між рівнем правової регламентації безпекових умов та здатністю системи освіти відповідати стратегічним запитам суспільства й держави.

**Ключові слова:** державне адміністрування, захисні споруди, безпековий простір, цивільний захист, ліцензійні умови, заклади освіти, воєнний стан.

# ON THE ISSUE OF STATE ADMINISTRATION OF THE SECURITY SPACE OF EDUCATIONAL INSTITUTIONS

Some problematic issues of legislative regulation of state control in terms of bringing the premises of protective structures (security space) of educational institutions operating under martial law to conditions that meet the requirements of the current legislation of Ukraine on education, civil defense, licensing, etc. are considered.

The authors substantiate the need to modernize the legal basis for the functioning of the security space of educational institutions. It is stated that in the absence of systemic requirements for security and effective external control, there is a deterministic threat of a decrease in the quality of educational services, as well as a threat to the life and health of people who may be in the protective

structures of educational institutions. A direct correlation between the level of legal regulation of security conditions and the ability of the education system to meet the strategic needs of society and the state is revealed.

**Keywords:** state administration, protective structures, security space, civil defense, licensing conditions, educational institutions, martial law.

**Вступ**.

З лютого 2014 року Україна перебуває в умовах збройної агресії російської федерації, що виступає детермінантою екзистенційних викликів для національної правової системи. Цей стан зумовлює необхідність переосмислення парадигми виконання державою її позитивних зобов'язань щодо забезпечення основоположних прав і свобод людини, зокрема права на життя, особисту недоторканність, власність та освіту [1, с. 96; 2, с. 229].

Як слушно зауважує О. М. Литвинов, в умовах війни, коли значна частина освітнього процесу здійснюється в регіонах із підвищеним рівнем небезпеки, зокрема в Харкові, актуальність проблеми якісного оновлення освітнього середовища набуває особливого значення. На території постійних обстрілів університети стають не лише центрами знань, а й осередками стійкості, які формують довіру суспільства до української освіти, забезпечують відновлення людського капіталу й зміцнюють регіональну ідентичність [3, с. 4].

У контексті системних загроз воєнно-політичного характеру, що посягають на державний суверенітет та територіальну цілісність України, актуалізується питання формування комплексної стратегії захисту національних інтересів, й виключного значення набуває саме конституційно-правовий аспект цієї проблеми. Так, згідно з ч. 1 ст. 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Відповідно до положень ст. 27 Основного закону України, право на життя визнається невід'ємним, а його захист – фундаментальним обов'язком держави [4].

**Викладення основного матеріалу**.

В умовах воєнної агресії цей обов'язок трансформується із площини внутрішньодержавного правопорядку в площину забезпечення виживання нації та збереження інституційної спроможності держави як єдиного гаранта реалізації людських прав. Таким чином, виникає наукова потреба у дослідженні механізмів адаптації державного апарату до нових безпекових реалій при неухильному дотриманні конституційних імперативів. Зокрема, говорячи про традиційний або очний формат освітнього процесу, робота закладів освіти у багатьох випадках є значно обмеженою або ж взагалі стає неможливою, хоча при цьому необхідно швидко реагувати на виклики сьогодення та адаптувати освітній процес під ті умови, в яких ми, на превеликий жаль, зараз перебуваємо.

Такий процес адаптації відбувається, зокрема, й шляхом впровадження освітнього процесу у так званому змішаному форматі, що запроваджується у приміщеннях безпекового простору. Відповідно до положень ст. 32 Кодексу цивільного захисту України до захисних споруд цивільного захисту належать сховища та протирадіаційні укриття, крім того для укриття населення також використовуються споруди подвійного призначення та найпростіші укриття [5].

При цьому, у розумінні постанови Кабінету міністрів України № 1187 від 30.12.2015 року «Про затвердження Ліцензійних умов провадження освітньої діяльності» не передбачено будь яких ліцензійних вимог та відповідних дозвільних документів до безпекового простору, як місця провадження освітньої діяльності – об'єкту (приміщення, будівлі, земельної ділянки та/або території, та/або їх сукупності), що розташовані за певною

(певними) адресою (адресами), у межах якого (якої/яких) провадиться освітня діяльність за відповідним рівнем освіти, відповідно до вимог Закону України «Про освіту» [6; 7].

Ба більше, відсутнє й нормативне врегулювання вимог щодо доступності до навчальних приміщень зазначеного типу для осіб з інвалідністю та інших маломобільних груп населення під час провадження освітньої діяльності, розміщення їх у місці, доступному для візуального сприйняття дорослим, що супроводжує дитину тощо.

Таким чином, відсутність правового врегулювання зазначених питань суперечить концепції інституту якості освіти, адже, відповідно до вимог ч. 6 ст. 25 Закону України «Про освіту», засновник закладу освіти зобов'язаний забезпечити утримання та розвиток матеріально-технічної бази заснованого ним закладу освіти на рівні, достатньому для виконання вимог стандартів освіти та ліцензійних умов [8].

Крім того, як вже наголошувалося нами у попередніх публікаціях, залишається відкритим й питання зовнішнього контролю за дотриманням суб'єктами господарювання ліцензійних умов провадження освітньої діяльності та законодавства у сфері освіти [2, с. 229-231]. Так, відповідно до положень ч. 2 ст. 19 Конституції України: органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [4].

Згідно з приписами ст. 2 Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» функції державного нагляду (контролю) за додержанням законодавства у сфері освіти, ліцензійних умов тощо покладено на центральний орган виконавчої влади із забезпечення якості освіти та його територіальні органи [8].

Поряд із цим, жодним з нормативно-правових актів України не передбачено порядку проведення таких заходів у безпековому просторі закладів освіти. Ба більше, постановою Кабінету міністрів України № 303 від 13.04.2022 року «Про припинення заходів державного нагляду (контролю) в умовах воєнного стану» можливість проведення будь-яких перевірок із вказаних питань фактично виключена [9].

При цьому, як свідчить практика перевірок проведених, зокрема, Державною службою України з надзвичайних ситуацій, вказані приміщення не у повній мірі відповідають вимогам законодавства у сфері техногенної та пожежної безпеки, що створює реальну загрозу життю та здоров'ю людей, які в них можуть перебувати. Принагідно зауважимо, що переважна кількість виявлених порушень під час таких перевірок не є формальними, а стосуються відсутності необхідної системи заходів для запобігання небезпеці та швидкого реагування у разі її виникнення.

**Висновки**.

Таким чином, можна констатувати, що сучасний стан правового регулювання безпекового простору закладів освіти характеризується фрагментарністю та відсутністю цілісної системи забезпечення стандартів освіти. Дефіцит дієвих механізмів зовнішнього контролю та моніторингу дотримання ліцензійних умов створює ризики деградації якісних показників освітнього процесу, а це, у свою чергу, унеможливлює повноцінну реалізацію освітніх стандартів й перешкоджає задоволенню актуальних потреб особистості та суспільства у безпечному середовищі. Тому, на наше переконання, питання правового регулювання виконання вимог стандартів освіти та ліцензійних умов у безпековому просторі закладів освіти потребує суттєвого доопрацювання.

**Список використаних джерел:**


1. Кондратов Д., Шевелев К. І знову до проблеми кримінально-правової охорони особистої таємниці. Пропілеї права та безпеки. 2025. № 8. С. 96–99. DOI: https://doi.org/10.32620/ pls.2025.8.18.

2. Кондратов Д., Шевелев К. Окремі аспекти судової практики з вирішення спорів про обов'язки балансоутримувача приміщень захисних споруд цивільного захисту. Пропілеї права та безпеки. 2025. № 8. С. 229–231. DOI: https://doi.org/10.32620/ pls.2025.8.58.

3. Литвинов О. М. Забезпечення стійкості прифронтового університету: 15 есе про досвід ХАІ. Харків: Право, 2025. 192 с.

4. Конституція України: закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України»/Верховна Рада України. URL: https:// https://zakon.rada.gov.ua/laws/show/%20254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 15.04.2026).

5. Кодекс цивільного захисту України: закон України від 02.10.2012 № 5403-VI // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/5403-17 (дата звернення: 15.04.2026).

6. Про затвердження Ліцензійних умов провадження освітньої діяльності: постанова Кабінету міністрів України від 30.12.2015 № 1187 // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF (дата звернення: 15.04.2026).

7. Про освіту: закон України від 05.09.2017 № 2145-VIII // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2145-19 (дата звернення: 15.04.2026).

8. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: закон України від 05.04.2007 № 877-V // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/877-16 (дата звернення: 15.04.2026).

9. Про припинення заходів державного нагляду (контролю) в умовах воєнного стану: постанова Кабінету міністрів України від 13.03.2022 № 303 // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/303-2022-%D0%BF (дата звернення: 15.04.2026).

https://doi.org/10.5281/zenodo.20497365

***Анастасія МІРОШНІЧЕНКО,***
*Студентка групи 726ю*
*гуманітарного-правового факультету*
*Національного аерокосмічного університету*
*м. Харків, Україна*

**Науковий кервник**:
***Світлана ГУЦУ,***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: https://orcid.org/0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

# ПРАВОВІ ВИКЛИКИ ЗАЛУЧЕННЯ ІНОЗЕМНИХ ФАХІВЦІВ ДО РОБОТИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Стаття присвячена комплексному аналізу правових проблем залучення іноземних фахівців до роботи на об'єктах критичної інфраструктури України в умовах воєнного стану. Досліджено колізії між дерегуляцією ринку праці та вимогами національної безпеки, міграційно-бюрократичну десинхронізацію, ризики спрощеної нострифікації кваліфікацій, а також прогалини у сфері соціально-трудових гарантій. Особливу увагу приділено проблемі трудової дискримінації та забезпеченню принципу рівної оплати за рівну працю. Окремо проаналізовано ризики інформаційної безпеки при допуску іноземців до критичних систем. Запропоновано напрями вдосконалення законодавства та міжвідомчої координації.

**Ключові слова:** критична інфраструктура, іноземні працівники, воєнний стан, національна безпека, міграційна політика, інформаційна безпека, military risk premium.

# LEGAL PROBLEMS OF INVOLVING FOREIGN SPECIALISTS IN WORK AT CRITICAL INFRASTRUCTURE FACILITIES OF UKRAINE UNDER MARTIAL LAW

The article provides a comprehensive analysis of legal issues related to the involvement of foreign specialists in work at critical infrastructure facilities of Ukraine under martial law. It examines conflicts between labor market deregulation and national security requirements, migration-administrative desynchronization, risks of simplified recognition of qualifications, and gaps in social and labor protection. Particular attention is paid to labor discrimination and the principle of equal pay for equal work. The study also highlights information security risks associated with granting foreign personnel access to critical systems. Directions for improving legislation and interagency coordination are proposed.

**Keywords:** critical infrastructure, foreign workers, martial law, national security, migration policy, information security, military risk premium.

**Вступ**.

Збройна агресія Російської Федерації проти України спричинила не лише масштабні гуманітарні втрати, але й системну деструкцію об'єктів критичної інфраструктури (ОКІ), включаючи енергетичні системи, транспортні вузли, промислові підприємства та об'єкти життєзабезпечення населення. Відновлення таких об'єктів в умовах воєнного стану набуває характеру не лише економічного, а й безпекового імперативу, оскільки їх функціонування безпосередньо впливає на обороноздатність держави, стійкість суспільства та виконання базових соціальних функцій держави. У цих умовах особливого значення набуває оперативне залучення висококваліфікованих іноземних фахівців, здатних забезпечити технологічно складні процеси відновлення та модернізації інфраструктури. Така практика відповідає глобальним тенденціям інтернаціоналізації ринку праці та мобільності людського капіталу, що активно досліджуються в межах сучасної науки трудового права та міжнародного економічного права. Зокрема, у документах Міжнародна організація праці підкреслюється необхідність створення гнучких правових механізмів для регулювання транснаціональної зайнятості, особливо в кризових та постконфліктних умовах [1], [2].

Водночас специфіка об'єктів критичної інфраструктури як потенційних цілей військових атак і диверсій зумовлює підвищений рівень правового регулювання доступу до них. Це актуалізує питання співвідношення норм трудового, міграційного та безпекового права, що формує новий комплексний міжгалузевий правовий інститут. Відповідно до положень Організація Об'єднаних Націй щодо захисту критичної інфраструктури в умовах конфліктів, держави повинні забезпечувати баланс між відкритістю економіки та гарантіями національної безпеки, що є складним завданням для правових систем перехідного типу.

**Викладення основного матеріалу**.

Сьогодні в Україні відсутня цілісна доктрина правового регулювання праці іноземців на об'єктах критичної інфраструктури в умовах воєнного стану. Більшість існуючих наукових праць присвячені або загальним питанням трудової міграції, або проблемам національної безпеки, тоді як їх синергетичний перетин залишається недостатньо дослідженим. Це створює прогалину у правовій науці, яка потребує комплексного аналізу з урахуванням сучасних викликів гібридної війни, кіберзагроз та економічної нестабільності.

Окремого значення набуває проблема адаптації національного законодавства України до стандартів Європейського Союзу у контексті євроінтеграційних процесів. У сфері регулювання праці іноземців це передбачає імплементацію принципів недискримінації, рівності умов праці, а також забезпечення належного рівня соціального захисту, включаючи страхування професійних ризиків. Проте в умовах воєнного стану ці стандарти стикаються з об'єктивними обмеженнями, що породжує нові правові колізії та виклики.

По-перше, слід констатувати наявність колізії між політикою дерегуляції доступу іноземців до ринку праці та імперативами національної безпеки. Держава в умовах воєнного стану об'єктивно зацікавлена у максимально швидкому залученні висококваліфікованих іноземних фахівців, що зумовило ухвалення Постанови Кабінету Міністрів України № 437 від 27 травня 2022 року, спрямованої на оптимізацію та прискорення процедур видачі дозволів на застосування праці іноземців [3]. Вказаний нормативний акт передбачає спрощення адміністративних процедур, скорочення строків розгляду документів та зменшення регуляторного навантаження на роботодавців.

Водночас практична реалізація цих положень стикається з необхідністю дотримання вимог безпеки, закріплених у Законі України «Про національну безпеку України» [4] та суміжному законодавстві. Зокрема, допуск іноземних громадян до роботи на об'єктах критичної інфраструктури передбачає проведення поглиблених контррозвідувальних

перевірок, що здійснюються Служба безпеки України. Такі перевірки, з огляду на їх складність і необхідність міжвідомчої взаємодії, потребують значного часу та ресурсів.

У результаті формується ситуація нормативної асиметрії: спрощена de jure процедура доступу до ринку праці фактично нівелюється тривалими безпековими процедурами de facto. Це призводить до затримок у реалізації інфраструктурних проєктів, знижує ефективність антикризового управління та ставить під сумнів досягнення цілей дерегуляційної політики. З наукової точки зору, така колізія свідчить про відсутність належної інституційної координації між органами, відповідальними за економічну політику та безпековий сектор, що потребує впровадження спеціальних правових режимів або процедур прискореного погодження (fast-track) із одночасним дотриманням безпекових стандартів.

Окремого наукового осмислення потребують ризики інформаційної безпеки, що виникають у процесі залучення іноземних фахівців до роботи на об’єктах критичної інфраструктури. Специфіка функціонування ОКІ передбачає доступ до чутливої інформації, включаючи технічну документацію, дані про архітектуру систем управління, мережеву інфраструктуру, алгоритми функціонування автоматизованих систем (зокрема SCADA), а також відомості з обмеженим доступом. У таких умовах навіть ненавмисні дії працівника можуть призвести до витоку інформації або створення вразливостей, що можуть бути використані ворожими суб’єктами в межах гібридної війни. Нормативні засади забезпечення інформаційної безпеки визначені, зокрема, Законом України «Про захист інформації в інформаційно-комунікаційних системах» та Законом України «Про основні засади забезпечення кібербезпеки України», однак їх положення не містять спеціалізованих процедур допуску саме іноземних працівників до критичних цифрових систем. Водночас міжнародні підходи, що розробляються Організація Об'єднаних Націй та Міжнародна організація праці, акцентують увагу на необхідності інтеграції кібербезпеки у політику зайнятості в умовах конфлікту. У цьому контексті актуальним є запровадження багаторівневих механізмів контролю доступу (access control), обов’язкових процедур перевірки благонадійності (background check), а також спеціальних режимів роботи з інформацією (need-to-know principle). Відсутність комплексного правового регулювання у цій сфері створює додаткові загрози національній безпеці та вимагає розроблення міжгалузевого підходу, який би поєднував норми трудового, інформаційного та безпекового права [5].

По-друге, істотною проблемою є міграційно-бюрократична десинхронізація, яка проявляється у відсутності узгодженості між трудовими та міграційними процедурами. Отримання дозволу на застосування праці іноземця, що видається органами служби зайнятості, не створює автоматичних підстав для законного перебування особи на території України. Відповідно до положень Закону України «Про правовий статус іноземців та осіб без громадянства» [6], іноземний фахівець зобов’язаний додатково пройти процедури отримання довгострокової візи типу «D», а також оформлення посвідки на тимчасове проживання. Зазначені процедури перебувають у компетенції різних органів державної влади, зокрема Міністерства економіки України, Державного центру зайнятості, Державної міграційної служби України та Міністерства закордонних справ України. Відсутність єдиного координаційного механізму між цими інституціями призводить до фрагментації адміністративних процесів, дублювання вимог та затягування строків оформлення документів.

У підсумку формується ситуація, за якої іноземний спеціаліст, навіть за наявності дозволу на працю, стикається з тривалими та складними міграційними процедурами, що істотно знижує привабливість України як юрисдикції для висококваліфікованої праці в умовах воєнного стану. Така десинхронізація не лише гальмує процес відновлення об’єктів

критичної інфраструктури, але й свідчить про потребу у впровадженні інтегрованого адміністративного підходу, заснованого на принципі «єдиного вікна» та цифровізації відповідних процедур.

Також суттєвою проблемою є наявність правового вакууму у сфері соціально-трудових гарантій для працівників, залучених до виконання робіт на об'єктах критичної інфраструктури в умовах підвищеного військового ризику, а також відсутність нормативного закріплення механізму так званої «military risk premium» [7]. Чинне міжнародне та національне трудове законодавство, включаючи Закон України «Про зайнятість населення» [8], формувалося переважно в умовах мирного часу і не враховує специфіки праці цивільних осіб у зоні потенційних або реальних бойових дій. Зокрема, на нормативному рівні відсутні:

– чітко визначені механізми обов'язкового страхування життя та здоров'я працівників, які виконують трудові функції в умовах воєнної небезпеки;

– правові підстави для запровадження обов'язкових компенсаційних виплат за підвищений ризик (risk-based compensation);

– стандарти відповідальності роботодавця та держави у разі настання страхових випадків, пов'язаних із воєнними діями.

Міжнародні стандарти, зокрема акти Міжнародна організація праці, декларують принцип забезпечення безпечних і гідних умов праці, однак не містять спеціалізованих механізмів регулювання праці в умовах збройного конфлікту для цивільних працівників. У свою чергу, відсутність уніфікованих підходів до страхування воєнних ризиків ускладнює укладення роботодавцями договорів страхування з міжнародними страховими компаніями, оскільки такі ризики часто виключаються зі стандартних страхових полісів (war exclusions).

Як наслідок, роботодавці фактично позбавлені належних правових інструментів для забезпечення комплексного соціального захисту як іноземних, так і національних працівників, що негативно впливає на рівень правової визначеності та може стримувати залучення висококваліфікованих кадрів [7].

Нарешті, особливої уваги потребує етико-правова колізія, пов'язана з потенційною трудовою дискримінацією у сфері оплати праці та соціальних гарантій. Практика залучення іноземних фахівців до роботи на прифронтових об'єктах критичної інфраструктури, як правило, супроводжується наданням їм значних фінансових стимулів, включаючи підвищену оплату праці, компенсаційні пакети, страхування та гарантії евакуації. Водночас українські працівники, які виконують аналогічні трудові функції в ідентичних або навіть більш небезпечних умовах, нерідко отримують стандартну оплату праці без належних компенсацій за підвищений ризик. Така ситуація фактично формує асиметрію у трудових правах і соціально-економічному становищі працівників залежно від їх громадянства. З юридичної точки зору, подібна практика може містити ознаки непрямої (прихованої) дискримінації, що суперечить:

1. статті 24 Конституції України, яка закріплює принцип рівності громадян перед законом;

2. міжнародним стандартам у сфері праці, зокрема Конвенції №111 Міжнародна організація праці;

3. базовому принципу «рівної оплати за рівну працю».

Крім того, така диспропорція створює ризики демотивації національного кадрового потенціалу, стимулює відтік кваліфікованих працівників та підриває засади соціальної справедливості. В умовах воєнного стану це набуває особливої критичності, оскільки

стабільність функціонування об’єктів критичної інфраструктури значною мірою залежить саме від національних кадрів.

У цьому контексті постає об’єктивна необхідність законодавчого закріплення єдиних стандартів компенсації за роботу в умовах підвищеного ризику (у тому числі «military risk premium»), які мають застосовуватися незалежно від громадянства працівника. Такий підхід дозволить забезпечити дотримання принципу рівності, підвищити рівень соціального захисту працівників та зміцнити кадровий потенціал держави в умовах воєнних викликів.

**Висновки**.

Залучення іноземних фахівців на об'єкти критичної інфраструктури України є життєво необхідним кроком, проте воно не повинно відбуватися ціною послаблення національної безпеки чи знецінення прав національних кадрів. Вбачається за необхідне розроблення єдиного міжвідомчого протоколу (Fast-track) для синхронізації безпекових та міграційних перевірок. Крім того, нагальним є внесення змін до трудового законодавства з метою імплементації єдиного та обов'язкового для всіх механізму страхування воєнних ризиків та нарахування military risk premium. Це забезпечить соціальну справедливість та допоможе зберегти вітчизняний кадровий потенціал.

**Список використаних джерел:**


1. Міжнародна організація праці Employment and decent work in the Humanitarian-Development-Peace Nexus. Geneva: ILO, 2021. 56 p. URL: https://www.ilo.org/publications/employment-and-decent-work-humanitarian-development-peace-nexus
2. Міжнародна організація праці; Організація Об'єднаних Націй Sustaining peace through decent work and employment. Geneva: ILO, 2019. 48 p. URL: https://www.ilo.org/publications/sustaining-peace-through-decent-work-and-employment
3. Деякі питання застосування праці іноземців та осіб без громадянства в Україні і надання послуг з посередництва у працевлаштуванні за кордоном : Постанова Кабінету Міністрів України від 24.01.2023 № 437. URL: https://zakon.rada.gov.ua/laws/show/437-2023-%D0%BF#Text
4. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 01 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. Гуцу С., Правове регулювання інформаційної безпеки в авіаційній сфері: міжнародно-правовий аспект // Міждисциплінарна науково-практична конференція «Сучасні проблеми розвитку авіаційно-космічної галузі України: інженерія, бізнес, право» [Електронний ресурс] : тези доповідей науково-практичної конференції, 5 листопада 2024 року, Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут».– Харків : ХАІ, 2024. – С.93-98.
6. Про правовий статус іноземців та осіб без громадянства : Закон України від 22.09.2011 № 3773-VI : станом на 28 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3773-17#Text
7. Гуцу С.Ф. Соціальний захист: визначення сфери дії та державної політики // «Правові реалії сьогодення»: Матеріали І Всеукраїнської науково практичної конференції (15 травня 2024 р.). Харків: Харківський національний економічний університет ім. С. Кузнеця, 2024. С.83-88.Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
8. Про зайнятість населення : Закон України від 05.07.2012 № 5067-VI : станом на 14 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/5067-17#Text

https://doi.org/10.5281/zenodo.20497862

***Муса НІДЖАТ МАГЕРРАМ ОГЛИ,***
*здобувач вищої освіти третього освітньо-наукового рівня*
*(доктор філософії з права) Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*

**Науковий керівник**:
***Михайло ФІАЛКА,***
*кандидат юридичних наук, професор,*
*професор кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: https://orcid.org/0000-0001-5599-3335*
*e-mail: fialkami70@gmail.com*

# СУБ'ЄКТ НЕЗАКОННОГО ПРИДБАННЯ, ПЕРЕДАЧІ, ЗБУТУ, ЗБЕРІГАННЯ, ПЕРЕВЕЗЕННЯ ТА ТРАНСПОРТУВАННЯ ВОГНЕПАЛЬНОЇ ЗБРОЇ, ЇЇ СКЛАДОВИХ ЧАСТИН, БОЙОВИХ ПРИПАСІВ, ВИБУХОВИХ РЕЧОВИН І ПРИСТРОЇВ (СТ. 228 КК АЗЕРБАЙДЖАНУ): АНАЛІЗ ОБОВ'ЯЗКОВИХ ОЗНАК

Здійснено комплексний аналіз суб'єкта злочину, передбаченого ст. 228 Кримінального кодексу Азербайджану, що регулює відповідальність за незаконний обіг вогнепальної зброї, її складових частин, боєприпасів та вибухових речовин. Досліджено обов'язкові ознаки суб'єкта злочину, зокрема фізичну природу особи, осудність та досягнення встановленого віку кримінальної відповідальності. Окрема увага приділяється доктринальним підходам до розуміння суб'єкта як правової та соціально-психологічної категорії. Обґрунтовано необхідність комплексного підходу до оцінки суб'єкта злочину з урахуванням його соціальних характеристик та мотивації

**Ключові слова:** Кримінальний кодекс Азербайджану, суб'єкт злочину, фізична особа, осудність, вік кримінальної відповідальності, кримінальна відповідальність суб'єкта злочину

# SUBJECT OF ILLEGAL ACQUISITION, TRANSFER, SALE, STORAGE, TRANSPORTATION AND TRANSPORTATION OF FIREARMS, ITS COMPONENTS, ORDERS, EXPLOSIVES AND DEVICES (ART. 228 OF THE CRIMINAL CODE OF AZERBAIJAN): ANALYSIS OF MANDATORY SIGNS

The article carries out a comprehensive analysis of the subject of the crime, provided for in Art. 228 of the Criminal Code of Azerbaijan, which regulates liability for the illegal circulation of firearms, their components, ammunition and explosives. The mandatory features of the subject of the crime are studied, in particular the physical nature of the person, sanity and reaching the established age of criminal responsibility. Special attention is paid to doctrinal approaches to understanding the subject as a legal and socio-psychological category. The need for a comprehensive approach to assessing the subject of the crime, taking into account his social characteristics and motivation, is substantiated.

**Keywords:** Criminal Code of Azerbaijan, subject of crime, individual, sanity, age of criminal responsibility, criminal liability of the perpetrator

**Вступ**.

У сучасну епоху забезпечення громадської безпеки на об’єктах критичної інфраструктури є не лише однією з основних функцій держави, а й виступає одним із показників ефективності правової системи. У цьому контексті незаконний обіг вогнепальної зброї, її компонентів, боєприпасів, вибухових речовин та пристроїв слід оцінювати як складне соціально-правове явище, що становить високу загрозу для суспільства. Актуальність дослідження обумовлена необхідністю вдосконалення кримінально-правового регулювання у сфері незаконного обігу зброї, що становить підвищену загрозу громадській безпеці в умовах збройного конфлікту на об’єктах критичної інфраструктури. Окремим питанням в цьому випадку стоїть позитивний досвід кримінально-правових систем зарубіжних країн.

З цієї причини ст. 228 Кримінального кодексу Азербайджанської Республіки (*далі – КК Азербайджану*) виступає одним із важливих правових механізмів, спрямованих на захист громадської безпеки як взагалі в суспільстві та державі, так і на об’єктах критичної інфраструктури – окремо. Ця норма не лише встановлює заборонені види поведінки, але й визначає рамки відповідальності осіб, які вчиняють ці види поведінки.

При цьому, суб’єкт має особливе значення в структурі складу кримінального правопорушення (злочину). Оскільки без наявності суб’єкта застосування кримінальної відповідальності неможливе. Водночас, характеристики суб’єкта не обмежуються лише формально-правовими критеріями, а й тісно пов'язані з його психічним настроєм, соціальними характеристиками та поведінковою мотивацією. У зв’язку з цим, комплексний аналіз суб’єкта злочину за ст. 228 Азербайджана є актуальним як теоретично, так і практично.

**Викладення основного матеріалу**.

Починаючи аналіз даної проблеми, треба зазначити той факт, що і в теорії, і в кримінально-правовому закріпленні суспільно-небезпечне каране діяння в кримінально-правовій теорії Азербайджану, на відміну від кримінально-правової теорії України, визначається як злочин.

Серед науковців, які систематично працюють над питаннями суб’єкта злочину в теорії кримінального права Азербайджану та цитуються з цієї теми, щонайменше можливо виділити Ф. Й. Самандарова [1], І. Б. Агаєв [2], О. М. Аббасов [3], Р. Рустамова [4].

В КК Азербайджану в положеннях ст. 19 наголошується на тому, що суб’єктом є осудна особа, яка досягла граничного віку, встановленого цим Кодексом, та вчинила злочин, підлягає кримінальній відповідальності [5]. Ця норма систематично визначає основні ознаки суб'єкта кримінального правопорушення (злочину), і до цих ознак належать наступні:

– будучи фізичною особою, юридичні особи не виступають суб'єктами кримінальної відповідальності;

– гранічний вік – мінімальний вік, встановлений Кримінальним кодексом (зазвичай 16 років);

– осудність – усвідомлення особою суспільно небезпечного характеру своїх дій та здатність керувати ними.

Поняття суб'єкта в теорії кримінального права Азербайджану вивчається з різних аспектів протягом тривалого часу. Згідно з класичним підходом, суб’єкт – це фізична особа, яка вчиняє злочинне діяння та несе відповідальність у межах умов, встановлених законом. Як зазначає І. Джафаров, суб’єкт злочину, будучи одним із центральних елементів інституту юридичної відповідальності, діє у взаємодії з іншими складовими злочину та забезпечує їх

реалізацію [6, с. 112]. Такий підхід дозволяє оцінювати суб'єкта не лише як правову категорію, а й як системний елемент.

В азербайджанській кримінально-правовій доктрині ця ознака вважається обов'язковою, оскільки кримінальна відповідальність має індивідуальний характер. Р. Рустамов пояснює це тим, що фізичні особи можуть бути суб'єктом злочину в кожному конкретному випадку… Юридичні особи не можуть вважатися суб'єктом злочину та бути притягнутими до кримінальної відповідальності. Причина полягає у відсутності психічного ставлення до діяння у юридичної особи. Ця ідея підтверджує нормативну логіку: кримінально-правові заходи, що застосовуються до юридичної особи, є окремим інститутом в азербайджанській системі, пов'язаним з діянням, вчиненим фізичною особою, але в класичному розумінні «суб'єкт злочину» все одно залишається фізичною особою [4].

З іншого боку, Р. Гусейнов підходить до поняття суб'єкта з ширшої точки зору та стверджує, що суб'єкт є не лише носієм формальної відповідальності у кримінальному праві, а й носієм психологічних та соціальних основ суспільно небезпечної поведінки [7, с. 87]. Порівняння цих двох підходів показує, що в сучасній азербайджанській кримінально-правовій доктрині поняття суб'єкта все частіше сприймається як складне та багаторівневе явище.

Згідно з КК Азербайджану, суб'єкт злочину, передбачений ст. 228, вважається загальним суб'єктом [5]. Це означає, що для вчинення злочину особі не потрібно мати спеціальний правовий статус. На думку А. Алієва, цей підхід відображає цілеспрямовану політику законодавця, а саме: замість того, щоб обмежувати коло суб'єктів у злочинах, пов'язаних з торгівлею зброєю, їх розширення ефективніше служить забезпеченню громадської безпеки [8, с. 54]. Однак, Ф. Гасімов, критично підходячи до цього питання, зазначає, що застосування моделі загального суб'єкта в деяких випадках послаблює запобігання злочинам, оскільки окрема правова оцінка груп ризику не проводиться [9, с. 33]. Таким чином, порівняння цих двох підходів показує те, що, хоча й забезпечується простота з нормативної точки зору, необхідність диференційованого підходу з кримінологічної точки зору залишається.

Однією з необхідних умов виникнення кримінальної відповідальності є досягнення особою певного віку. Згідно зі ст. 20 КК Азербайджану, загальним правилом є 16 років, а для деяких окремо перелічених злочинів передбачено 14 років [5]. У лекції Р. Рустамова також зазначається те, що кримінальний закон визнає досягнення особою граничного віку, встановленого законом, та її осудність необхідними ознаками суб'єкта злочину. З доктринальної точки зору, цей підхід ґрунтується на тому, що кримінальна відповідальність може бути застосована лише до особи, яка досягла встановленого законом мінімуму соціальної та психологічної зрілості.

Застосування цієї норми показує, що законодавець вимагає певного рівня соціальної та психологічної зрілості для вчинення злочинів, пов'язаних з обігом зброї. Водночас слід зазначити, що деякі автори в сучасній юридичній літературі пропонують переглянути цю вікову межу. На їхню думку, збільшення обігу зброї серед молоді може вимагати посилення правового регулювання в цій сфері. Іншими словами, в азербайджанській кримінально-правовій доктрині питання зниження віку кримінальної відповідальності до 14 років за ст. 228 КК Азербайджану не отримало широкого розвитку як окреме та самостійне дослідницьке питання. Однак, зазначається, що ця проблема обговорюється опосередковано в дослідженнях, проведених з диференціації кримінальної відповідальності неповнолітніх [10].

Ще однією з головних ознак суб'єкта є осудність особи. Вона виражається усвідомленням особою суспільно небезпечного характеру своїх дій та здатністю керувати ними. І. Джафаров пояснює це питання тим, що осудність є необхідною психологічною

умовою для застосування кримінальної відповідальності, а за її відсутності юридична відповідальність виключається [6, с. 198]. Такий підхід показує, що не лише правовий, а й психологічний стан суб'єкта відіграє вирішальну роль у визначенні кримінальної відповідальності.

Враховуючи той факт, що суспільно-небезпечні діяння, які передбачаються ст. 228 КК Азербайджану, в об'єктивній дійсності вчиняються умисно можливо наголошувати на тому, що суб'єкт усвідомлюючи протиправний характер своїх дій і, тим не менш, здійснює ці дії. На думку Р. Гусейнова, для існування умислу важливо, щоб особа усвідомлювала правовий статус суб'єкта [7, с. 142]. На противагу цьому, Ф. Гасімов зазначає те, що незнання у сфері високого ризику, такій як торгівля зброєю, не повинно виключати відповідальність у деяких випадках [9, с. 41]. Порівняння цих двох підходів показує те, що суб'єктивний підхід базується на принципах класичного кримінального права. Але при цьому, завжди треба пам'ятати той факт, що об'єктивний підхід підкреслює пріоритет громадської безпеки. У практиці правоохоронних органів Азербайджану переважно переважає перший підхід, але враховуються також і елементи другого підходу.

Крім того, досліджуючи проблематику суб'єкта передбаченого в ст. 228 КК Азербайджану, завжди треба мати на увазі питання помилки суб'єкта щодо правового статусу об'єкта. В цій ситуації вона оцінюється як фактична помилка. І. Джафаров зазначає те, що в цьому випадку змінюється зміст вини, і це безпосередньо впливає на правову кваліфікацію злочину. В той же час, А. Алієв додає те, що в таких випадках питання пов'язане не лише з існуванням відповідальності, але й з її обсягом та характером. Таким чином, інститут фактичної помилки відіграє важливу роль у диференціації відповідальності суб'єкта.

У сучасних юридичних дослідженнях спостерігається тенденція враховувати не лише юридичні, а й соціальні характеристики суб'єкта. До цих характеристик належать: зв'язок зі злочинним середовищем; рівень участі в торгівлі зброєю; мотивація та мета. За словами Ф. Гасимова, соціальний портрет суб'єкта дозволяє пояснити не лише факт злочину, а й його причини. Цей підхід, на відміну від класичного юридичного аналізу, відображає ширший – кримінологічний підхід.

**Висновки**.

Узагальнивши вищезазначене можливо зробити певний висновок. Проведений широкий аналіз показує, що суб'єкт злочину, передбаченого ст. 228 КК Азербайджану, крім того, що є загальним суб'єктом, має складні юридичні та соціальні характеристики. Хоча правовий статус суб'єкта є простим, його психічне ставлення, фактичні помилки та соціальні характеристики відіграють вирішальну роль у правильній оцінці злочину. Порівняльний аналіз наукових дискусій показує, що сучасна правова доктрина розвивається в напрямку ширшого та складнішого розуміння поняття суб'єкта.

**Список використаних джерел:**

1. Səməndərov F. Y. *Cinayət hüququ: ümumi hissə: dərslik* / Firudin Səməndərov. – Yenidən işlənmiş təkrar nəşr. Bakı: DİGESTA, 2009. 699 s.

2. Ağayev İ. *Cinayət tərkibi: dərs vəsaiti* / İsfəndiyar Ağayev; elmi red. F. Səməndərov. – Bakı: Təhsil, 2005. – 496 s.

3. Abbasov O. M. *Cinayətin subyekti və cinayətkarın şəxsiyyəti anlayışlarının qarşılıqlı müqayisəli təhlili* // *Azərbaycan Respublikasında dövlət və hüquq quruculuğunun aktual problemləri. Elmi məqalələr məcmuəsi*. Bakı, 2007. 17-ci buraxılış. S. 341–346.

4. Rüstəmov R. *Cinayətin subyekti* // Azərbaycan Respublikası Daxili İşlər Nazirliyi Polis Akademiyası, «Cinayət hüququ» fənni üzrə mühazirə mətni. Bakı, 2016. 17 s. URL: https://www.pa.edu.az/library/1/10/19_m._8.pdf (дата звернення: 07.04.2026).

5. Azərbaycan Respublikasının Cinayət Məcəlləsi. – Bakı: Hüquq ədəbiyyatı nəşriyyatı, 2019. 432 s. URL: https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/64893/AZE-64893.pdf (дата звернення: 03.04.2026).

6. Cəfərov İ. Azərbaycan Respublikasının cinayət hüququ : dərslik. – Bakı: Hüquq ədəbiyyatı nəşriyyatı, 2020. 352 s.

7. Hüseynov R. Cinayət hüququ : dərslik. – Bakı: Qanun nəşriyyatı, 2019. – 280 s.

8. Əliyev Ə. İctimai təhlükəsizlik əleyhinə cinayətlər. Bakı: Elm və təhsil, 2021. 198 s.

9. Qasımov F. Silah dövriyyəsi ilə bağlı cinayətlərin hüquqi problemləri // Hüquq jurnalı. 2022. № 2. s. 30–45.

10. Yetkinlik yaşına çatmayanların cinayət məsuliyyəti // Hüquqi maarifləndirmə məqaləsi. 2022. s. 1-5.

https://doi.org/10.5281/zenodo.20497903

***Єлизавета НІКІТІНА,***
*студентка 4-го курсу кафедри права*
*гуманітарно-правового факультету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*e-mail: nikitina2003liza@gmail.com*

Науковий керівник:
***Алла ГОРДЕЮК,***
*кандидат юридичних наук, доцент, професор «ХАІ»*
*доцент кафедри права Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID:* orcid.org/0000-0001-7423-3673
*e-meil:a.hordeiuk@khai.edu*

## ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ЦИФРОВИХ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

У статті розглянуто правове забезпечення кіберзахисту цифрових об'єктів інтелектуальної власності під час збройного конфлікту. Досліджено особливості застосування норм міжнародного гуманітарного права до цифрових об'єктів (програмне забезпечення, бази даних, дані), що мають воєнне значення та пов'язані з функціонуванням критичної інфраструктури. Аналізується історична практика воєнних трофеїв та сучасні виклики їх використання в умовах гібридної війни. Розглянуто застосування норм МГП до кібероперацій, проблеми кваліфікації даних як «майна» та «захищених об'єктів». Висвітлено нормативні прогалини у сфері захисту таких об'єктів у сучасних умовах кібервійни. Обґрунтовано потребу розвитку міжнародно-правових механізмів кіберзахисту.

**Ключові слова:** інтелектуальна власність, міжнародне гуманітарне право, цифрові об'єкти, кібератаки, кіберзахист.

## LEGAL FRAMEWORK FOR THE CYBER PROTECTION OF DIGITAL INTELLECTUAL PROPERTY ASSETS DURING ARMED CONFLICT

This article explores the legal framework for the cyber protection of digital intellectual property during armed conflict. It examines the specifics of applying international humanitarian law to digital objects (software, databases, data) that are of military significance and related to the functioning of critical infrastructure. The article analyzes historical practices regarding war trophies and the contemporary challenges of their use in the context of hybrid warfare. The application of IHL norms to cyber operations is examined, along with the issues of classifying data as "property" and "protected objects." Regulatory gaps in the protection of such objects in the current context of cyberwarfare are highlighted. The need to develop international legal mechanisms for cyber protection is substantiated.

**Keywords:** intellectual property, international humanitarian law, digital assets, cyberattacks, cybersecurity.

**Вступ**.

Історично під час війни переможці в якості трофею забирали з собою зброю, обладунки, матеріальні цінності ворога, які уособлювали перемогу та військову могутність. Сучасні ж способи ведення війни розширили коло таких об'єктів, охопивши програмне забезпечення, бази даних та інші цифрові об'єкти, що мають воєнне значення та залишаються об'єктами інтелектуальної власності, які підпадають під окремий правовий режим. Крім того, такі цифрові об'єкти тісно пов'язані з функціонуванням критичної інфраструктури, зокрема

енергетичних систем, транспортних мереж і комунікаційних платформ, що забезпечують життєдіяльність суспільства. Це актуалізує питання правового становища та кіберзахисту таких об’єктів під час збройного конфлікту.

**Викладення основного матеріалу**.

Якщо розглядати проблему в контексті МГП та звичаєвого права, то відповідно до ст. 53 Гаазьких конвенцій 1907 р., окупаційна армія може заволодіти всією рухомою власністю держави, що може бути використана для військових дій [1]. Тією мірою, якою ці об'єкти можуть бути вилучені, вони фактично є військовими трофеями, навіть якщо технічно їх неможливо захопити або знайти на полі бою.

Відмінність між захопленням військових трофеїв як звичаєм міжнародного права та під час окупації полягає у двох аспектах: по-перше, стаття 53 починає діяти лише в момент встановлення воєнної окупації, тобто «після того, як на території противника закріпився ефективний контроль». По-друге, захоплення під час воєнної окупації можуть включати все майно, «яке може бути використане для військових операцій», що відсутнє у звичайних визначеннях військових трофеїв [2].

Держава не має жодних зобов'язань, звичаєвих чи інших, платити за військову здобич, захоплену на полі бою, а також немає потреби у виплаті компенсації, оскільки передача є автоматичною, держава, що захоплює, може використовувати здобич будь-яким способом, який вона вважає за потрібне. Це включає продаж майна та відчуження коштів на рішення держави, і будь-яка така передача третій стороні гарантується від стягнення [2].

Важливо враховувати те, що військова здобич, коли її захоплення виправдане військовою необхідністю, належить державі, яка її захопила, і не стає власністю приватних осіб чи організацій, якщо окремі солдати захоплюють майно для приватного використання або особистої вигоди, така поведінка забороняється як розграбування (Гаазькі правила 1907 року , ст. 47; ЖК IV 1949 року , ст. 33). Розграбування карається військовим законодавством або загальним кримінальним законодавством у багатьох країнах. Це вважається забороненим згідно зі звичаєвим міжнародним правом та є воєнним злочином згідно зі статтею 8(2)(b)(xvi) Римського статуту Міжнародного кримінального суду [3].

Щодо використання МГП в інформаційно-комунікаційних технологіях (далі – ІКТ) у випадках збройного конфлікту, то в такому середовищі діють основоположні принципи МГП, зокрема принципи гуманності, військової необхідності, розмежування та пропорційності, які визначають допустимі межі застосування кіберзасобів і методів ведення війни. Сторони конфлікту зобов’язані розрізняти військові цілі й цивільні об’єкти, утримуватися від спрямування кібератак проти цивільної інфраструктури, а також оцінювати можливі прямі й непрямі наслідки для цивільного населення та функціонування критично важливих систем.

У контексті ІКТ правове значення мають не лише фізичні пошкодження, а й порушення роботи мереж, втрата функціональності цифрових систем, ураження даних і дестабілізація інфраструктури, що впливають на безпеку цивільного населення. З огляду на це застосування МГП до ІКТ середовища спрямоване на обмеження наслідків кібератак і забезпечення захисту цивільних осіб, цивільних даних та цивільної інфраструктури під час збройного конфлікту [4].

Поява нових засобів і методів ведення війни, зокрема кібероперацій, породжує правову невизначеність щодо самого змісту права, оскільки традиційні норми МГП не адаптовані до цифрового середовища, де бази даних, комп'ютерні програми та дані стають об'єктами захоплення чи атаки. Кібератаки можуть класифікуватися як «атаки» за МГП, якщо вони спричиняють функціональне пошкодження (Правило 49 ICRC), але становище цифрових об'єктів лишається досить неоднозначним, тому постає питання чи є такі об’єкти «майном ворога» для здобичі, чи захищеними цивільними об’єктами?

Програмне забезпечення, бази даних, дані, комерційна таємниця та вихідний код мають нематеріальну природу, що кардинально відрізняє їх від традиційних матеріальних трофеїв минулих війн, таких як зброя, прапори чи військова техніка. Їхнє копіювання можливе без фізичного вилучення чи руйнування оригіналу, оскільки вони існують у цифровій формі та можуть миттєво дублюватися через кібератаки, фішинг чи витоки. Така особливість робить їх ідеальними об’єктами для сучасних гібридних конфліктів, де контроль над інформацією

забезпечує стратегічну перевагу без видимих слідів захоплення, на противагу традиційним матеріальним об'єктам.

Бази даних і комп'ютерні програми охороняються авторським правом на міжнародному, європейському та національному рівнях. Так, ч. 5 ст. 7 Директиви 96/9/ЄС забороняє повторюване й систематичне витягнення або повторне використання незначних частин вмісту бази даних, якщо це суперечить її нормальному використанню або невиправдано шкодить законним інтересам розробника [5]. Відповідно до ч. 1 ст. 20 Закону України «Про авторське право і суміжні права» охорона поширюється на оригінальні комп'ютерні програми, виражені у вихідному чи об'єктному коді, а згідно з ч. 1 ст. 21 цього Закону авторським правом охороняються і бази даних, якщо вони є результатом творчого добору чи упорядкування [6]. Аналогічний підхід закріплено у ст. 10 Угоди TRIPS, яка захищає комп'ютерні програми як літературні твори, а компіляції даних як результати інтелектуальної творчості, тоді як ст. 13 TRIPS допускає лише такі обмеження й винятки, що не суперечать звичайному використанню твору та не завдають надмірної шкоди законним інтересам власника прав [7].

Проте ці всі норми здебільшого діють в мирний час, зокрема ст.73 TRIPS передбачає винятки щодо безпеки і встановлює, що ніщо в Угоді не слід тлумачити як таке, що перешкоджає державі вживати заходів, які вона вважає необхідними для захисту своїх основних інтересів безпеки, зокрема «вжитих під час війни або в умовах інших надзвичайних ситуацій у міжнародних відносинах» [7]. Відповідно виникає питання щодо співвідношення режиму охорони ІВ з нормами МГП щодо майна під час збройного конфлікту.

Відсутність спеціального регулювання цифрових об'єктів у МГП ускладнює розмежування між правомірним захопленням військового майна та незаконним використанням об'єктів ІВ. Захоплення військового майна допускається ст. 53 Гаазької конвенції IV, тоді як копіювання програмного забезпечення, баз даних та інших об'єктів ІВ не має чіткої правової кваліфікації в умовах збройного конфлікту. Така прогалина актуалізує потребу в адаптації МГП та розширення тлумачення для врегулювання ІВ у кібервійні.

Проблема полягає в тому, що після того, як право власності набувається як військова здобич, остаточне розпорядження майном визначається внутрішнім законодавством держави, що його захопила. Наприклад, уряд рф видав урядову постанову № 506 від 29 березня 2022 року, яка дозволила ввозити оригінальні іноземні товари без згоди правовласників і виключила відповідальність за такі дії щодо визначених категорій товарів. Це фактично надало російським підприємствам право використовувати ІВ із «недружніх країн» без компенсації, легітимізувавши такі практики на рівні національного права в умовах міжнародного збройного конфлікту [3].

Це особливо можна спостерігати під час гібридної війни, що значною мірою розгортається у правовій та фактичній «сірій зоні» [8]. Держави будуть активно шукати цю сіру зону, як це робить рф в кіберпросторі. Наприклад, очевидно, що кібероперації, які мають значні фізичні наслідки, кваліфікуються як застосування сили, законодавство не дає чіткої відповіді щодо тих, що не мають таких наслідків. Це робить такі операції привабливими для держави, яка не хоче, щоб її вважали такою, що порушує міжнародне право, або яка бажає викликати розбіжності серед інших держав щодо того, чи зробила вона це [8].

Сучасні кіберможливості мають унікальну цінність для послаблення оборони противника. Вони можуть засліплювати ворожі системи раннього попередження, виводити з ладу оборонні засоби, вводити дезінформацію в системи противника та забезпечувати доступ до його процесу ухвалення рішень і дій завдяки присутності всередині систем противника [8].

Дискусійним залишається питання, чи є дані, отримані під час кібероперацій (кібератак), «об'єктами» у розумінні права збройного конфлікту. Держави не мають єдиної думки з цього питання. Наприклад, позиція Німеччини полягає в тому, що «цивільний об'єкт, такий як комп'ютер, комп'ютерні мережі та кіберінфраструктура, або навіть бази даних, може стати військовою ціллю, якщо його використовують як для цивільних, так і для військових цілей, або виключно для останніх». Інші держави, такі як Норвегія, стверджують, що дані

можна вважати об’єктом під час вибору цілі. Франція вважає, що дані цивільного контенту можна вважати захищеним об’єктом [9].

У той час як Румунія погодилася, що кібератаки проти даних призводять до застосування МГП, і цивільні об’єкти/дані не можуть бути атаковані. На противагу цьому, такі країни, як Ізраїль, Данія та Чилі, вважають, що «згідно з чинним міжнародним гуманітарним правом «дані в принципі не кваліфікуються як об’єкти, оскільки вони є нематеріальними». Тобто, відсутність державного консенсусу ускладнює визначення подальших шляхів регулювання кіберпростору [9].

**Висновки**.

Враховуючи вищезазначене, можна дійти до висновків, що сучасні методи військового протистояння, вимагають оновлення норм МГП, оскільки пошук державами «сірих зон» спричиняє до нівелювання захисту прав ІВ для цифрових об’єктів під час збройних конфліктів. Правомірне вилучення цифрових об’єктів можливе лише за військової необхідності та в межах окупаційного режиму. За відсутності таких умов їх копіювання, передача третім особам чи інше використання можуть кваліфікуватися як незаконне привласнення або незаконне кібервтручання. Тому виникає гостра потреба в удосконалення самої моделі воєнної здобичі у цифровому просторі та розширене тлумачення норм МГП (з урахування забезпечення кібербезпеки певних цифрових об’єктів), які будуть ефективно визначати правові межі сучасних збройних конфліктів.

**Список використаних джерел:**

1.IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі від 18.10.1907 (дата звернення 01.04.2026)
URL: https://zakon.rada.gov.ua/laws/show/995_222#n141

2.Walker-Munro B.Can Autonomous Weapon Systems be Seized? Interactions with the Law of Prize and War Booty, Journal of Conflict and Security Law, Volume 29, Issue 1.2024, pp 143–163 URL: https://academic.oup.com/jcsl/article/29/1/143/7512115

3.Malis C. Ukraine Symposium – The THeMIS Bounty Part II: Stealing Enemy Technology.2022 URL: https://lieber.westpoint.edu/themis-bounty-part-ii-stealing-enemy-technology/

4. Mačák K.,Rodenhäuser T.Towards common understandings: the application of established IHL principles to cyber operations.2023 URL: https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/

5.Директива 96/9/ЄС Європейського Парламенту та Ради «Про правовий захист баз даних» від 11.03.1996.Редакція від 06.06.2019
URL: https://zakon.rada.gov.ua/laws/show/994_241#Text (дата звернення 10.04.2026)

6.Закон України «Про авторське право і суміжні права» від 01.01.2022 № 2811-IX.Редакція від 12.12.2025 URL: https://zakon.rada.gov.ua/laws/show/2811-20#n298(дата звернення 10.04.2026)

7.Угода «Про торговельні аспекти прав інтелектуальної власності» від 15.04.1994. Редакція від 06.12.2005 URL: https://zakon.rada.gov.ua/laws/show/981_018#Text (дата звернення 10.04.2026)

8.Schmitt M.The Influence of Weaponry on the Jus ad Bellum.2024 URL: https://lieber.westpoint.edu/influence-weaponry-jus-ad-bellum/

9.Giovannelli D.Customary International Law, National Law, and Considering Data as Objects.2023 URL: https://lieber.westpoint.edu/customary-international-law-national-law-considering-data-objects/

https://doi.org/10.5281/zenodo.20498021

***Тетяна НІКІТІНА,***
*кандидат технічних наук,*
*доцент кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*e-mail: t.nikitina@khai.edu*
*ORCID https://orcid.org/0009-0000-7549-1017*

***Ольга МОРОЗОВА,***
*доктор технічних наук,*
*професор кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*e-mail: o.morozova@khai.edu*
*ORCID https://orcid.org/0000-0001-7706-3155*

***Вячеслав ХАРЧЕНКО,***
*доктор технічних наук,*
*професор, завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*ORCID https://orcid.org/0000-0001-5352-077X*
*e-mail: v.kharchenko@csn.khai.edu*

# РЕЗИЛЬЄНТНІСТЬ НАУКОВОЇ ДІЯЛЬНОСТІ УНІВЕРСИТЕТУ В УМОВАХ ЗБУРЕНЬ: КОНЦЕПТУАЛЬНА МОДЕЛЬ КООРДИНАЦІЇ, АДАПТАЦІЇ ТА БЕЗПЕРЕРВНОСТІ

У сучасних умовах війни, гібридних загроз, релокації персоналу та обмеженого доступу до інфраструктури університети стикаються не лише з порушенням освітнього процесу, а й із порушенням наукової діяльності. Особливо вразливими є наукові підрозділи, для яких безперервність досліджень залежить від координації дослідників, проєктів, компетентностей, ресурсів та зовнішніх партнерств. У роботі проаналізовано сучасні підходи до резильєнтності університетів і безперервності діяльності в умовах кризи та запропоновано концептуальну модель координації наукової діяльності в умовах збурень. Запропонований підхід ґрунтується на багаторівневій архітектурі, що інтегрує рівень даних, рівень обробки та рівень прийняття рішень, а також враховує людиноцентричний підхід і гібридне прийняття рішень. Концептуальна модель орієнтована на підтримку безперервності наукової діяльності, адаптивний перерозподіл завдань і ресурсів, а також збереження людського капіталу в умовах нестабільного середовища.

**Ключові слова:** резильєнтність наукової діяльності, координація досліджень, порушення функціонування; безперервність діяльності університету, людиноцентричний підхід, гібридне прийняття рішень, кризова адаптація

# UNIVERSITY RESEARCH RESILIENCE UNDER DISRUPTION: A CONCEPTUAL MODEL FOR COORDINATION, ADAPTATION, AND CONTINUITY

Universities operating under crisis and disruption face not only interruptions in teaching and administration, but also fragmentation of research activity, reduced access to infrastructure, displacement of personnel, and increasing uncertainty in project execution. In such conditions, the resilience of research activity depends on the institution’s ability to coordinate human capital, competencies, projects,

infrastructure, and external support in an adaptive and timely manner.

Contemporary studies address university resilience, digital continuity, crisis adaptation, and cloud-based institutional models; however, the problem of research coordination under disruption remains insufficiently elaborated as a distinct dimension of university functioning. In particular, research units and departments require targeted coordination mechanisms capable of supporting continuity of scientific activity, flexible reallocation of tasks and resources, and adaptive decision-making under unstable conditions. In response to this gap, the present study proposes a conceptual model for research coordination under disruption, with emphasis on resilience factors, coordination logic, and human-centered as well as hybrid decision-making principles.

**Keywords**: research resilience, research coordination, disruption, university continuity, human-centered model, decision-making, crisis adaptation.

**Introduction**.

Educational institutions' resilience under unstable conditions is a key dimension of wider societal resilience. Universities are responsible not only for professional education, but also for research generation and the preservation of long-term national development capacity. In the context of hybrid threats, physical, digital, and social infrastructures become increasingly vulnerable, creating a strong demand for adaptive digital ecosystems, as demonstrated by Nikitina et al., [1] in their study on wartime university resilience.

The aim of this study is to analyze the factors affecting university research resilience under disruption and to present a conceptual model for coordination, adaptation, and continuity of research activity in crisis conditions. The objectives of the study are as follows:

- to analyze the factors affecting university research resilience under disruption;
- to review existing approaches to resilience, continuity, and crisis management in higher education;
- to identify the limitations of current approaches in supporting research coordination under crisis conditions;
- to systematize the key dimensions of research resilience in universities;
- to justify the role of intelligent coordination support in ensuring continuity of research activity;
- to propose a conceptual model for coordination, adaptation, and continuity of university research under disruption.

**Presentation of the Main Material**.

*A review of contemporary approaches and an analysis of modern crisis cases under hybrid threats.* As one of the relevant prior studies, the work by Shaya et al. [2] examines organizational resilience in higher education during the COVID-19 crisis and highlights the importance of leadership, resources, coordination, and adaptive organizational capacity as key factors of resilience. The study by Matos-Jiménez et al. [3] examines research challenges from the perspective of collaborative adaptation within a disrupted research network. It shows that continuity of research activity depends not only on institutional rules, but also on communication, shared problem identification, and collective mechanisms for overcoming logistical and organizational barriers, thereby supporting the development of methodological approaches to research coordination under disruption. The reviewed studies [2, 3, 4] are valuable because they identifies the organizational conditions and human factors shaping university resilience under prolonged disruption.

The study by Błaszczyk et al. [5] is valuable for the current analysis because it highlights the importance of social and organizational mechanisms of resilience in wartime university functioning. For the research context, this is especially relevant, since continuity at the department level depends not only on equipment or funding, but also on the preservation of internal ties, flexible redistribution of roles, informal mutual support, procedural adaptability, and the institution's ability to keep researchers engaged in the working environment.

This handbook [6] is relevant to our study because it translates institutional resilience into concrete continuity planning components, including critical functions, personnel, infrastructure, equipment, and crisis-response procedures. These elements provide a useful basis for extending the

analysis toward methodological approaches to university-level coordination under disruption.

The studies [1, 7] and Tarasenko et al. [8] propose broader and practice-oriented models of university resilience, covering infrastructure, digital environments, cloud-based solutions, and institution-wide continuity mechanisms under wartime conditions. In contrast, the present study adopts a narrower perspective by focusing specifically on research activity as a distinct university process and on strengthening the resilience, coordination, and continuity of research units under disruption.

In contrast to the broader institutional perspective presented in the reviewed studies [1-8], the present paper focuses on a more specific dimension, namely research coordination under disruption.

In this research, particular attention is focused on the factors affecting the continuity, resilience, and adaptive organization of research activity within university research units and departments. Fig. 1 presents a simplified conceptual view of university research resilience under disruption, showing the transition from disruption conditions through resilience factors and intelligent coordination support to continuity and adaptation outcomes.

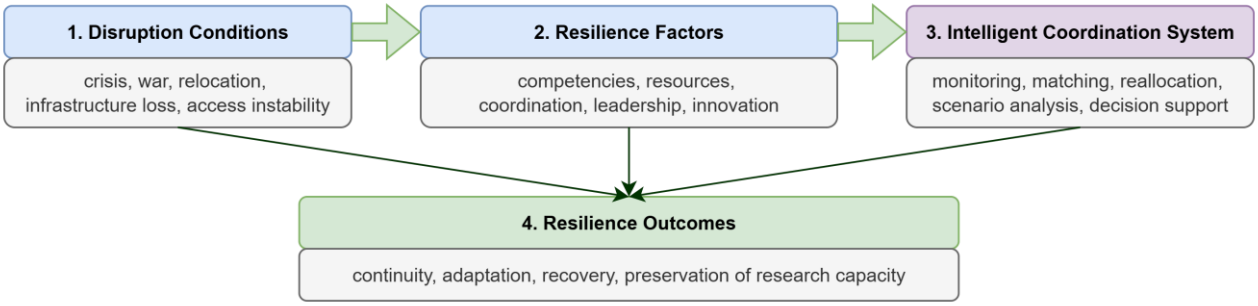


Fig. 1. Conceptual scheme of resilience factors and coordination mechanisms for research activity under disruption

**Development of the conceptual model.** The conceptual architecture of the research activity coordination system (Fig. 2) reflects the logic of data processing and decision-making under dynamic and unstable conditions. The system is designed as a multi-level structure that ensures a consistent transition from data collection to the formulation of management decisions and the assessment of their impact.

1. At the top level, the system objective is defined as ensuring the continuity of research activities, adaptation to disruption conditions, and effective reallocation of resources. This level establishes the overall logic of system operation and determines its strategic orientation.

2. The Data Layer includes the core informational entities managed by the system, including personnel, competencies, projects, infrastructure, and partners. This layer forms the foundation for subsequent data processing.

3. The Processing Layer integrates data from multiple sources and accounts for the influence of the external environment. At this level, the system analyzes personnel availability, infrastructure status, project characteristics, and opportunities for partner collaboration. A key feature of this layer is the consideration of external factors such as security risks, relocation, and loss of access to resources.

4. The Decision Layer supports the formulation of management actions aimed at stabilizing and sustaining research activities. These actions include task reallocation, replacement of personnel, relocation of staff, and optimization of infrastructure usage.

5. The final component of the architecture is the Impact Layer, which reflects the achievement of the system's primary objectives, including ensuring research continuity, reducing resource losses, and supporting human capital.

Thus, the proposed architecture enables the integration of heterogeneous data, accounts for dynamic environmental conditions, and supports adaptive management of research activities and supporting human capital.

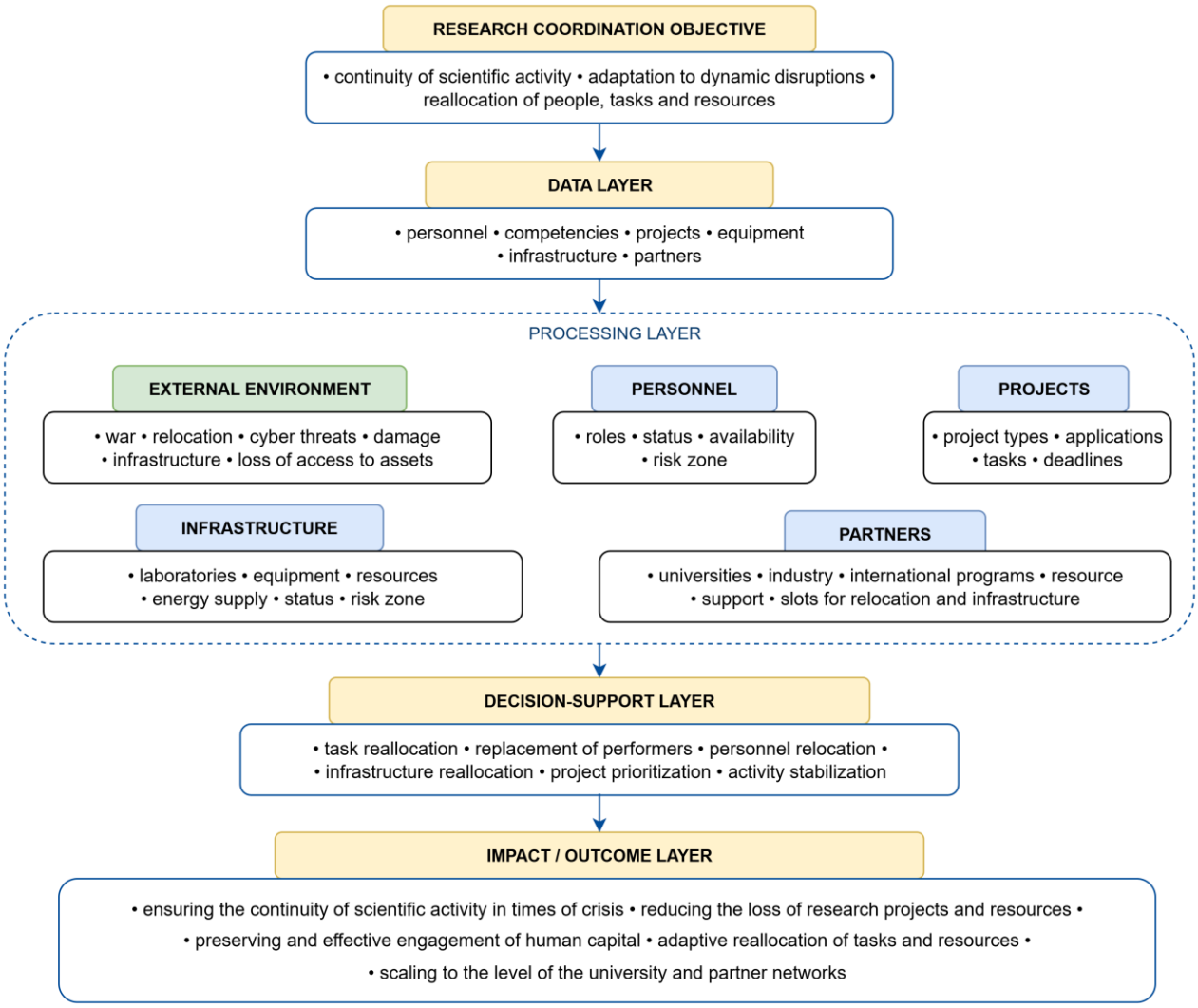


Fig. 2. Conceptual architecture of a research coordination system under disruption

*Human-centric approach.* A key component of the system concept is its human-centric approach, according to which personnel are considered not only as resources for project execution but also as key subjects of support in crisis conditions. The system acknowledges that researchers operate in dynamic and potentially hazardous environments, which may involve relocation, limited access to resources, and psychological factors affecting their performance.

Accordingly, decision-making is oriented not only toward task efficiency but also toward supporting researchers and maintaining the resilience of human capital. The system supporting interaction with users regarding aspects such as readiness for relocation, availability to work under different conditions, and individual constraints. This enables the formation of adaptive decisions that are aligned with the capabilities and current state of individuals.

*Hybrid decision-making approach.* The system implements a hybrid decision-making approach that combines automated mechanisms with human involvement (human-supervised decision-making). Depending on the context and the level of criticality, decisions may be made in fully automated mode, semi-automated mode with administrator confirmation, or under full human control.

Such an approach ensures efficient data processing and rapid response, while maintaining control and accountability for the decisions made. The system administrator acts as a coordinator and control element, with the ability to approve, modify, or reject the decisions proposed by the system. The scheme presented in Fig. 3 illustrates the overall hybrid decision-making approach, which integrates human-centric coordination and human-supervised decision-making, ensuring not only effective management of research processes but also the preservation of human capital.


Fig. 3. Human-in-the-Loop Coordination Model under Disrupted Environments

A multi-layer conceptual model for research coordination under disruption is proposed to support the continuity of scientific activity in dynamic and unstable conditions. The model is designed to integrate heterogeneous data related to personnel, projects, infrastructure, and external factors, and to transform this data into adaptive coordination and decision-support mechanisms.

A key feature of the model is its orientation toward disruption conditions, in which the availability of personnel, resources, and infrastructure is unstable and requires continuous monitoring, reassessment, and inclusion in the decision-making process. The following subsections describe the main architectural layers of the proposed model, beginning with the Data Layer, which forms the foundation of the overall coordination model.

**Prototype perspective.** An initial prototype [9] of the proposed research coordination platform has already been developed to demonstrate the core logic of task coordination, competency registration, task matching, infrastructure awareness, and crisis scenario support. At the present stage, the prototype serves as an illustrative implementation of the proposed conceptual model and provides a basis for further refinement and validation in future studies.

**Conclusions**. The conducted analysis showed that existing studies mainly address resilience at the broader institutional level, while the coordination of research activity under disruption remains insufficiently elaborated. In response, this paper proposes a conceptual model for research coordination under disruption that integrates heterogeneous data, adaptive coordination logic, and human-centered as well as hybrid decision-making principles. The proposed model is intended to support the continuity of research activity, preservation of human capital, and adaptive reallocation of tasks and resources in crisis conditions. Future work will include the development of methodological approaches and coordination models, further refinement of the prototype, scenario-based evaluation, and the extension of the model toward practical university-level implementation.

**Список використаних джерел:**

1. Nikitina, T., Morozova, O., Kharchenko, V. (2025). A Resilience Model for Borderline University Infrastructure in Wartime. In: Ermolayev, V., et al. Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2025. Communications in Computer and Information Science, vol 2763. Springer, Cham. https://doi.org/10.1007/978-3-032-10477-9_13

2. Shaya, N., Abukhait, R., Madani, R., & Khattak, M. N. (2023). Organizational Resilience of Higher Education Institutions: An Empirical Study during Covid-19 Pandemic. Higher Education Policy, 36, 529–555. DOI: https://doi.org/10.1057/s41307-022-00272-2

3. Matos-Jiménez K, Alamo-Rodriguez N, Fernández-Repollet E. Navigating Research Challenges: Collaborative Insights from a Research Retreat During a Healthcare Emergency in Puerto Rico. Int J Environ Res Public Health. 2025 Apr 16;22(4):623. https://doi.org/10.3390/ijerph22040623. PMID: 40283847; PMCID: PMC12027351.

4. Watermeyer, R., Crick, T., Knight, C. et al. COVID-19 and digital disruption in UK universities: afflictions and affordances of emergency online migration. High Educ 81, 623–641 (2021). https://doi.org/10.1007/s10734-020-00561-y

5. Błaszczyk, M., Kovalisko, N., Pieńkowski, P. et al. Coping with adversity: mechanisms of resilience in Ukrainian universities during the Russian-Ukrainian War—a perspective from Lviv University students. High Educ (2025). https://doi.org/10.1007/s10734-025-01506-z

6. Palkova, K., & Palkova, A. (Eds.). (2024). Handbook for Academic and Scientific Institutions: Improve Risk Management and Institutional Resilience in the face of Security Threats. Rīga Stradiņš University. DOI: https://doi.org/10.25143/handbook_ISBN-978-9934-618-61-1

7. Нікітіна Т. С., Морозова О. І., Харченко В. С. Резильєнтність інфраструктури університету в умовах війни: системна модель та її компоненти // Пропілеї права та безпеки. – 2025. – № 8. – С. 243–246. DOI: https://doi.org/10.32620/pls.2025.8.62

8. Tarasenko, S., Vorontsova, A., Régent, V., Soss, J., & Mylenkova, R. (2025). Science mapping analysis of challenges surrounding cloud universities and their impact on the resilience of higher education. Knowledge and Performance Management, 9(2), 1–17. DOI: http://dx.doi.org/10.21511/kpm.09(2).2025.01

9. Research Coordination Prototype for crisis-adaptive research task coordination. Web resource. Available at: https://sites.google.com/khai.edu/coordination-research-platform (accessed: 20.04.2026).

https://doi.org/10.5281/zenodo.20498067

***Максим ОЖОГІН,***
*Студент 2 курсу, група 726ю кафедри права*
*гуманітарного-правового факультету*
*Національного аерокосмічного університету*
*м. Харків, Україна*
*e-mail: m.o.ozohohin@student.khai.edu*

**Науковий керівник**:
***Світлана ГУЦУ,***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут»*
*м. Харків, Україна*
*ORCID: https://orcid.org/ 0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

# ЗАБЕЗПЕЧЕННЯ СТАНДАРТІВ ГІДНОЇ ПРАЦІ ДОМАШНІХ ПРАЦІВНИКІВ В УКРАЇНІ В УМОВАХ ВОЄННОЇ АГРЕСІЇ

Досліджено особливості забезпечення стандартів гідної праці домашніх працівників в Україні в умовах воєнної агресії. Проаналізовано сучасний стан правового регулювання, зокрема положення Закону України № 3680-IX, та виявлено його основні прогалини. Окрему увагу приділено невизначеності статусу роботодавця, проблемам контролю, захисту персональних даних і відмежуванню суміжних форм зайнятості. Розкрито міжнародні стандарти МОП та запропоновано напрями вдосконалення національного законодавства. Обґрунтовано необхідність імплементації Конвенції МОП № 189 і посилення соціального захисту домашніх працівників.

**Ключові слова**: домашні працівники, гідна праця, трудове право, воєнний стан, неформальна зайнятість, соціальний захист, персональні дані, трудові гарантії.

# ENSURING DECENT WORK STANDARDS FOR DOMESTIC WORKERS IN UKRAINE UNDER CONDITIONS OF ARMED AGGRESSION

The article examines the specifics of ensuring decent work standards for domestic workers in Ukraine under conditions of armed aggression. It analyzes the current state of legal regulation, in particular the provisions of the Law of Ukraine No. 3680-IX, and identifies its main gaps. Special attention is paid to the uncertainty of the employer's legal status, issues of labor control, protection of personal data, and differentiation between related forms of employment. International ILO standards are considered, and directions for improving national legislation are proposed. The necessity of implementing ILO Convention No. 189 and strengthening social protection for domestic workers is substantiated.

**Keywords:** domestic workers, decent work, labor law, martial law, informal employment, social protection, personal data, labor guarantees.

**Вступ**.

Серед різних форм реалізації права на працю сфера застосування домашньої праці тривалий час залишалася недостатньо врегульованою трудовим законодавством України. Попри існування окремих нормативних актів, зокрема наказу Міністерства праці України від 08.06.2001 № 260, який передбачає форму трудового договору між працівником і фізичною особою, що використовує найману працю, комплексного правового регулювання цієї сфери фактично не існувало. Це спричинило формування значного сегмента неформальної

зайнятості, що, у свою чергу, обумовило системні порушення трудових прав цієї категорії працівників. За даними Міжнародна організація праці у світі налічується близько 75,6 млн домашніх працівників (віком 15+). Водночас з урахуванням тіньової зайнятості оцінки можуть сягати до 100 млн осіб. В Україні статистика теж показова: близько 162 тис. осіб зайняті у сфері домашньої праці (за оцінками Держстату). При цьому до 80% працюють неофіційно. Фактично це означає значно більший «прихований» ринок робочої сили в сфері домашньої праці.

**Викладення основного матеріалу**.

Суттєві зміни у правовому регулюванні праці домашніх працівників відбулися з прийняттям 25 квітня 2024 року Закону України № 3680-IX «Про внесення змін до деяких законодавчих актів України щодо регулювання праці домашніх працівників» [1], яким уперше на законодавчому рівні закріплено правовий статус домашніх працівників та визначено особливості їхньої праці. Документ є важливим етапом у формуванні правового регулювання праці домашніх працівників в Україні, оскільки спрямований на закріплення ключових трудових і соціальних гарантій, зокрема щодо умов праці, порядку укладення трудового договору, оплати праці та участі у системі соціального страхування. Його прийняття зумовлене об'єктивною необхідністю виведення значної частини цієї сфери з тіньового сектору та забезпечення належного рівня захисту працівників, які традиційно залишалися поза ефективним правовим регулюванням. Водночас окремі положення закону потребують суттєвого доопрацювання, зокрема щодо чіткого визначення статусу роботодавця, усунення суперечливих підстав звільнення та запровадження дієвого механізму контролю за дотриманням трудового законодавства з урахуванням принципу недоторканності приватного життя [2]. У цьому контексті подальше вдосконалення законодавства має здійснюватися з урахуванням міжнародних і європейських стандартів, зокрема, положень Конвенції Міжнародної організації праці № 189 про гідну працю домашніх працівників (2011 р.) [3] та Рекомендації МОП № 201 [4], що дозволить підвищити рівень соціального захисту домашніх працівників і забезпечити баланс між приватними та публічними інтересами.

Актуальність теми значно посилюється в умовах воєнної агресії проти України. Воєнний стан спричинив глибокі трансформації ринку праці, серед яких особливої уваги заслуговують: масове переміщення населення, зростання рівня бідності, збільшення навантаження на сферу догляду, а також поширення нестандартних і неформальних форм зайнятості. У таких умовах домашні працівники стають однією з найбільш соціально вразливих груп, що обумовлено поєднанням приватного характеру праці та обмежених можливостей державного контролю.

Доцільно чітко відмежовувати поняття «дистанційна робота», «надомна робота» та «домашня праця», оскільки вони відображають різні форми реалізації працівником трудової функції. Дистанційна та надомна робота належать до так званих атипових форм зайнятості, адже передбачають виконання роботи поза місцезнаходженням роботодавця. Зокрема, дистанційна робота характеризується виконанням трудових обов'язків поза традиційним робочим місцем із використанням інформаційно-комунікаційних технологій, гнучкістю трудових відносин і, як правило, відсутністю підпорядкування правилам внутрішнього трудового розпорядку (ст. $60^2$ КЗпП України) [5].

Надомна робота, своєю чергою, передбачає виконання працівником роботи у визначеному ним приміщенні, яке має відповідне технічне оснащення та закріплену робочу зону, необхідну для виробництва продукції, надання послуг чи виконання робіт поза виробничими або службовими приміщеннями роботодавця (ст. $60^1$ КЗпП України), у тому числі з використанням сучасних засобів телекомунікації. Натомість домашня праця має іншу правову природу: вона виконується безпосередньо в домогосподарстві або для нього, за місцем проживання роботодавця – фізичної особи, і пов'язана з обслуговуванням побутових потреб. Така форма зайнятості передбачає специфічний режим організації праці, включаючи особливості обліку робочого часу та правового регулювання трудових відносин.

Ключовою проблемою є те, що праця домашніх працівників здійснюється у межах приватного домогосподарства, яке традиційно розглядається як сфера, захищена правом на недоторканність житла та приватного життя. Це створює конфлікт між необхідністю

забезпечення державного нагляду за дотриманням трудових прав і повагою до приватності. Внаслідок цього інспекційні механізми у сфері праці фактично не поширюються на домашні господарства або застосовуються обмежено, що сприяє латентності порушень.

Додатковою суттєвою проблемою є невизначеність правового статусу роботодавця – фізичної особи, яка використовує працю домашнього працівника. На відміну від роботодавця-суб'єкта господарювання, така особа не здійснює підприємницької діяльності, не має обов'язку ведення кадрової документації у класичному розумінні та не завжди підпадає під стандартні процедури державного нагляду. Це ускладнює застосування до неї механізмів юридичної відповідальності, зокрема адміністративної та фінансової, а також істотно обмежує можливості інспекційних органів щодо перевірки дотримання трудового законодавства. Крім того, відсутність уніфікованого підходу до визначення обсягу обов'язків такого роботодавця (зокрема щодо охорони праці, ведення обліку робочого часу, забезпечення соціального страхування) створює правову невизначеність як для самого роботодавця, так і для працівника, що сприяє поширенню неформальної зайнятості.

Не менш проблемним є відсутність чітких критеріїв розмежування понять «домогосподарство» та «сім'я», які хоча й перетинаються, але не є тотожними з юридичної точки зору. Особливість домашньої праці полягає в тому, що вона виконується у або для домогосподарства, яке об'єднує осіб, пов'язаних спільним проживанням, побутом і витратами [6]. Домогосподарство може включати осіб, не пов'язаних сімейними чи родинними зв'язками, але об'єднаних спільним проживанням і веденням побуту, тоді як сім'я має більш вузьке правове визначення, пов'язане з особистими немайновими та майновими правами й обов'язками. Невизначеність цих категорій створює ризики маніпуляцій, зокрема маскування трудових відносин під сімейні або побутові, що дозволяє уникати укладення трудового договору, сплати податків і соціальних внесків. У результаті домашні працівники можуть бути фактично позбавлені статусу найманих працівників і відповідних гарантій, що підриває ефективність правового регулювання та унеможливлює належний захист їхніх прав.

Також постає проблема захисту персональних даних домашніх працівників, оскільки їхня трудова діяльність здійснюється у приватному домогосподарстві, де межа між професійною взаємодією та втручанням у приватне життя є особливо тонкою. У процесі працевлаштування та виконання трудових обов'язків роботодавець-фізична особа може отримувати доступ до значного обсягу персональної інформації працівника, включаючи паспортні дані, відомості про сімейний стан, стан здоров'я, місце проживання, банківські реквізити тощо. Відсутність чітких процедур обробки, зберігання та захисту таких даних підвищує ризики їх неправомірного використання, розголошення або передачі третім особам без згоди працівника [7].

Додатковою проблемою є складність застосування загальних положень законодавства про захист персональних даних у приватному домогосподарстві, яке не завжди усвідомлюється як суб'єкт, що обробляє персональні дані. Домашні працівники часто не мають ефективних механізмів контролю за тим, як саме використовується їхня інформація, а також обмежені у можливості оперативного захисту своїх прав. У цьому контексті актуальним є запровадження спеціальних гарантій у сфері домашньої праці, які б передбачали обов'язок роботодавця забезпечувати конфіденційність персональних даних, а також встановлювали б чіткі правила їх обробки та відповідальність за порушення режиму захисту інформації.

У міжнародному праві проблема захисту домашніх працівників отримала належне нормативне закріплення. Зокрема, Конвенція МОП № 189 встановлює принцип рівності домашніх працівників з іншими категоріями працівників щодо основних трудових прав, включаючи:

- право на справедливі умови праці та гідну оплату;
- обмеження робочого часу та гарантії відпочинку;
- доступ до системи соціального забезпечення;
- захист від насильства, домагань та експлуатації;
- право на укладення письмового трудового договору.

Крім того, важливе значення мають положення міжнародних актів у сфері прав людини, зокрема Міжнародного пакту про економічні, соціальні і культурні права (1966 р.), Європейської соціальної хартії (переглянутої), а також практики Європейського суду з прав людини, яка підкреслює необхідність забезпечення балансу між правом на приватність і захистом трудових прав.

Порівняльно-правовий аналіз свідчить, що у багатьох державах, які ратифікували Конвенцію МОП № 189 (наприклад, Італія, Іспанія, Португалія), запроваджено спеціальні механізми легалізації домашньої праці, включаючи спрощені процедури укладення трудових договорів, податкові стимули для роботодавців та обов'язкове соціальне страхування.

В Україні ж однією з найбільш критичних проблем залишається добровільний характер соціального страхування домашніх працівників. Такий підхід суперечить загальним принципам соціальної держави та міжнародним стандартам, оскільки фактично позбавляє працівників гарантій у разі втрати працездатності, безробіття або настання інших соціальних ризиків. У контексті воєнного стану це створює додаткові загрози соціальній безпеці [8].

З огляду на викладене, доцільно запропонувати комплексний підхід до вдосконалення правового регулювання, який включає:

1. Ратифікацію Конвенції МОП № 189 та гармонізацію національного законодавства з її положеннями, що дозволить інтегрувати міжнародні стандарти у внутрішню правову систему.
2. Запровадження обов'язкового соціального страхування домашніх працівників із покладенням відповідних обов'язків на роботодавця – фізичну особу, з можливим застосуванням спрощених механізмів адміністрування внесків.
3. Створення спеціального правового режиму контролю за дотриманням трудових прав у домогосподарствах, який би забезпечував баланс між правом на приватність і необхідністю державного нагляду (наприклад, через інститут повідомної інспекції або альтернативні механізми моніторингу).
4. Цифровізацію трудових відносин у цій сфері, зокрема через використання державних електронних сервісів для реєстрації трудових договорів, обліку робочого часу та сплати соціальних внесків.
5. Запровадження стимулюючих механізмів для легалізації праці, включаючи податкові пільги для домогосподарств, що офіційно оформлюють трудові відносини.
6. Посилення гарантій захисту від дискримінації та насильства, з урахуванням гендерного аспекту, оскільки переважна більшість домашніх працівників – жінки.

**Висновки**.

Таким чином, правове регулювання праці домашніх працівників в Україні перебуває на етапі формування, а прийняття Закону України № 3680-IX є важливим, але недостатнім кроком у напрямі забезпечення стандартів гідної праці. В умовах воєнної агресії наявні прогалини законодавства набувають особливої гостроти, що вимагає системного підходу до їх усунення.

Ключовими напрямами вдосконалення є імплементація міжнародних стандартів, інституціоналізація соціального захисту, адаптація механізмів контролю до специфіки домашньої праці та забезпечення ефективного балансу між приватними і публічними інтересами. Реалізація зазначених заходів сприятиме не лише захисту прав домашніх працівників, а й детінізації ринку праці та зміцненню соціальної державності України.

**Список використаних джерел:**

1. Закон України «Про внесення змін до деяких законодавчих актів України щодо регулювання праці домашніх працівників» [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/3680-20#Text

2. Пожарова О. В. Законодавче забезпечення праці домашніх працівників: сучасний стан // Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) / за заг. ред. С. В. Ківалова. Одеса, 2023. Т. 1. С. 470–472.

3. Конвенція Міжнародної організації праці № 189 про гідну працю домашніх працівників (2011 р.) [Електронний ресурс]. URL: https://www.ilo.org

4. Рекомендація Міжнародної організації праці № 201 щодо гідної праці домашніх працівників [Електронний ресурс]. URL: https://www.ilo.org

5. Кодекс законів про працю України (Глава XI-A. Праця домашніх працівників) [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text

6. Мокрицька Н. П. Члени домашнього господарства: проблеми правового статусу // Аналітично-порівняльне правознавство. 2022. № 6. С. 121–126.

7. Спіцина Г., Гуцу С. Ф. Щодо питання правового захисту персональних даних працівників // Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 76, ч. 1. С. 255–260.

8. Гуцу С. Ф. Соціальний захист: визначення сфери дії та державної політики // Правові реалії сьогодення : матеріали I Всеукр. наук.-практ. конф. (15 трав. 2024 р.). Харків : ХНЕУ ім. С. Кузнеця, 2024. С. 83–88.

https://doi.org/10.5281/zenodo.20498104

***Сергій ОНОПРІЄНКО,***
*провідний інженер лабораторії*
*інформаційно-аналітичного забезпечення*
*судово-експертної діяльності,*
*сертифікації та контролю якості досліджень*
*ORCID: https://orcid.org/0000-0001-7574-7457*

***Тетяна ЛАЗАРЕВА,***
*магістр правоохоронної діяльності,*
*завідувачка лабораторії кафедри права*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://orcid.org/0009-0009-3827-6102*
*e-mail: t.lazareva@khai.edu,*

# КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ: СУЧАСНІ ВИКЛИКИ ПРАВОВОГО РЕГУЛЮВАННЯ В УКРАЇНІ

У роботі розглянуто сучасні тенденції кіберзлочинності в Україні, зокрема використання криптовалют у злочинних цілях, проблеми юрисдикції та допустимості електронних доказів у кримінальному процесі. Проаналізовано статистику кіберінцидентів, яка свідчить про стрімке зростання кількості атак на державні органи, критичну інфраструктуру та фінансові установи. Визначено ключові проблеми правового регулювання – відсутність комплексного законодавства щодо віртуальних активів, складнощі міжнародної співпраці та потреба у гармонізації українських норм із європейськими стандартами. Зроблено висновок про необхідність системного підходу, що поєднує правові, організаційні та технологічні інструменти для ефективної протидії кіберзлочинності.

**Ключові слова**: кіберзлочинність, електронні докази, криптовалюти, кібербезпека, правоохоронні органи, юрисдикція, віртуальні активи.

## CYBERCRIME AND ELECTRONIC EVIDENCE: CURRENT CHALLENGES OF LEGAL REGULATION IN UKRAINE

The paper examines current trends in cybercrime in Ukraine, in particular the use of cryptocurrencies for criminal purposes, jurisdictional challenges, and the admissibility of electronic evidence in criminal proceedings. Cyber incident statistics are analyzed, demonstrating a sharp increase in the number of attacks on government institutions, critical infrastructure, and financial organizations. Key problems of legal regulation are identified, including the absence of comprehensive legislation on virtual assets, difficulties in international cooperation, and the need to harmonize Ukrainian norms with European standards. The conclusion emphasizes the necessity of a systemic approach that integrates legal, organizational, and technological instruments to effectively counter cybercrime.

**Keywords**: cybercrime, electronic evidence, cryptocurrencies, cybersecurity, law enforcement agencies, jurisdiction, virtual assets.

**Вступ**.

Інформаційні технології стали невід’ємною частиною як механізму державного управління, так і повсякденних практик у житті мільйонів людей. Зростання обсягів інформації, розвиток комп’ютерних мереж і збільшення кількості користувачів, а також спрощення доступу до мережевих ресурсів суттєво підвищують суспільну небезпеку

комп’ютерних злочинів. Використання сучасних інформаційно-комунікаційних технологій у злочинній діяльності дозволяє готувати, здійснювати та приховувати правопорушення безконтактним способом, а також протидіяти їх розслідуванню. У процесі безпосереднього вчинення посягання злочинці можуть розподіляти ролі та координувати свої дії дистанційно за допомогою цифрових засобів. Процес учинення комп’ютерних злочинів стає дедалі прихованішим, що ускладнює їх виявлення, припинення, розслідування та попередження. Найбільші труднощі у виявленні злочинів і доведенні вини у кримінальних провадженнях щодо кіберзлочинності викликає транснаціональний характер таких діянь, що у ряді випадків спричиняє юрисдикційні колізії. В інформаційно-комунікаційних мережах відсутні загальновизнані державні кордони, що формує потенційно конфліктне середовище з відносно низьким рівнем безпеки обігу інформації. Негативний вплив мають і значні відмінності у національному кримінальному законодавстві різних країн світу у сфері боротьби з кіберзлочинністю, у правозастосовній практиці та діяльності правоохоронних органів окремих держав.

**Викладення основного матеріалу**.

Аналіз якісних і кількісних показників кіберзлочинності за період 2020–2026 років свідчить про необхідність суттєвого підвищення вимог до ефективності діяльності правоохоронних органів, адже масштаби проблеми зростають щороку. За даними Департаменту кіберполіції Національної поліції України, у 2024 році було зафіксовано понад 4 315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році (2 541 випадок), причому найбільше атакували державні органи, сектор оборони, енергетику та телекомунікації. У 2020–2021 роках домінували інтернет-шахрайства та фішингові атаки, у 2022–2023 роках – після початку повномасштабної агресії РФ – різко зросли атаки на державні системи та критичну інфраструктуру, а у 2025–2026 роках прогнозується збільшення атак із використанням штучного інтелекту та криптовалютних платформ для відмивання коштів.

Особливого значення набуває робота всіх правоохоронних інституцій України – Національної поліції, Кіберполіції, Служби безпеки України, прокуратури та Держспецзв’язку, адже їхня діяльність має бути спрямована не лише на розслідування окремих випадків, але й на системне попередження загроз, розвиток міжнародної співпраці та гармонізацію законодавства з нормами ЄС. Зростання кількості злочинів із використанням сучасних технологій створює загрозу не лише майновим правам, але й правам особи та національній безпеці, що підтверджує необхідність комплексної протидії та посилення міжнародної взаємодії.

Поширилася практика використання криптовалют у злочинних цілях, зокрема для легалізації доходів, отриманих у результаті кіберзлочинів. Це явище стало особливо актуальним на тлі зростання кількості атак на державні реєстри, фінансові установи та критичну інфраструктуру. Оскільки значна частина зафіксованих інцидентів пов’язана з використанням криптовалютних платформ для відмивання коштів та фінансування злочинних угруповань, проблеми виникають не лише через відсутність остаточного правового регулювання віртуальних активів, а й через складність застосування традиційних процесуальних процедур, таких як накладення арешту на кошти у криптогаманцях. Недосконалість процесуального законодавства ускладнює проведення досудового розслідування, зокрема щодо визначення підслідності матеріалів перевірки. В Україні питання правового статусу криптовалют досі остаточно не врегульоване: хоча у 2021 році був ухвалений Закон «Про віртуальні активи», він усе ще потребує комплексної імплементації у фінансову та кримінально-правову системи.

Особливої актуальності набули проблеми юрисдикції та отримання даних від постачальників інформаційних послуг, зареєстрованих за кордоном. Це ускладнює проведення оперативно-розшукових заходів та подальше використання отриманої інформації у кримінальному процесі. Аналіз практики показує певну гнучкість у використанні електронних доказів, однак вона супроводжується невизначеністю щодо правил їх допустимості. У судовій практиці трапляються випадки скасування обвинувальних вироків через процесуальні сумніви, що свідчить про необхідність чіткого законодавчого регулювання. Водночас електронні докази відіграють ключову роль у доведенні обставин злочину. В Україні ці питання регулюються Кримінальним процесуальним кодексом, який у ст. 99 визначає електронні докази як самостійний вид доказів, а також практикою Верховного Суду (наприклад, Постанова від 21.12.2021 у справі № 761/4625/20). Проте питання міжнародного доступу до даних залишаються відкритими, що потребує розвитку механізмів міжнародної допомоги та гармонізації норм із європейськими стандартами.

**Висновки**.

Таким чином, підсумовуючи викладене, хочемо зазначити, що сучасна кіберзлочинність в Україні є багатовимірним явищем, яке виходить далеко за межі класичних форм злочинів у сфері комп'ютерної інформації. Вона охоплює використання криптовалют, проблеми юрисдикції, складнощі з допустимістю цифрових доказів, а також нові виклики штучного інтелекту. Це вимагає не лише вдосконалення законодавства, а й формування єдиної стратегії взаємодії правоохоронних органів, розвитку міжнародної співпраці та створення прозорих процесуальних стандартів. Лише комплексний підхід, що поєднує правові, організаційні та технологічні інструменти, здатен забезпечити ефективну протидію кіберзлочинності та захистити права громадян і національну безпеку України.

**Список використаних джерел:**

1. Верховна Рада України. Кримінальний кодекс України : Закон від 5 квітня 2001 р. № 2341-III (зі змінами). URL: https://zakon.rada.gov.ua/go/2341-14

2. Верховна Рада України. Кримінальний процесуальний кодекс України : Закон від 13 квітня 2012 р. № 4651-VI (зі змінами). URL: https://zakon.rada.gov.ua/go/4651-17

3. Верховна Рада України. Про основні засади забезпечення кібербезпеки України : Закон від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19

4. Президент України. Стратегія кібербезпеки України : Указ від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/go/447/2021

5. Верховна Рада України. Про електронні комунікації : Закон від 16 грудня 2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/go/1089-20

6. Верховна Рада України. Про віртуальні активи : Закон від 17 лютого 2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/go/2074-20 (zakon.rada.gov.ua in Bing)

7. Верховний Суд України. Постанова від 21 грудня 2021 р. у справі № 761/4625/20. URL: https://reyestr.court.gov.ua/Review/102123456

8. Департамент кіберполіції Національної поліції України. Звіт про кіберінциденти 2024 року. URL: https://cyberpolice.gov.ua

https://doi.org/10.5281/zenodo.20498142

***Віталій ПАВЛИКІВСЬКИЙ***,
*доктор юридичних наук, професор*
*завідувач кафедри права Національного аерокосмічного*
*університету «Харківський авіаційний інститут», м. Харків, Україна*
ORCID: https://orcid.org/0000-0002-1190-9303
e-mail: v.pavlykivskyi@khai.edu

# ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УКРАЇНІ (ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ)

У тезах здійснено аналіз законодавчих ініціатив щодо посилення адміністративної та кримінальної відповідальності за порушення правил використання безпілотних повітряних суден в Україні. Розглянуто положення законопроєкту № 13600 та обґрунтовано його основні недоліки, зокрема надмірно репресивний характер і дублювання функцій державних органів. Визначено ризики запровадження обов'язкової реєстрації та сертифікації для широкого кола користувачів. Проведено порівняльний аналіз підходів до правового регулювання використання БПЛА у США, що базуються на принципах превенції та ризик-орієнтованості. Обґрунтовано необхідність формування збалансованої моделі правового регулювання в Україні. Запропоновано напрями вдосконалення законодавства з урахуванням міжнародного досвіду.

**Ключові слова**: безпілотні повітряні судна; БПЛА; правове регулювання; адміністративна відповідальність; кримінальна відповідальність; повітряний простір; законопроєкт № 13600.

## USE OF UNMANNED AIRCRAFT IN UKRAINE (LEGAL REGULATION ISSUES)

The theses analyze legislative initiatives to strengthen administrative and criminal liability for violations of the rules for the use of unmanned aerial vehicles in Ukraine. The provisions of draft law No. 13600 are considered and its main shortcomings are substantiated, in particular, the excessively repressive nature and duplication of functions of state bodies. The risks of introducing mandatory registration and certification for a wide range of users are identified. A comparative analysis of approaches to legal regulation of the use of UAVs in the USA, based on the principles of prevention and risk-orientation, is conducted. The need to form a balanced model of legal regulation in Ukraine is substantiated. Directions for improving legislation are proposed, taking into account international experience.

**Keywords**: unmanned aerial vehicles; UAVs; legal regulation; administrative liability; criminal liability; airspace; draft law №. 13600.

**Вступ**.

У 2025 році до Верховної Ради України Комітетом з питань правоохоронної діяльності було внесено законопроєкт № 13600 "Про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального кодексу України та Повітряного кодексу України щодо посилення відповідальності за правопорушення в галузі цивільної авіації після припинення або скасування воєнного стану в Україні", згідно з яким пропонувалося передбачити адміністративну відповідальність за експлуатацію безпілотного повітряного судна без реєстрації в Державному реєстрі цивільних повітряних суден України або без

проведення державного обліку в органах Національної поліції, або без документів, що дають право виконувати польоти, або з порушенням строку дії таких документів чи встановлених ними вимог [3]. Також передбачалося встановити адміністративну відповідальність за керування безпілотними повітряними суднами в стані алкогольного, наркотичного чи іншого сп'яніння або під впливом лікарських препаратів, що знижують їх увагу та швидкість реакції, а також передачу керування безпілотним повітряним судном особі, яка перебуває в стані сп'яніння чи під впливом таких лікарських препаратів.

**Викладення основного матеріалу**.

Цим проєктом, змінами до кримінального кодексу пропонувалося встановити відповідальність за експлуатацію безпілотного повітряного судна без реєстрації в Державному реєстрі цивільних повітряних суден України або без проведення державного обліку в органах Національної поліції України, або без документів, що дають право виконувати польоти, або з порушенням строку дії таких документів чи встановлених ними вимог, або інше порушення правил та порядку використання повітряного простору України, якщо це спричинило потерпілому середньої тяжкості тілесні ушкодження або заподіяло матеріальну шкоду у великому розмірі, керування безпілотними повітряними суднами в стані алкогольного, наркотичного чи іншого сп'яніння або під впливом лікарських препаратів, що знижують їх увагу та швидкість реакції, а також передачу керування безпілотним повітряним судном особі, яка перебуває в стані сп'яніння чи під впливом таких лікарських препаратів, якщо це спричинило потерпілому середньої тяжкості тілесні ушкодження або заподіяло матеріальну шкоду у великому розмірі [3]. Крім того, проєктом Закону передбачалося внесення змін до Повітряного кодексу України щодо необхідності здійснення обліку безпілотних повітряних суден, максимальна злітна вага яких становить від 0,25 до 20 кілограмів і які використовуються для розваг, в освітньому процесі для здобуття позашкільної освіти, у науковій та спортивній діяльності. Такі повітряні судна підлягають державному обліку в органах Національної поліції України [3].

Враховуючи особливості напрямку діяльності комітету-ініціатора законопроекту, вказані пропозиції законопроекту несли суттєві ризики. Як зазначила перша заступниця голови Комітету ВР з питань транспорту та інфраструктури Юлія Кліменко, спірним моментом пропонованого законопроєкту було те, що він не враховував особливості категорізації та призначення існуючих на сьогодні безпілотних літальних апаратів, зокрема цивільні, промислові, військові тощо. Головним же ризиком даного законопроєкту є обов'язковість включення будь-яких безпілотних літальних апаратів до реєстру, ведення якого покладається на Міністерство внутрішніх справ, який по суті повинен дублювати державний реєстр повітряних суден України Державної авіаційної служби України. При цьому, реєстрація в такому реєстрі повинна здійснюватися за кошти власника з обов'язковим платним навчанням і сертифікацією у визначених кампаніях. Як наслідок Верховна Рада відхилила цей законопроект в першому ж читанні [4].

Слід вказати на суттєву різницю в підходах щодо організації та контролю за використанням безпілотних літальних апаратів в Європейському Союзі та США. На відміну від поданого законопроекту, правила Федерального управління цивільної авіації (FAA) спрямовані не на покарання порушника, а на забезпечення безпеки користування безпілотними літальними апаратами та ознайомлення користувачів з відповідними вимогами щодо безпеки польотів. Згідно правил Федерального управління цивільної авіації польоти БПЛА поділяються на розважальні (рекреаційні) та комерційні [1]. Використання БПЛА з розважальною метою вагою меншою за 250 г не потребує реєстрації та ідентифікації літального апарату. За наявності ваги понад 250 г БПЛА підлягає обов'язковій онлайн

реєстрації виключно через офіційний портал FAA DroneZone FAADroneZone ($5 на 3 роки) та маркування дрона ((FAA) 49 U.S.C. 44809). Для користування БПЛА з розважальною метою Пілот повинен пройти безкоштовний онлайн-тест TRUST та отримати відповідний сертифікат. Безкоштовний онлайн-тест TRUST (The Recreational UAS Safety Test) розроблений Федеральним управлінням цивільної авіації США (FAA) у тісній співпраці з представниками індустрії безпілотників та іншими зацікавленими сторонами. Безпосередньо тест проводиться уповноваженими FAA адміністраторами (Test Administrators), які надають доступ до тесту на своїх веб-ресурсах, зокрема Pilot Institute [2]. Вказаний тест є безкоштовним та складається з чотирьох блоків (повітряний простір, передпольотні вимоги, лінія видимості, системи дронів). При цьому, за кожним блоком слід відповісти на контрольні питання (загальна кількість складає 30-40 питань). Курс дозволяє ознайомитися з вимогами та заборонами щодо безпеки пілотування, зокрема вимогами щодо польотів над людьми, закритими зонами, в межах прямого зорового контакту БПЛА. За результатами позитивного проходження тесту кандидат отримує електронний сертифікат на своє ім’я.

У випадку використання БПЛА вагою понад 250 гр. або з комерційною метою незалежно від ваги, вимагається обов’язкова реєстрація та наявність ідентифікаційного номеру (Remote ID:). Для комерційних польотів пілот повинен отримати професійний сертифікат на управління БПЛА (Remote Pilot Certificate) зі складанням відповідного платного професійного іспиту в акредитованому центрі FAA.

Регламентовано також виробництво та продаж БПЛА, зокрема відповідними вимогами American Security Drone Act (ASDA) та рішеннями FCC (Federal Register). За останні декілька років запроваджено жорсткі обмеження на імпорт та використання нових моделей китайських компаній (DJI, Autel) для держструктур та їх підрядників. Крім того, виробники в обов’язковому порядку повинні вбудовувати систему Remote ID у нові апарати.

Слід зазначити, ще одну деталь, яка відрізняє підходи в регулюванні діяльності з використання БПЛА в нашій країні та США. Розробка правил з використання БПЛА для розваг покладається на громадські організації, визнані Федеральним управлінням цивільної авіації (FAA), а не на державні структури. Перші забезпечують інформування пілотів-аматорів щодо безпеки використання БПЛА, контрольованих та неконтрольованих зон використання літальних апаратів, правових наслідків порушення відповідних правил.

**Висновки**.

Таким чином, проведений аналіз законодавчої ініціативи щодо посилення відповідальності за правопорушення у сфері використання безпілотних повітряних суден дозволяє сформулювати такі узагальнюючі висновки.

По-перше, законопроєкт № 13600 відображає загальну тенденцію до посилення державного контролю за використанням безпілотних літальних апаратів, що є об’єктивно зумовленим зростанням їх поширеності та потенційних ризиків для безпеки повітряного простору. Водночас запропонований підхід має переважно репресивний характер, оскільки орієнтований насамперед на встановлення адміністративної та кримінальної відповідальності, а не на формування превентивних механізмів безпечного використання БПЛА.

По-друге, запропоноване законодавче регулювання не враховує належним чином різноманітність категорій безпілотних повітряних суден (цивільних, комерційних, промислових, військових тощо), що призводить до надмірної уніфікації правового режиму їх використання. Такий підхід створює ризики необґрунтованого обтяження користувачів, зокрема у сфері рекреаційного та освітнього застосування БПЛА.

По-третє, суттєвим недоліком законопроєкту є запровадження паралельної системи державного обліку безпілотних повітряних суден в органах Національної поліції, що фактично

дублює функції Державної авіаційної служби України. Це суперечить принципам ефективного державного управління, створює надмірні адміністративні бар'єри та підвищує фінансове навантаження на власників БПЛА.

По-четверте, встановлення обов'язкової платної реєстрації, навчання та сертифікації для широкого кола користувачів, незалежно від характеру використання БПЛА, може мати стримуючий вплив на розвиток інновацій, наукової діяльності, позашкільної освіти та технологічного підприємництва.

По-п'яте, порівняльний аналіз із підходами, що застосовуються у США, свідчить про доцільність переорієнтації на превентивну модель регулювання. Зокрема, правила Федерального управління цивільної авіації (FAA) базуються на диференціації режимів використання БПЛА залежно від мети (рекреаційна чи комерційна), ваги апарата та рівня ризику, а також на пріоритеті інформування та навчання користувачів. Важливим елементом цієї моделі є доступність процедур (онлайн-реєстрація, безкоштовне базове навчання) та залучення громадських організацій до формування культури безпечного використання БПЛА.

По-шосте, ефективне правове регулювання у цій сфері має ґрунтуватися на принципах пропорційності, ризик-орієнтованого підходу та недопущення надмірного адміністративного тиску.

**Список використаних джерел:**

1. FAA Regulations. An official website of the United States government. Department of Transportation. Federal Aviation Administration United States URL: https://www.faa.gov/regulations_policies/faa_regulations (дата звернення: 2.04.2026 р.).

2. Recreational UAS Safety Test (TRUST) Online Portal. URL: https://trust.pilotinstitute.com/ (дата звернення: 2.04.2026 р.).

3. Проект Закону про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального кодексу України та Повітряного кодексу України щодо посилення відповідальності за правопорушення в галузі цивільної авіації після припинення або скасування воєнного стану в Україні від 05.08.2025. № 13600 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/56924 (дата звернення: 2.04.2026 р.).

4. Рада не підтримала законопроєкт про обіг дронів. Депутатка пояснила чому і які подальші кроки https://lb.ua/society/2026/02/25/724279_rada_pidtrimala_zakonoproiekt.html (дата звернення: 2.04.2026 р.).

https://doi.org/10.5281/zenodo.20498193

***Дмитро РАСПУТНІЙ,***
*здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з права)*
*Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків,* Україна
*ORCID ID: https//0000-0002-9911-6374*
*e-mail: d.o.rasputnii95off@gmail.com*

**Науковий керівник**:
***Михайло ФІАЛКА,***
*кандидат юридичних наук, професор,*
*професор кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: https://orcid.org/0000-0001-5599-3335*
*e-mail: fialkami70@gmail.com*

# ДЕЯКІ ПИТАННЯ КРИМІНОЛОГІЧНОЇ ХАРАКТЕРИСТИКИ ОСІБ, ЯКІ ВЧИНЯЮТЬ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ПАЛИВНО-ЕНЕРГЕТИЧНОГО КОМПЛЕКСУ

У статті досліджено правові та кримінологічні особливості злочинності у сфері паливно-енергетичного комплексу України. Проаналізовано нормативно-правові засади функціонування об’єктів електроенергетики та особливості кримінально-правової охорони відповідних відносин. Особливу увагу приділено характеристиці кримінальних правопорушень проти власності, передбачених ст. 194-1 Кримінального кодексу України, а також особам, які їх вчиняють.

**Ключові слова:** паливно-енергетичний комплекс, електроенергетика, кримінологія, злочинність, розкрадання, пошкодження.

## SOME ISSUES OF THE CRIMINOLOGICAL CHARACTERISTICS OF PERSONS WHO COMMIT CRIMINAL OFFENSES IN THE FUEL AND ENERGY SECTOR

The article examines the legal and criminological features of crime in the field of the fuel and energy complex of Ukraine. It analyzes the regulatory and legal framework governing the functioning of electricity sector facilities and the specifics of criminal-law protection of the relevant relations. Special attention is paid to the characteristics of property-related criminal offenses under Article 194-1 of the Criminal Code of Ukraine, as well as to the individuals who commit them.

**Keywords:** fuel and energy complex, electricity sector, criminology, crime, theft, damage.

**Вступ**.

Питання вивчення особи, яка вчинила кримінальне правопорушення, у кримінологічній науці не є новим. На сучасному етапі її дослідженням займалися і продовжують займатися такі відомі вітчизняні та зарубіжні науковці, як О. І. Алєксєєв, Ю. М. Антонян, В. В. Голіна, Б. М. Головкін, І. М. Даньшин, В. Н. Кудрявцев, В. Є. Емінов, М. І. Фіалка та інші.

Правовий режим об'єктів електроенергетики визначено Законом України «Про ринок електричної енергії». Відповідно до законодавства, до об'єктів електроенергетики належать електростанції (крім ядерної частини атомної електричної станції), електричні підстанції, електричні мережі, установки зберігання електричної енергії [1].

Такі об'єкти формують технологічно взаємопов'язану систему: генерація → передача → розподіл → зберігання → постачання електричної енергії.

Крім того, інфраструктура України передбачає функціонування єдиної об'єднаної системи електропостачання. У зв'язку з цим, на нашу думку, доцільно розглянути кваліфікацію та зміст дій, що посягають на цілісність об'єктів електроенергетики.

**Викладення основного матеріалу**.

Кваліфікація кримінальних правопорушень у сфері електроенергетики здійснюється за критерієм предмета посягання. Зокрема, у разі впливу на матеріальні об'єкти електроенергетики діяння підлягає кваліфікації за спеціальною нормою — ст. 194-1 КК України, тоді як посягання на електричну енергію охоплюється ст. 188-1 КК України. У випадках, коли об'єкт не належить до енергетичної інфраструктури, але пов'язаний із паливно-енергетичним комплексом, пошкодження таких об'єктів кваліфікується за загальною нормою, передбаченою ст. 194 КК України, а викрадення відповідних компонентів — за ст. 185 КК України або ст. 186 КК України залежно від характеру вчинених дій.

Це підтверджується думкою та практикою того, що слід враховувати, що юрисдикційне розмежування у сфері електроенергетики здійснюється за критерієм правової природи. Зокрема, об'єкти електроенергетики виступають як матеріальні об'єкти цивільних прав та в приватному випадку права власності.

Зазначена норма свідчить про виокремлення об'єктів паливно енергетичного комплексу (далі — ПЕК) як об'єкту підвищеної кримінально-правової охорони, що зумовлено їх значенням для забезпечення національної безпеки, функціонування критичної інфраструктури та стійкості економіки держави.

Водночас у системі Особливої частини Кримінального кодексу України (далі — КК України) відповідні посягання формально віднесено до кримінальних правопорушень проти власності, що загалом є обґрунтованим, оскільки шкода завдається матеріальним об'єктам, які мають майнову цінність. Разом із тим коректно зазначити, що така кваліфікація не повною мірою відображає їх комплексну правову природу, адже фактично посягання зачіпає не лише відносини в контексті права власності, а й суспільні відносини у сфері забезпечення економічної та енергетичної безпеки.

Визначившись із кримінально-правовою характеристикою дій та об'єктів, що охороняються кримінальним законодавством, на нашу думку, доцільно перейти до кримінологічної характеристики осіб, які вчиняють діяння, кваліфіковані за ст. 194-1 КК України.

Кримінологічна характеристика особистості кримінального правопорушника. Слово «характеристика» походить від грецького «charakter», що у перекладі означає риса, особливість. Тобто характеристика — це опис, визначення відмінних, тобто специфічних рис, якостей чого-небудь [2, с. 164].

Тобто встановлення притаманних тому чи іншому явищу специфічних якостей.

К. Є. Ігошева зазначала: «Яка б конкретна особа не вивчалася, який би вид злочинної діяльності не розглядався, в усіх випадках, як і в кожному окремому, одиничному, в них виявляються риси і властивості загального порядку, котрі входять у характеристику злочинця як соціального типу» [3, с. 120].

Ми повністю погоджуємося з наведеними вище тезами, тож у подальшому більш детально розглянемо саме соціальні та біологічні характеристики особи кримінального правопорушника.

У межах розгляду кримінологічної характеристики злочинності у сфері ПЕК слід зазначити, що вона становить сукупність суспільно небезпечних діянь, які вчиняються у зв'язку з функціонуванням енергетичної інфраструктури та безпосередньо об'єктів електроенергетики.

У загальній структурі злочинності в комплексі ПЕК можна виокремити такі групи: розкрадання майна та енергетичних ресурсів, кримінальні правопорушення у сфері господарської діяльності, корупційні кримінальні правопорушення, умисні пошкодження інфраструктури, екологічні кримінальні правопорушення, необережні кримінальні правопорушення, що спричинили шкоду об'єктам ПЕК.

З урахуванням предмета дослідження особливого значення набувають кримінальні правопорушення проти власності, діяння, що кваліфікуються за ст. 194-1 КК України.

Детермінуючим чинником посягань на об'єкти електроенергетики в комплексі ПЕК переважно виступає саме корисливий фактор. Адже такого роду об'єкти містять значний обсяг товарно-матеріальних цінностей та мають істотне значення для системи суспільних відносин, що формуються внаслідок їх функціонування, і, як наслідок, становлять особливий інтерес для суб'єктів, які вчиняють кримінально карані діяння. Відповідно можна виокремити такі типи осіб:

а) учасники організованих груп, які вчиняють розкрадання обладнання та енергетичних ресурсів;

б) особи, що вчиняють епізодичні або ситуативні розкрадання, зокрема дрібні крадіжки та акти вандалізму;

в) особи, які завдають шкоди інфраструктурі без вираженої корисливої мотивації, наприклад з ідейних мотивів, із помсти або з хуліганських спонукань.

Зазначена класифікація має кримінологічний характер і відображає стійкі моделі кримінальної протиправної поведінки. Водночас цей перелік не є вичерпним, однак є достатнім.

У контексті дослідження питання кримінологічної характеристики осіб, які вчиняють посягання на об'єкти електроенергетики, доцільно визначити мотиваційну структуру кримінальної протиправної поведінки.

Аналіз правозастосовної практики свідчить про переважання корисливої мотивації у кримінальних правопорушеннях цієї категорії. Водночас мотиваційна структура не є однорідною та може включати прагнення до матеріального збагачення, соціальну адаптацію в девіантних групах, потребу в самоствердженні, вплив кримінально активного середовища, а також ситуативні чинники.

Підвищені матеріальні потреби, сформовані під впливом розриву між реальним економічним добробутом і соціальними очікуваннями, а також складні життєві обставини спонукають соціально та економічно незахищені верстви населення до вчинення кримінальних правопорушень, пов'язаних із пошкодженням об'єктів електроенергетики як предикатного кримінального правопорушення або як закінченого правопорушення з метою заволодіння майном, енергетичними чи іншими ресурсами.

Девіантна поведінка та антисуспільні установки формуються внаслідок недостатності загальносоціальних заходів запобігання злочинності, зокрема в аспекті виховання та нагляду за молодими особами. Таким чином, можна констатувати, що мотивація злочинної поведінки має комплексний і багаторівневий характер, де корисливий чинник, хоча й виступає певним стимулом, не завжди є першочерговим фактором.

Про обґрунтованість цього твердження можна судити, виходячи з того, що за звітний період 2024–2025 років за зазначеним видом правопорушень було зареєстровано 112 випадків,

з яких 7 були вчинені неповнолітніми, що становить приблизно 11,29 %. У 2024 році зафіксовано лише 1 випадок із 50 зареєстрованих, що становить 2 %.

У складі групи осіб у 2025 році було вчинено 12 правопорушень із 62, що становить близько 19,35 %. У 2024 році таких випадків не зафіксовано.

Факт рецидивної злочинності було встановлено у 7 випадках у 2025 році, тобто приблизно 11,29 %. Натомість у 2024 році зафіксовано лише 1 випадок із 50 зареєстрованих, що відповідає 2 % [4].

Тобто в окремих випадках, пов'язаних із пошкодженням об'єктів електроенергетики, зокрема вчиненням дій, кваліфікованих за ст. 194-1 КК України як предикатного правопорушення, або закінченого кримінального правопорушення, спостерігається певний рівень рецидиву та професіоналізації. Такі форми злочинності характеризуються стійкими зв'язками між учасниками, наявністю розподілу ролей та елементами організованості. Нерідко така протиправна діяльність виступає основним або єдиним джерелом доходу, що дозволяє розглядати її як частково інституціоналізовану форму кримінальної активності.

Натомість в інших видах злочинної діяльності у сфері ПЕК частка осіб із попередньою судимістю є низькою.

В особі злочинця притаманна система ознак, властивостей, якостей, що визначають її як людину, яка вчинила кримінальне правопорушення. Вітчизняні кримінологи поділяють основні ознаки особи злочинця на такі основні групи: соціально-демографічні, кримінально-правові, соціально-рольові, морально-психологічні характеристики. [5, с. 136].

Ці ознаки властиві будь-якій особі і самі пособі не мають кримінологічного значення. Проте у статистичній звітності стосовно осіб, які вчинили кримінальне правопорушення, соціально-демографічні ознаки дають важливу інформацію, без якої неможлива повна кримінологічна характеристика особи злочинців. [5, с. 136].

Соціально-демографічні характеристики злочинності у сфері паливно-енергетичного комплексу (ПЕК) характеризуються такими особливостями:

• Віковий діапазон охоплює як неповнолітніх, для яких характерне переважання актів вандалізму, спрямованих на самоствердження, так і осіб похилого та передпенсійного віку, у яких у зв'язку з погіршенням матеріального становища може виникати схильність до вчинення протиправних діянь.

• спостерігається виражене переважання чоловіків, що зумовлено професійною структурою галузі та характером середньої спеціальної освіти, де процес формування знань і навичок часто передбачає роботу з технікою та прикладними видами діяльності;

• значна частка правопорушників має технічну або спеціальну освіту, у окремих випадках — вищу. Окремі категорії кримінальних правопорушень потребують наявності професійних навичок і спеціалізації правопорушника, що свідчить про зв'язок злочинної активності з трудовою діяльністю та доступом до інфраструктури.

Слід зазначити, що в контексті жіночої злочинності «жіночими» сферами залишаються переважно «білокомірцеві» кримінальні правопорушення, тобто розкрадання цінних паперів, фальсифікація документації. Відповідно вплив жінок у статистиці правопорушень, кваліфікованих за ст. 194-1 КК України, є незначним.

**Висновки**.

У підсумку слід зазначити, що злочинність у сфері паливно-енергетичного комплексу України є складним соціально-правовим явищем, зумовленим сукупністю економічних, соціальних і професійних чинників. Переважання корисливої мотивації, високий рівень організованості окремих форм злочинної діяльності, а також наявність специфічних професійних компетенцій у суб'єктів правопорушень свідчать про домінування корисливого мотиву у посяганнях на об'єкти електроенергетики. Водночас не слід ігнорувати тенденцію до

зростання частки правопорушень, вчинених неповнолітніми, що обумовлює необхідність диференційованого підходу до запобігання та розслідування таких діянь.

Отже, кримінологічний портрет особи, яка вчиняє кримінальні правопорушення, передбачені ст. 194-1 КК України, характеризується як особа переважно чоловічої статі працездатного віку, яка часто не зайнята суспільно корисною працею та має середній або середньо-спеціальний рівень освіти, інколи — вищий. У випадках відсутності корисливого мотиву правопорушення можуть вчинятися у стані алкогольного сп'яніння та мати характер вандалізму або хуліганських дій. Натомість корисливо мотивовані діяння, як правило, відзначаються більш високим рівнем організованості, чіткістю дій та можуть вчинятися як одноособово, так і у складі організованих груп.

Аналіз статистичних даних дозволяє констатувати одночасне зростання як професіоналізованих форм злочинності, так і правопорушень, вчинених неповнолітніми. У зв'язку з цим доцільно умовно виділити дві вікові групи правопорушників: молодшу 14–21 рік, для якої більш характерні некорисливі мотиви, зокрема вандалізм та імпульсивні дії, та старшу 22–50 років, у межах якої переважають корисливі посягання, часто пов'язані з організованими формами злочинної діяльності. В інших випадках такі діяння здебільшого вчиняються одноособово.

**Список використаних джерел:**


1. Про ринок електричної енергії: ЗАКОН УКРАЇНИ від 25.03.2026 № 4825-IX від 25.03.2026 (Відомості Верховної Ради (ВВР), 2017, № 27-28, ст.312) URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text (дата звернення: 20.04.2026).
2. Фіалка, М. І. Кримінологічна характеристика та кримінологічний портрет особистості злочинця: сутність та співвідношення понять. *Вісник Кримінологічної асоціації України.* 2019. № 2 (21). С. 162-171. URL:
https://dspace.univd.edu.ua/server/api/core/bitstreams/aa0905b8-d49f-43c1-ae62-98fa247dcf9d/content
3. Головкін Б. М. Корислива насильницька злочинність в Україні: *феномен, детермінація, запобігання* : монографія. Харків : Право, 2011. 440 с. https://library.nlu.edu.ua/POLN_TEXT/MONOGRAFII_2013/Golovkin_2011.pdf
4. Єдиний звіт про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: статистична інформація Генеральної прокуратури України. Генеральна прокуратура України : офіц. сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
(дата звернення: 20.04.2026).
5. Шалгунова С. А., Орлеан А. М., Скок О. С., Шевченко Т. В., Крамаренко Ю. М., Барабаш Г. В., Волошина Ю. В., Шило І. В. / Кримінологія : навч. посібник-практикум (для здобувачів вищоїосвіти, що навчаються на першому (бакалаврському) рівні вищої освіти(081 «Право», 262 «Правоохоронна діяльність») / за заг. ред. к.ю.н., доц. С. А. Шалгунової. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. 332 с. URL:
https://er.dduvs.edu.ua/bitstream/123456789/5157/1/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F.pdf

https://doi.org/10.5281/zenodo.20498228

***Артем РИКОВ,***
*здобувач вищої освіти другого року навчання,*
*спеціальність 103 Науки про Землю, третій освітньо-науковий рівень доктор PhD*
*кафедри геоінформаційних технологій та космічного моніторингу Землі*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: https://orcid.org/0009-0001-4568-7112*
*e-mail: a.m.rykov@khai.edu*

**Науковий керівник**:
***Людмила СУХОМЛІН,***
*кандидат економічних наук, доцент кафедри геоінформаційних технологій та космічного моніторингу Землі Національного аерокосмічного університету «Харківський авіаційний інститут»*
*м. Харків, Україна*
*ORCID: https://orcid.org/0009-0005-7971-8289*
*e-mail: mailto:l.sukhomlin@khai.edu*

# ОСОБЛИВОСТІ ФУНКЦІЮВАННЯ ДЕРЖАВНОГО ЕЛЕКТРОННОГО РЕЄСТРУ РЕЧОВИХ ПРАВ НА НЕРУХОМЕ МАЙНО В УМОВАХ ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

Анотація. Розглянуто правила та закони, що регулюють роботу державного електронного реєстру нерухомого майна України. Це відбувається в умовах військового стану. Проаналізовані рішення мали на меті захист від незаконного впливу. Цей захист стосувався зміни прав державних інтересів, фізичних та юридичних осіб. Він був потрібен через загрозу їхньому життю та здоров'ю, а також користувачам реєстрів з боку агресорів.

Ключові слова: військовий стан, електронні реєстрі, обмеження, заборона.

# PECULIARITIES OF THE FUNCTIONING OF THE STATE ELECTRONIC REGISTER OF PROPERTY RIGHTS TO IMMOVABLE PROPERTY UNDER MARTIAL LAW IN UKRAINE

Abstract. The normative and legal support function of the Ukraine state electronic registers in the conditions of martial law is considered. The analyzed decisions were aimed to protecting against illegal and unauthorized influence of the changing the rights of the state, individuals, legal interest's entities due to threats to their lives and health, both themselves and users of registers by aggressors.

Keywords: martial law, electronic registers, restrictions, prohibition.

**Вступ.**

В Україні розвивається інформаційне суспільство. Державні послуги стають більш доступними завдяки інформатизації. Тому були створені електронні реєстри. Електронний реєстр – це автоматизована система для обліку інформації. Вона містить дані про людей, майно та документи. Держава створює та веде ці реєстри для виконання своїх завдань [1]. Насамперед метою їх створення було захист прав та інтересів фізичних та юридичних осіб. Державний реєстр веде уповноважений орган. Це робиться для накопичення та обробки інформації. Також

реєстр потрібен, щоб надати певним відомостям офіційного визнання [1]. Так, наприклад, відповідно до Закону України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» державна реєстрація речових прав на нерухоме майно та їх обтяжень це – офіційне визнання і підтвердження державою фактів набуття, зміни або припинення речових прав на нерухоме майно, обтяжень таких прав шляхом внесення відповідних відомостей до Державного реєстру речових прав на нерухоме майно. Відомості, що містяться у Державному реєстрі прав, повинні відповідати відомостям, що містяться в документах, на підставі яких проведені реєстраційні дії. У разі невідповідності даних, головними є відомості з документів. Реєстраційні дії проводяться на підставі цих документів [1]. Порядок ведення Державного реєстру визначає Кабінет Міністрів України. Це включає вимоги до документів і взаємодію з іншими реєстрами. Він встановлений Постановою від 25 грудня 2015 року. № 1127 (з подальшими змінами) [5].

**Викладення основного матеріалу.**

У зв'язку з введенням воєнного стану урядом України внесені ряд коректив у діяльність щодо надання адміністративних послуг, так відповідно до Постанови Кабінету Міністрів України від 6 березня 2022 р. № 209 «Про деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану» запроваджено тимчасові обмеження доступу до єдиних та державних реєстрів Міністерства юстиції України та проведення реєстраційних дій на територіях активних бойових дій і тимчасово окупованих територіях, а також нотаріусами, робочі місця яких розташовані в межах відповідних адміністративно-територіальних одиниць (п. 1, 2 [2]). Такі заходи мали на меті захистити державні інформаційні ресурси. Також вони мали зменшити ризики несанкціонованого втручання в їхню роботу під час воєнного стану. А саме, Єдиний державний реєстр нормативно-правових актів; Реєстр спеціальних бланків документів інформаційної системи Міністерства юстиції України; Єдиний реєстр спеціальних бланків нотаріальних документів; Єдиний реєстр нотаріусів України, Спадковий реєстр; Єдиний реєстр довіреностей; Державний реєстр обтяжень рухомого майна; Єдиний реєстр громадських формувань; Реєстр атестованих судових експертів; Реєстр методик проведення судових експертиз; Єдиний державний реєстр осіб, які вчинили корупційні правопорушення; Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство; Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань; Реєстр громадських об’єднань; Державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб’єктів інформаційної діяльності; Єдиний реєстр громадських формувань; Державний реєстр актів цивільного стану громадян; Державний реєстр речових прав на нерухоме майно [2,6].

Також, щоб захистити життя та здоров'я суддів і учасників судового процесу під час воєнного стану, доступ до Єдиного державного реєстру судових рішень тимчасово призупинено. Крім того, призупинено роботу сервісу «Стан розгляду справ».

Наступна Постанова Кабінету Міністрів України від 19 квітня 2022 № 480 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо діяльності нотаріусів та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану» частково розблокувала роботу державних реєстрів, зокрема Державний реєстр речових прав на нерухоме майно. Доступ до реєстрів та внесення змін мають лише державні реєстратори. Також це можуть робити посадові особи Мін’юсту та нотаріуси (державні та приватні). Але деякі дії доступні тільки нотаріусам зі спеціального переліку. Цей перелік визначає нотаріусів, які можуть працювати з цінним майном під час

воєнного стану. Передбачені територіальні обмеження. Робота реєстрів розблокована тільки в тих регіонах, де не відбуваються бойові дії [3].

Відповідно до п. п.18 Ст.1 та п.4. Ст. 9 Закону України «Про критичну інфраструктуру» зазначено, що електронні реєстри є об'єктами критичної інфраструктури. Вони містять перелік інформації, яка є найбільш важливою для нормального функціонування суспільства та держави [4]. Тому у відповідних рішеннях Кабінету міністрів України щодо обмежень функціонування державних електронних реєстрів була закладена мета убезпечити від незаконного та несанкціонованого впливу на зміну прав державних інтересів, фізичних та юридичних осіб через загрозу їх життю та здоров'ю з боку агресорів так і до уповноважених осіб реєстраторів. А також через використання несприятливих обставин для фізичних та юридичних осіб зі сторони уповноважених осіб реєстраторів.

**Висновки.**

Взаємозв'язок Державного реєстру речових прав на нерухоме майно з платформою «Дія» в умовах воєнного стану базується на аналізі нормативних актів та офіційних роз'яснень. Зокрема, з початку повномасштабного вторгнення (з 24 лютого 2022 року) Міністерство юстиції України тимчасово призупинило доступ до державних реєстрів, включаючи Державний реєстр речових прав на нерухоме майно, для запобігання витоку даних та забезпечення кібербезпеки (відповідно до Постанови КМУ від 06.03.2022 № 209 «Деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану»). Це безпосередньо вплинуло на електронні послуги в «Дії», оскільки платформа працює на основі автоматизованої взаємодії з реєстрами: дані про нерухоме майно, витяги, реєстрацію бізнесу та інші сервіси витягуються саме з них [2].

**Список використаних джерел:**


1. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень: Закон України від 01.07.2004 № 1952-IV URL: https://zakon.rada.gov.ua/laws/show/1952-15#Text
2. Про деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану: Постанова Кабінету Міністрів України від 6 березня 2022 р. № 209 URL: https://zakon.rada.gov.ua/laws/show/209-2022-%D0%BF#Text
3. Постанова Кабінету Міністрів України від 19 квітня 2022 № 480 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо діяльності нотаріусів та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану» URL: https://www.kmu.gov.ua/npas/pro-vnesennya-zmin-do-deyakih-postanov-kabinetu-ministriv-ukrayini-480-190422
4. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень: Постанова Кабінету Міністрів України від 25 грудня 2015 р. № 1127 (з подальшими змінами). Цей акт встановлює порядок державної реєстрації, вимоги до документів та взаємодію з реєстрами, включаючи особливості в умовах воєнного стану. URL: https://zakon.rada.gov.ua/laws/show/1127-2015-%D0%BF#Text
6. Єдині та Державні реєстри: Офіційний веб-сайт Міністерства юстиції України. URL: https://minjust.gov.ua/m/edini-ta-derjavni-reestri.

https://doi.org/10.5281/zenodo.20498250

***Володимир СЕЛЕВКО***,
*кандидат філософських наук, доцент,*
*доцент кафедри права Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID: https://orcid.org/0000-0002-9543-4981*
*e-mail: v.selevko@khai.edu*

***Станіслав КРАВЧЕНКО,***
*доктор філософії (PhD),*
*старший викладач кафедри аерогідродинаміки*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID ID: https://orcid.org/0009-0009-6409-4767*
*e-mail: s.kravchenko@khai.edu*

# ПРАВОВЕ РЕГУЛЮВАННЯ ВПРОВАДЖЕННЯ ТА ЕКСПЛУАТАЦІЯ ГАЗОТУРБІННИХ ТА ДИЗЕЛЬНИХ ГЕНЕРАТОРНИХ УСТАНОВОК В УМОВАХ ВОЄННОГО СТАНУ

**Анотація:** В тезах розглянуто важливість правового регулювання розвитку когенераційної та блочно-модульної енергетики в умовах воєнного стану в Україні. Проаналізовано вплив воєнного періоду на енергетичну безпеку країни, зокрема при наявності залежності від зовнішніх негативних обставин. Визначено, що розвиток децентралізованої енергетики може сприяти стійкості енергетичної системи та забезпечити енергетичну незалежність. Висвітлені потенційні проблеми та ризики, які можуть виникати у зв'язку з терміновим введенням в експлуатацію та масовому застосуванню автономних рішень когенераційної енергетики в умовах воєнного стану. Запропоновані практичні рекомендації з подолання цих перешкод через внесення змін та доповнень до нормативно-правових актів.
**Ключові слова:** військовий стан, правове регулювання, децентралізована енергетика, газотурбінні та дизельні генеруючі установки, енергетична безпека, технічна безпека.

## LEGAL REGULATION OF THE IMPLEMENTATION AND OPERATION OF GAS TURBINE AND DIESEL GENERATING UNITS IN MARTIAL ARTS CONDITIONS

**Abstract:** The conference theses considered the importance of legal regulation of the development of cogeneration and block-modular energy in the conditions of martial law in Ukraine. The impact of the war period on the country's energy security was analyzed. It was determined that the development of decentralized energy can contribute to the stability of the energy system. Potential problems and risks that may arise in connection with the urgent commissioning and mass application of autonomous cogeneration energy solutions were highlighted. Practical recommendations were proposed to overcome these obstacles by making amendments and additions to regulatory legal acts.
**Keywords:** martial law, legal regulation, decentralized energy, gas turbine and diesel generating sets, energy security, technical security.

**Вступ.**

Забезпечення безперебійного електропостачання є одним із ключових завдань енергетичної безпеки держави. Системні атаки на енергетичну інфраструктуру України, що тривають з 2022 року, призвели до суттєвого скорочення генеруючих потужностей та формування сталого дефіциту електроенергії, який у пікові періоди може сягати кількох ГВт

[1, с. 1]. Наслідком цього є застосування графіків обмеження споживання та аварійних відключень, що негативно впливають на функціонування критично важливої інфраструктури, зокрема лікарень, об'єктів соціальної сфери, підприємств із безперервним циклом виробництва, тощо. Розвиток розподіленої генерації є ключовим напрямом підвищення стійкості енергосистеми України в умовах воєнних ризиків.

**Викладення основного матеріалу.**

В даних умовах особливої актуальності набуває використання мобільних та модульних енергетичних рішень, здатних оперативно компенсувати дефіцит потужності для окремих об'єктів. Одним із ефективних рішень є впровадження розподіленої генерації, зокрема блочних електростанцій потужністю до 5 МВт безпосередньо на місцях споживання. До таких установок належать газотурбінні агрегати малої потужності, що характеризуються високою питомою потужністю, швидким запуском та забезпечують відносну автономність [2, с. 2] та дизельні генератори, перевагами яких є швидке введення в експлуатацію, гнучкість у використанні, простота експлуатації та повна автономність [3, с. 2].

Нагальна потреба у швидкому впровадженні таких джерел живлення зумовила необхідність спрощення процедур їх встановлення та підключення. Це знайшло відображення у нормативних актах Кабінету Міністрів України. Зокрема, постанові Кабінету Міністрів України від 07.12.2023 № 1320 «Про деякі питання будівництва та/або відновлення, та/або реконструкції, та/або розміщення, та/або капітального ремонту газопоршневих та газотурбінних установок, зокрема когенераційних, блочно-модульних котелень, дизельних/бензинових та газових генераторів, об'єктів газосховищ, нафтогазовидобування, деяких об'єктів газотранспортної системи та ліній електропередачі системи передачі, на період воєнного стану», згідно якому установлено, що на період воєнного стану будівництво та/або розміщення суб'єктами господарювання газопоршневих та газотурбінних установок, зокрема когенераційних, блочно-модульних котелень, дизельних/бензинових та газових генераторів, установок зберігання енергії, ліній електропередачі системи передачі, а також пов'язаних з ними мереж електро-, тепло-, газо-, водопостачання, вузлів обліку, іншого пов'язаного обладнання, необхідного для забезпечення тепловою та/або електричною енергією об'єктів критичної інфраструктури (теплопостачання, водопостачання, водовідведення), закладів соціальної сфери (навчальних закладів, закладів охорони здоров'я), споживачів, зокрема під час застосування графіків відключення споживачів, будівництво та/або розміщення суб'єктами господарювання газопоршневих та/або газотурбінних установок, розташованих на суднах технічного флоту (спеціалізованих суднах) та призначених для виробництва електричної енергії, та будівництво мереж електро-, тепло-, газо-, водопостачання, вузлів обліку, іншого пов'язаного обладнання, що здійснюється операторами таких мереж з метою створення можливості підключення суб'єктами господарювання газопоршневих та/або газотурбінних установок здійснюється без: відповідної містобудівної документації; отримання містобудівних умов та обмежень забудови земельної ділянки; отримання звіту про результати проведення експертизи проектної документації на будівництво об'єктів; отримання права на виконання будівельних робіт; використання Єдиної державної електронної системи у сфері будівництва; схем теплопостачання населених пунктів; відведення земельних ділянок під об'єкт енергетики; відведення і погодження земельних ділянок під траси ліній електропередачі, газопостачання та водопостачання у разі приєднання до мереж [4].

Будівельні роботи можуть проводитися одночасно з розробленням проектної документації [4].

Початок експлуатації газопоршневих та газотурбінних установок, зокрема когенераційних, блочно-модульних котелень, дизельних/ бензинових та газових генераторів, установок зберігання енергії, ліній електропередачі системи передачі, а також пов'язаних з ними газових та електричних мереж, вузлів обліку, іншого пов'язаного обладнання, а також газопоршневих та/або газотурбінних установок, розташованих на суднах технічного флоту (спеціалізованих суднах), мереж електро-, тепло-, газо-, водопостачання, вузлів обліку, іншого пов'язаного обладнання, що будується/реконструюється операторами таких мереж з метою створення можливості підключення суб'єктами господарювання газопоршневих та/або газотурбінних установок, розташованих на суднах технічного флоту (спеціалізованих суднах) здійснюється без сертифіката про прийняття в експлуатацію закінченого будівництвом об'єкта, виданого відповідно до законодавства у сфері містобудівної діяльності, за умови проведення комплексних випробувань електроустановок в обсягах, передбачених галузевими нормативними документами [4].

Наступним нормативним документом стало розпорядження Кабінету Міністрів України від 18.07.2024 № 713-р схвалено Стратегію розвитку розподіленої генерації на період до 2035 року, якою визначено необхідність розвитку локальних джерел електроенергії та підвищення стійкості енергосистеми [5].

Додатково технічні аспекти приєднання генеруючих установок до електричних мереж були уточнені у нормативних актах НКРЕКП, зокрема постановою від 28.10.2025 № 1730, яка передбачає внесення змін до Кодексу систем розподілу та Кодексу системи передачі з метою спрощення приєднання генеруючих установок [6].

Таким чином, розвиток розподіленої генерації та спрощення процедур підключення локальних електростанцій є одним із ключових напрямів підвищення енергетичної стійкості України. Використання блочних генераторів потужністю до 5 МВт дозволяє забезпечити безперебійне електропостачання критично важливих об'єктів та зменшити залежність від централізованої енергосистеми в умовах кризових впливів.

Однак необхідно враховувати, що експлуатація газотурбінних [7, с. 3] та дизельних [8, с. 4] генераторних установок, особливо в умовах спрощеного введення в експлуатацію та їх масового розміщення поблизу об'єктів критичної інфраструктури, супроводжується комплексом технічних ризиків та ризиків впливу на людину і довкілля (див. таб. 1).

Таблиця 1

Основні ризики експлуатації генераторних установок та заходи їх мінімізації

| **Група ризиків** | **Опис ризику** | **Наслідки** | **Заходи мінімізації** |
|---|---|---|---|
| Технічні | Чутливість газотурбінних установок до якості палива | Зниження ККД, знос турбіни, аварійні зупинки | Контроль якості палива, фільтрація, регулярна діагностика |
| Технічні | Робота при змінних навантаженнях | Перевитрата палива, зниження ефективності | Оптимізація режимів роботи, використання систем автоматичного регулювання |
| Технічні | Недостатні пусконалагоджувальні випробування | Некоректна робота систем захисту, аварії | Повноцінне тестування навіть при спрощеному введенні в експлуатацію |
| Технічні | Порушення синхронізації з енергосистемою | Коливання частоти та напруги | Використання сучасних систем синхронізації та АСК |

| | | | |
|---|---|---|---|
| Людина / довкілля | Підвищений рівень шуму | Стрес, порушення сну, зниження працездатності | Шумоізоляційні кожухи, акустичні екрани, контейнерне виконання |
| Людина / довкілля | Викиди продуктів згоряння: $NO + NO_2$, CO, $PM_{2,5}$ / $PM_{10}$ (тверді частинки) | Погіршення якості повітря, вплив на здоров'я | Каталітичні нейтралізатори, фільтри, низькоемісійні пальники |
| Людина / довкілля | Теплове та вібраційне навантаження | Дискомфорт персоналу, знос конструкцій | Віброізоляція, вентиляція, тепловідведення |
| Людина / довкілля | Невдале розміщення поблизу житлових зон | Вплив на населення, екологічні скарги | Санітарно-захисні зони, правильне планування розміщення |
| Системні | Масове підключення розподіленої генерації | Дисбаланс потужності, коливання частоти | Координація з оператором системи, диспетчеризація, балансування |

До **технічних ризиків** відносяться наступні:

По-перше, для газотурбінних установок характерна висока чутливість до якості палива та стабільності режимів роботи. Відхилення складу газу або наявність домішок можуть призводити до зниження ефективності, перегріву елементів турбіни та прискореного зносу лопатевого апарату.

По-друге, як газотурбінні, так і дизельні генератори мають обмежену ефективність при роботі в змінних або частково навантажених режимах, що є типовим для аварійних та резервних систем енергозабезпечення. Це призводить до підвищеної витрати палива та зниження загального коефіцієнта корисної дії.

По-третє, спрощене введення в експлуатацію може створювати ризики, пов'язані з недостатнім обсягом пусконалагоджувальних випробувань, що підвищує ймовірність некоректної роботи систем автоматичного захисту, синхронізації з мережею та регулювання навантаження.

Окремо слід відзначити ризики інтеграції в енергосистему, зокрема виникнення локальних дисбалансів потужності, коливань частоти та напруги у разі одночасного підключення великої кількості розподілених джерел генерації без належної координації.

Розглянемо ***ризики впливу на людину та навколишнє середовище***.

Одним із ключових факторів є шумове навантаження. Газотурбінні та дизельні установки створюють високий рівень шуму під час роботи, який без застосування шумоізоляційних рішень може перевищувати допустимі санітарні норми. Це може спричиняти хронічний стрес, втому, порушення сну та зниження концентрації уваги у персоналу, що перебуває поблизу обладнання.

Другим важливим фактором є викиди продуктів згоряння. Дизельні установки є джерелом оксидів азоту, твердих частинок та оксиду вуглецю, що негативно впливають на якість повітря. Газотурбінні установки мають нижчий рівень викидів, однак також можуть продукувати оксиди азоту, особливо при змінних навантаженнях. У разі концентрації таких джерел у міських районах це створює локальні екологічні ризики.

Третім фактором є тепловий вплив та вібрація, які можуть негативно впливати як на персонал, так і на будівельні конструкції при недостатній ізоляції обладнання.

З метою ***запобігання та зниження вищезазначених ризиків*** рекомендується впровадження наступних заходів:

Для зниження технічних ризиків необхідним є впровадження системи повноцінного технічного контролю, включаючи регулярний моніторинг параметрів роботи, діагностику стану обладнання та автоматизовані системи захисту. Обов'язковим є проведення розширених пусконалагоджувальних випробувань навіть у разі спрощених процедур введення в експлуатацію.

Для зменшення впливу на людину доцільно застосовувати шумопоглинаючі кожухи, контейнерні виконання генераторів та акустичні екрани, що дозволяють знизити рівень шуму до нормативних значень.

З метою зменшення викидів слід використовувати системи очищення вихлопних газів, зокрема каталітичні нейтралізатори та фільтри твердих частинок для дизельних установок, а також низькоемісійні технології згоряння для газотурбінних систем.

Важливим є також раціональне розміщення генераторних установок, з урахуванням санітарно-захисних зон та віддалення від житлової забудови, а також забезпечення ефективної вентиляції та тепловідведення.

Додатково слід впроваджувати системи постійного екологічного та технічного моніторингу, які дозволяють контролювати рівень шуму, викидів, температурних режимів та вібрацій у режимі реального часу.

**Висновки.**

Таким чином, експлуатація газотурбінних і дизельних генераторних установок є ефективним інструментом забезпечення енергетичної стійкості, що однак потребує системного підходу до управління як технічними ризиками, так і ризиками впливу на людину та довкілля. Тільки комплексна реалізація заходів безпеки дозволяє забезпечити їх надійну та безпечну експлуатацію та (за необхідності) інтеграцію в енергетичну систему.

Вищезазначене, у свою чергу, вимагає відповідних змін та доповнень нормативно-правових актів. У контексті воєнного стану правове регулювання децентралізованої енергетики набуває великої важливості та актуальності. Вирішення даної нагальної потреби вимагає збалансованого підходу: з одного боку – прискорене забезпечення енергетичної незалежності локальних об'єктів від об'єднаної енергетичної системи країни за рахунок спрощеного введення в експлуатацію автономних енергетичних установок, з іншого – забезпечення їх безпечної експлуатації, та (за необхідністю) їх безпечна інтеграція у цю об'єднану систему.

Вищенаведене зумовлює необхідність розроблення та впровадження конкретних регламентів, що визначають нормативно-правове і технічне регулювання введення в експлуатацію автономних енергетичних установок та їх інтеграції в об'єднану енергосистему України. Окрім того, правове середовище повинно сприяти стимулюванню інвестицій у галузь виробництва газотурбінних та дизельних генераторних установок.

**Список використаних джерел:**

1. Проходження осінньо-зимового періоду 2024–2025. Стан енергосистеми: аналітика DiXi Group [Електронний ресурс]. URL: https://dixigroup.org/analytic/prohodzhennya-osinno-zymovogo-periodu-2024-2025/ (дата звернення: 20.04.2026).

2. Ejenavi O. W., Salisu S. I. Energy analysis of a gas turbine generator (a case study of 3 × 2.5 MW Centaur 40), 2019. URL: https://doi.org/10.21276/sjet (дата звернення: 20.04.2026).

3. Irianti B., Andriyanti A. D. N. Performance analysis of a 2 MW diesel engine generator as an additional power plant at PT Indolakto Purwosari // Indonesian Journal of Advanced Research. 2024. Vol. 3, No. 7. URL: https://doi.org/10.55927/ijar.v3i7.10333 (дата звернення: 20.04.2026)

4. Постанова Кабінету Міністрів України від 07.12.2023 № 1320 Про деякі питання будівництва та/або відновлення, та/або реконструкції, та/або розміщення, та/або капітального ремонту газопоршневих та газотурбінних установок, зокрема когенераційних, блочно-модульних котелень, дизельних/бензинових та газових генераторів, об'єктів газосховищ, нафтогазовидобування, деяких об'єктів газотранспортної системи та ліній електропередачі системи передачі, на період воєнного стану URL: https://zakon.rada.gov.ua/laws/show/1320-2023-%D0%BF#Text (дата звернення: 20.04.2026).

5. Про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року: Розпорядження Кабінету Міністрів України від 18.07.2024 № 713-р. URL: https://zakon.rada.gov.ua/go/713-2024-р (дата звернення: 20.04.2026).

6. Про внесення змін до Кодексу систем розподілу та Кодексу системи передачі: Постанова НКРЕКП від 28.10.2025 № 1730. URL: https://zakon.rada.gov.ua/go/v1730874-25 (дата звернення: 20.04.2026).

7. ISO 21789:2022 Gas turbine applications – Safety Published (Edition 2, 2022). https://www.iso.org/standard/74201.html (дата звернення: 20.04.2026).

8. Issa, M.; Ibrahim, H.; Hosni, H.; Ilinca, A.; Rezkallah, M. Effects of Low Charge and Environmental Conditions on Diesel Generators Operation. Eng 2020, 1, 137-152. https://doi.org/10.3390/eng1020009 (дата звернення: 20.04.2026).

https://doi.org/10.5281/zenodo.20498278

***Ганна ТИРГОАЛЕ,***
*студентка 5 курсу група 759д,*
*гуманітарного-правового факультету*
*Національного аерокосмічного університету*
*м. Харків, Україна*
*e-mail: h.o.tyrhoale@student.khai.edu,*

Науковий кервник:
***Світлана ГУЦУ,***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*м. Харків, Україна*
*ORCID: https://orcid.org/0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

## ПОРТАЛ «ДІЯ» ЯК ІНСТРУМЕНТ ПУБЛІЧНО-ПРАВОВОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: СТАН ТА ПЕРСПЕКТИВИ

**Анотація:** У тезах досліджується ключова роль єдиного державного порталу електронних послуг «Дія» як фундаментального елемента цифрової публічної інфраструктури в контексті забезпечення стійкості, безперервності управління та захисту критичної інфраструктури України. Здійснено комплексний аналіз чинної правової бази функціонування порталу та його критичного значення для стабільного надання публічних та адміністративних послуг населенню в умовах воєнного стану, спричиненого збройною агресією. Детально розглядаються сучасні гібридні загрози кібербезпеці, яким систематично піддається платформа, а також оцінюються наявні механізми їх правового врегулювання. На основі аналізу європейського досвіду обґрунтовується нагальна необхідність законодавчого визнання цифрових сервісів публічного управління повноцінними об'єктами критичної інфраструктури. Зроблено висновок про потребу формування комплексного публічно-правового підходу до кіберзахисту подібних платформ, що є необхідною умовою забезпечення національної безпеки та подальшої євроінтеграції.

**Ключові слова:** критична інфраструктура; портал «Дія»; цифрові публічні послуги; кібербезпека; публічне управління; воєнний стан; електронне урядування.

## THE «DIA» PORTAL AS AN INSTRUMENT OF PUBLIC-LAW PROTECTION OF UKRAINE'S CRITICAL INFRASTRUCTURE: CURRENT STATE AND PROSPECTS

**Abstract:** The article examines the key role of the «Diia» unified state web portal of electronic services as a fundamental element of digital public infrastructure in the context of ensuring the resilience, continuity of governance, and protection of Ukraine's critical infrastructure. A comprehensive analysis of the current legal framework governing the portal's operation and its critical significance for the stable provision of public and administrative services under martial law is conducted. The modern hybrid cybersecurity threats to which the platform is systematically exposed are examined in detail, along with an evaluation of existing legal mechanisms for their regulation. Based on European experience, the urgent necessity of legislative recognition of digital

public administration services as objects of critical infrastructure is substantiated. The conclusion is drawn about the need for a comprehensive public-law approach to protecting such platforms under conditions of hybrid warfare, which is a necessary condition for European integration.

**Keywords:** critical infrastructure; Diia portal; digital public services; cybersecurity; public administration; martial law; e-governance.

**Вступ.**

Цифровізація державного управління в Україні протягом останніх років досягла значного рівня розвитку, що стало можливим завдяки запровадженню порталу «Дія» — єдиного державного веб-порталу електронних послуг. Цей ресурс функціонує відповідно до положень Закону України «Про адміністративні послуги» та Постанови Кабінету Міністрів України від 04.12.2019 № 1137 «Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг» [1]. Починаючи з 2020 року, зазначена платформа забезпечує громадянам зручний та прозорий доступ до понад 130 послуг адміністративних послуг у режимі онлайн, а однойменний мобільний застосунок надає повну юридичну силу цифровим копіям особистих документів громадян.

**Викладення основного матеріалу.**

З початком повномасштабного вторгнення російської федерації на територію України у лютому 2022 року портал «Дія» вийшов за межі звичайного інструменту спрощення бюрократичних процедур. Він набув стратегічного значення для забезпечення життєдіяльності та безперервного функціонування держави в екстремальних умовах воєнного стану. В умовах масової внутрішньої та зовнішньої міграції, руйнування фізичних Центрів надання адміністративних послуг (ЦНАП) та втрати громадянами паперових документів, цифрова інфраструктура стала чи не єдиним надійним містком між державою та суспільством. Запровадження таких сервісів, як «єДокумент», подання заявок на компенсацію за пошкоджене майно («єВідновлення»), а також реєстрація внутрішньо переміщених осіб здійснювалися саме через цей портал, що засвідчує його критичну роль в управлінні державою під час війни.

У ширшому контексті інформаційної безпеки функціонування цифрових платформ публічного управління, зокрема порталу Дія, слід розглядати як складову національної безпеки, що охоплює не лише технічний захист інформаційних систем, а й гарантування цілісності, конфіденційності та доступності інформації [2]. Інформаційна безпека у цьому сенсі поєднує правові, організаційні та технологічні механізми, спрямовані на запобігання несанкціонованому доступу, витоку даних, маніпуляціям інформацією та підриву довіри до державних інститутів. Особливого значення набуває питання забезпечення стійкості до інформаційно-психологічних впливів, що можуть супроводжувати кібератаки та використовуватися як елемент гібридної війни.

Водночас розвиток електронного урядування актуалізує проблему інформаційної безпеки особистості [3]. Використання цифрових документів, електронної ідентифікації та доступ до державних реєстрів через «Дію» передбачає обробку значного обсягу персональних даних, що підвищує ризики їх неправомірного використання або компрометації. У цьому контексті ключового значення набуває дотримання вимог законодавства про захист персональних даних, а також впровадження принципів privacy by design та privacy by default у процесі розроблення і функціонування цифрових сервісів.

Окремої уваги потребує питання інформованості користувачів щодо ризиків, пов’язаних із використанням цифрових сервісів. Інформаційна безпека особистості включає не лише технічний захист з боку держави, але й формування належного рівня цифрової

грамотності громадян, їх здатності ідентифікувати кіберзагрози (фішинг, соціальну інженерію, шахрайські схеми) та відповідально поводитися з власними даними. У цьому сенсі держава має поєднувати розвиток цифрових сервісів із просвітницькими заходами у сфері кібергігієни. Таким чином, забезпечення інформаційної безпеки у функціонуванні платформи «Дія» має комплексний характер і охоплює як макрорівень (захист державних інформаційних систем і цифрового суверенітету), так і мікрорівень (захист прав та інтересів конкретної особи). Баланс між зручністю цифрових сервісів і належним рівнем безпеки персональних даних виступає ключовою умовою довіри до електронного урядування та його подальшого розвитку.

З публічно-правової точки зору, статус порталу «Дія» потребує глибшого аналізу через призму законодавства про національну безпеку. Відповідно до статті 9 Закону України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX, до переліку життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки, економіки, соціальної сфери чи навколишнього природного середовища, належать, серед іншого, урядування та надання найважливіших публічних послуг, інформаційні послуги та електронні комунікації [4]. Водночас законодавство передбачає окрему процедуру ідентифікації та категоризації об’єктів критичної інфраструктури, яка здійснюється за визначеними критеріями.

Аналіз функціональних можливостей порталу Дія дає підстави стверджувати, що він одночасно виконує інформаційні, комунікаційні, адміністративні та управлінські функції, які за своїм змістом відповідають ознакам систем, порушення роботи яких може суттєво впливати на соціально-економічну стабільність держави. Водночас формальне віднесення порталу або його окремих компонентів до об’єктів критичної інфраструктури здійснюється в межах спеціальної процедури, результати якої не завжди підлягають публічному розкриттю. У зв’язку з цим більш обґрунтованим є підхід, за якого акцент робиться не на відсутності відповідного правового статусу, а на недостатній визначеності критеріїв і підходів до класифікації комплексних державних цифрових систем у цій сфері.

Це створює суттєву правову прогалину у сфері його комплексного захисту. Практика функціонування платформи в умовах гібридної війни довела абсолютну реальність кіберзагроз: ще напередодні та в перші дні повномасштабного вторгнення (у лютому 2022 року) портал зазнав безпрецедентних за масштабом масованих DDoS-атак з боку російських хакерських угруповань, метою яких був колапс державного апарату [5].

На сьогодні базовою правовою основою протидії таким загрозам виступає Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [6]. Однак його норми мають переважно рамковий характер і не передбачають деталізованого спеціального режиму захисту саме для масштабних цифрових сервісів публічного управління, що перебувають під особливим екстремальним навантаженням у воєнний час.

Варто зазначити, що на практиці забезпечення кіберзахисту державних цифрових сервісів, включаючи портал «Дія», здійснюється із застосуванням комплексу організаційних і технічних заходів, зокрема резервування інфраструктури, використання хмарних технологій, а також взаємодії з суб’єктами національної системи кібербезпеки. Однак такі механізми переважно закріплені на рівні підзаконного регулювання та адміністративної практики, що зумовлює потребу у більш системному та прозорому нормативному врегулюванні. Відсутність імперативних норм щодо обов’язкового резервування потужностей, специфічних протоколів кризового реагування для «Дії» та гарантій фінансування її безпекових потреб як об’єкта критичної інфраструктури створює ризики для інформаційного суверенітету держави.

У цьому контексті надзвичайно корисним є аналіз закордонного досвіду, зокрема країн-лідерів у сфері електронного урядування. Практика свідчить, що Естонська Республіка, чия інфраструктура обміну даними X-Road стала прототипом для багатьох українських рішень, ще у 2011 році включила ключові державні е-сервіси до закритого переліку об'єктів критичної інфраструктури. Хоча X-Road не є прямим аналогом українського порталу, відповідний підхід до визначення критичності цифрових сервісів та їх захисту свідчить про важливість інтегрованого нормативного регулювання. Такий публічно-правовий підхід дозволив Естонії забезпечити високий рівень стійкості (resilience) та безперервне функціонування державних систем навіть в умовах системних кіберінцидентів [7].

Аналогічний концептуальний підхід наразі закріплений і на рівні законодавства Європейського Союзу. Зокрема, ухвалена Директива ЄС NIS2 (Directive (EU) 2022/2555) [8], спрямована на забезпечення високого спільного рівня кібербезпеки в усьому Союзі, розширює коло суб'єктів, на яких поширюються вимоги кібербезпеки, включаючи органи державного управління та постачальників цифрових послуг. Водночас директива встановлює рамкові вимоги та залишає державам-членам значну дискрецію у визначенні конкретних об'єктів і механізмів регулювання. Ця Директива розширює розуміння критичної інфраструктури, переносячи акцент з суто фізичних об'єктів (заводів, електростанцій) на інформаційні та цифрові масиви даних, від яких залежить урядування.

Безповоротний євроінтеграційний курс України та отримання статусу кандидата на вступ до ЄС зумовлює безальтернативну необхідність гармонізації національного законодавства із зазначеними європейськими стандартами у сфері кібербезпеки. Зважаючи на те, що післявоєнна відбудова України значною мірою спиратиметься на цифрові рішення, захист таких платформ стає питанням не лише безпеки, але й довіри з боку міжнародних партнерів та інвесторів.

З огляду на викладене, з метою підвищення рівня правової визначеності та стійкості державних цифрових платформ доцільно розглянути такі напрями вдосконалення нормативного регулювання:

По-перше, передбачити у Законі України «Про критичну інфраструктуру» удосконалення критеріїв віднесення державних інформаційних систем та цифрових платформ до об'єктів критичної інфраструктури з урахуванням їх функціонального навантаження, обсягу оброблюваних даних та ролі у забезпеченні публічних послуг [4]. Відсутність чітко визначеної категоризації державних цифрових платформ як об'єктів критичної інфраструктури або як окремого виду «цифрової критичної інфраструктури» створює системні прогалини у правовому регулюванні їх захисту. Це ускладнює формування єдиних обов'язкових стандартів кіберзахисту, належного рівня резервування та кризового реагування, а також призводить до фрагментарності підходів у забезпеченні їх стійкості до кіберзагроз і функціональної безперервності в умовах надзвичайних ситуацій та воєнного стану.

По-друге, доцільним є розроблення на рівні підзаконних нормативно-правових актів Кабінету Міністрів України спеціального регламенту кіберзахисту порталу Дія як комплексної цифрової платформи публічного управління. Такий регламент має встановлювати не лише загальні вимоги безпеки, а й деталізовані процедурні механізми, зокрема обов'язкове проведення регулярних незалежних аудитів кібербезпеки із залученням зовнішніх експертів та застосуванням механізмів типу Bug Bounty. Окремо доцільно передбачити впровадження обов'язкових протоколів Business Continuity Planning (BCP) і Disaster Recovery (DR), які забезпечуватимуть оперативне відновлення функціонування системи у разі масштабних технічних збоїв або цілеспрямованих кібератак.

По-третє, необхідним є законодавче закріплення імперативного обов'язку Міністерства цифрової трансформації України як центрального органу виконавчої влади, що формує та реалізує державну політику у сфері цифровізації, щодо гарантування безперервності надання електронних публічних послуг в умовах надзвичайного та воєнного стану. При цьому доцільно нормативно визначити систему вимірюваних індикаторів (KPI) такої безперервності, включаючи допустимі рівні простою системи, час відновлення сервісів та вимоги до резервування інфраструктури, а також передбачити юридичну відповідальність за недотримання встановлених стандартів стійкості цифрових сервісів.

**Висновки.**

Таким чином, портал Дія давно вийшов за межі виключно сервісного інструмента та набув ознак системоутворюючого елементу сучасного публічного управління. У практичному вимірі він забезпечує реалізацію ключових функцій держави в цифровій формі та фактично виконує роль критично важливої складової цифрової інфраструктури в умовах триваючих безпекових загроз і гібридної війни. Разом із тим, чинна модель правового регулювання не повною мірою відображає реальний масштаб його функціональної значущості. Відсутність чітко закріпленого публічно-правового статусу та спеціалізованих законодавчих механізмів його захисту свідчить про наявність нормативної невідповідності між фактичною роллю цифрових сервісів і рівнем їх правової інституалізації. Це формує потребу у подальшому розвитку законодавства з метою усунення зазначених дисбалансів. Вирішення цієї проблеми шляхом імплементації запропонованих підходів є актуальним як у контексті гармонізації національного законодавства з правом Європейського Союзу, зокрема положеннями Directive (EU) 2022/2555 (NIS2), так і з точки зору зміцнення національної стійкості, інформаційної безпеки та довіри до цифрових державних сервісів.

У підсумку, «Дію» доцільно розглядати не лише як інструмент надання адміністративних послуг, а як базовий компонент сучасної цифрової державної інфраструктури. Водночас правове регулювання у цій сфері потребує подальшої систематизації та вдосконалення з метою забезпечення належного рівня кіберзахисту, функціональної стійкості та відповідності європейським стандартам у сфері цифрової безпеки.

**Список використаних джерел:**


1. Про адміністративні послуги : Закон України від 06.09.2012 № 5203-VI : станом на 2 берез. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text (дата звернення: 15.04.2026).
2. Гуцу С.Ф. Правове регулювання мережі Інтернет: міжнародний і вітчизняний досвід // Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право». – 2018. (№ 2/2018). С.114-118. URL : http://visnyk-psp.kpi.ua/issue/view/9248 (дата звернення: 15.04.2026).
3. Ганна Спіцина, Світлана Гуцу Легалізація поняття інформаційної безпеки особистості в українському законодавстві // Пропілеї права та безпеки : наук. журнал / Ред. кол. Н.Є. Філіпенко, І.Р. Шинкаренко, С.Ю. Лукашевич, та ін. – Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2023. №. 2-3.С. 37-41.
4. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.04.2026).

5. Центр прав людини ZMINA. З кінця лютого 2022 року в Україні зафіксували понад 2000 кібератак з боку РФ. *zmina.info*. URL: https://zmina.info/news/z-kinczya-lyutogo-2022-roku-v-ukrayini-zafiksuvaly-ponad-2000-kiberatak-z-boku-rf/ (дата звернення: 15.04.2026).
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.04.2026).
7. Центр міжнародної безпеки та партнерства. "Країна в смартфоні" по-естонськи: цифрова держава як ключ до подолання корупції. *ispc.org.ua*. URL: https://www.ispc.org.ua/archives/5508 (дата звернення: 15.04.2026).
8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) URL: https://eur-lex.europa.eu/eli/dir/2022/2555 (дата звернення: 28.03.2025).

https://doi.org/10.5281/zenodo.20498309

***Наталія ФЕДОСЕНКО,***
*кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового факультета Національного аерокосмічного університету «Харківський авіаційний інститут»,*
*м. Харків, Україна,*
*ORCID: https://orcid.org/0000-0002-6615-3937*
*e-mail: n.fedosenko@khai.edu*

# ОСОБЛИВОСТІ ДОКАЗУВАННЯ ПРАВ НА ЦИФРОВІ АКТИВИ У ЦИВІЛЬНОМУ ПРОЦЕСІ

**Анотація:** У тезах розглядаються актуальні процесуальні проблеми доказування прав на цифрові активи (криптовалюти, токени, NFT) у цивільному процесі України. Аналізуються труднощі ідентифікації власників цифрових гаманців, специфіка атрибуції анонімних транзакцій та особливості перевірки автентичності записів у розподіленому реєстрі (блокчейні). Особлива увага приділяється допустимості та належності електронних доказів. Обґрунтовується роль комп'ютерно-технічної експертизи як ключового засобу встановлення обставин справи та пропонуються шляхи адаптації цивільного процесуального законодавства до викликів цифрової економіки з метою забезпечення ефективного судового захисту.
**Ключові слова:** цифрові активи, доказування, цивільний процес, електронні докази, блокчейн, ідентифікація, атрибуція.

## SPECIFICS OF PROVING RIGHTS TO DIGITAL ASSETS IN CIVIL PROCEDURE

**Abstract:** The abstract examines current procedural challenges in proving rights to digital assets (cryptocurrencies, tokens, NFTs) within the civil proceedings of Ukraine. It analyzes the difficulties of identifying digital wallet owners, the specifics of attributing anonymous transactions, and the peculiarities of verifying the authenticity of records in a distributed ledger (blockchain). Special attention is paid to the admissibility and relevance of electronic evidence. The role of computer-technical expertise as a key means of establishing the circumstances of the case is substantiated, and ways to adapt civil procedural legislation to the challenges of the digital economy are proposed to ensure effective judicial protection.
**Key words:** digital assets, burden of proof, civil procedure, electronic evidence, blockchain, identification, attribution.

**Вступ.**

Сучасний стан розвитку приватноправових відносин характеризується інтенсивним залученням цифрових активів до структури цивільного обороту, що стало прямим наслідком стрімкої еволюції технологій розподіленого реєстру. Попри прийняття Закону України «Про віртуальні активи», який заклав підґрунтя для нормативного визначення їхнього статусу, процесуальні аспекти захисту прав на такі об'єкти все ще позбавлені комплексного врегулювання. У межах цивільного судочинства процедура доказування прав на криптовалюти, токени та NFT стикається з низкою специфічних викликів, детермінованих

складною технічною природою блокчейну, що вимагає переосмислення традиційних засад оцінки доказів у цифрову епоху

**Викладення основного матеріалу.**

Фундаментальне значення для вирішення спорів щодо приналежності цифрових активів має належна процесуальна фіксація інформації, де основним джерелом відомостей, відповідно до приписів статті 100 Цивільного процесуального кодексу України, виступають електронні докази [1]. Проте правозастосовна практика виявляє суттєві труднощі в контексті оцінювання їхньої належності та достовірності, що зумовлено специфікою технічного втілення таких об'єктів. На відміну від традиційних електронних документів, які мають централізований характер зберігання, записи в розподіленому реєстрі (блокчейні) існують у децентралізованому середовищі, що ускладнює процедуру їхньої автентифікації за класичними критеріями. У науковій літературі слушно наголошується, що відсутність матеріального втілення та специфічний порядок генерації даних у блокчейні вимагають від суду застосування критеріїв цілісності цифрового сліду, а не лише формальної наявності скріншота інтерфейсу, який за своєю правовою природою є лише похідним електронним доказом [4]

Одним із найбільш складних аспектів у межах судового доказування є процедура атрибуції, встановлення юридично значущого зв'язку між анонімізованою адресою цифрового гаманця та конкретним суб'єктом цивільних правовідносин. Оскільки технологічна природа розподіленого реєстру базується на засадах псевдонімності, пряма ідентифікація володільця активу за даними блокчейну є неможливою, що створює ситуацію процесуальної невизначеності. У цьому контексті тягар доказування зміщується у площину аналізу сукупності непрямих доказів та залучення відомостей від постачальників послуг, пов'язаних із віртуальними активами (VASP). Як зазначається у спеціальній літературі, подолання такої децентралізованої анонімності вимагає від суду застосування стандартів доказування, що базуються на ідентифікації через процедури KYC (Know Your Customer) та аналізі цифрових слідів транзакцій, що дозволяє деанонімізувати учасника обороту та забезпечити невідворотність цивільно-правової відповідальності [3; 5].

З огляду на високу технологічну складність об'єктів дослідження та специфіку їхнього існування у віртуальному просторі, особливого значення у системі засобів доказування набуває інститут судової експертизи. Самостійне оцінювання судом автентичності цифрових записів та перевірка цілісності транзакцій часто виявляються недостатніми для повного встановлення фактичних обставин справи, що детермінує необхідність залучення спеціальних знань. Призначення комп'ютерно-технічної експертизи дозволяє верифікувати санкціонованість доступу до приватних ключів та встановити факт ініціювання транзакції з конкретного апаратного пристрою. Водночас судово-економічна експертиза стає незамінним інструментом для коректної конвертації волатильної вартості цифрового активу у фіатний еквівалент на момент порушення права, що є базовою умовою для розрахунку збитків та визначення ціни позову.

Окремим аспектом забезпечення правової стійкості в умовах цифровізації є вдосконалення механізмів забезпечення позову, спрямованих на запобігання миттєвому відчуженню віртуальних активів. Висока мобільність таких об'єктів вимагає від цивільного процесу оперативності, яка б дозволяла накладати арешт на активи через судові приписи постачальникам кастодіальних послуг або через обмеження доступу до цифрових адрес. У підсумку, адаптація цивільного процесуального законодавства до викликів цифрової економіки має базуватися на принципах гнучкості та технологічної нейтральності. Це дозволить сформувати цілісну концепцію судового захисту, де цифровий актив визнається

повноцінним об’єктом майнових прав, а засоби його доказування відповідають сучасним стандартам технологічного розвитку.

**Висновки.**

Підсумовуючи викладене, слід констатувати, що ефективність судового захисту прав на цифрові активи безпосередньо залежить від готовності цивільного процесу до впровадження нових стандартів роботи з цифровими даними.

По-перше, пропонується визнати за записами у розподіленому реєстрі (блокчейні) статус первинних електронних доказів із презумпцією їхньої достовірності, тоді як скріншоти інтерфейсів розглядати як похідні докази, що потребують обов’язкової верифікації.

По-друге, розв’язання проблеми атрибуції має ґрунтуватися на комплексному поєднанні технічних даних блокчейну з відомостями, отриманими від постачальників послуг у межах процедур ідентифікації користувачів.

Зрештою, лише поєднання технологічної нейтральності законодавства із активним залученням спеціальних знань (експертизи) дозволить сформувати надійний механізм захисту інноваційних майнових прав у межах цивільного судочинства.

**Список використаних джерел:**


1. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15.
2. Про віртуальні активи: Закон України від 15.03.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20.
3. Некіт К. Г. Правовий статус криптовалют в Україні та світі. *Юридичний науковий журнал*. № 1. 2018. С. 40–42.
4. Капліна В. А. Місце криптовалюти в системі об’єктів цивільних прав. *Право та інноваційне суспільство*. 2019. № 1 (12). С. 30–36.
5. Логойда В. М. Криптовалюти як об'єкт цивільних прав: порівняльно-правовий аналіз. *Ужгородський національний університет*. 2021. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/45948.

https://doi.org/10.5281/zenodo.20498337

***Михайло ФІАЛКА,***
*кандидат юридичних наук, професор,*
*професор кафедри права*
*гуманітарно-правового факультету*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*
*ORCID: https://orcid.org/0000-0001-5599-3335*
*e-mail: fialkami70@gmail.com*

# БЕЗПІЛОТНЕ ПОВІТРЯНЕ СУДНО ЯК ПРЕДМЕТ ПОРУШЕННЯ ПРАВИЛ ПОВІТРЯНИХ ПОЛЬОТІВ (СТ. 281 КК УКРАЇНИ)

**Анотація:** У статті здійснено комплексний науковий аналіз предмета складу кримінального правопорушення, передбаченого ст. 281 КК України. Досліджено етимологічну, філологічну та нормативно-правову природу поняття «повітряне судно». Особливу увагу приділено співвідношенню категорій «повітряне судно» та «безпілотне повітряне судно» у контексті сучасного авіаційного та кримінального права. Проаналізовано наукові підходи до визначення правового статусу безпілотних повітряних суден та можливості їх віднесення до предмета кримінального правопорушення. Сформульовано авторську позицію щодо необхідності розширеного тлумачення ст. 281 КК України.

**Ключові слова:** повітряне судно; безпілотне повітряне судно; кримінальне правопорушення; безпека польотів; предмет кримінального правопорушення; авіаційне право

# UNMANNED AIRCRAFT AS THE SUBJECT OF VIOLATION OF AIR FLIGHT RULES (ART. 281 OF THE CRIMINAL CODE OF UKRAINE)

**Abstract:** The article carries out a comprehensive scientific analysis of the subject of the criminal offense provided for in Art. 281 of the Criminal Code of Ukraine. The etymological, philological and regulatory nature of the concept of “aircraft” is studied. Particular attention is paid to the correlation of the categories “aircraft” and “unmanned aircraft” in the context of modern aviation and criminal law. Scientific approaches to determining the legal status of unmanned aircraft and the possibility of their inclusion in the subject of a criminal offense are analyzed. The author’s position on the need for an expanded interpretation of Art. 281 of the Criminal Code of Ukraine is formulated.

**Keywords:** aircraft; unmanned aircraft; criminal offense; flight safety; subject of criminal offense; aviation law

**Вступ.**

Стрімкий розвиток авіаційних технологій, зокрема поширення безпілотних повітряних суден, істотно впливає на трансформацію правового регулювання у сфері безпеки повітряного руху. У сучасних умовах особливого значення набуває питання адекватного кримінально-правового реагування на порушення правил повітряних польотів, що створюють загрозу життю та здоров’ю людей.

**Викладення основного матеріалу.**

Особливої актуальності це питання набуло в умовах воєнного стану в Україні, коли дрони стали не лише засобом цивільного використання, але й інструментом ведення бойових дій, розвідки, логістики та спостереження. У зв'язку з цим постає необхідність переосмислення змісту окремих кримінально-правових норм, зокрема ст. 281 Кримінального кодексу України (*далі – КК України*), яка передбачає відповідальність за порушення правил повітряних польотів [1]. Водночас диспозиція зазначеної статті формувалася в умовах, коли безпілотні повітряні судна не мали такого поширення, як сьогодні, що зумовлює необхідність її сучасного тлумачення.

Ключовим питанням у цьому контексті є визначення предмета складу кримінального правопорушення, а саме – з'ясування змісту поняття «повітряне судно» та встановлення його співвідношення з категорією «безпілотне повітряне судно».

Відповідно до ст. 281 КК України, кримінально караним є порушення правил безпеки польотів повітряних суден особами, які не є працівниками повітряного транспорту, якщо такі дії створили небезпеку для життя людей або настання інших тяжких наслідків [1].

Безпосереднім об'єктом даного кримінального правопорушення виступає безпека руху та експлуатації повітряного транспорту. Додатковим факультативним об'єктом можуть бути життя, здоров'я людей або власність [2, с. 339].

У теорії кримінального права предмет кримінального правопорушення визначається як речі матеріального світу, щодо яких або у зв'язку з якими вчиняється кримінальне правопорушення. У межах ст. 281 КК України таким предметом виступає повітряне судно.

Саме тому правильне тлумачення поняття «повітряне судно» має фундаментальне значення для визначення меж кримінальної відповідальності.

Термін «повітряне судно» є складним словосполученням, яке складається з двох понять: «повітряний» та «судно».

Слово «повітряний» походить від слова «повітря», тобто газоподібного середовища атмосфери Землі. У буквальному розумінні воно означає те, що перебуває або функціонує в атмосферному просторі.

Термін «судно» історично використовувався для позначення транспортного засобу, призначеного для пересування у певному середовищі – водному або повітряному. У філологічному аспекті поняття «судно» не обов'язково передбачає наявність людини на борту. Його сутність полягає саме у здатності здійснювати рух у відповідному середовищі та бути технічним транспортним об'єктом.

Таким чином, уже на рівні етимології поняття «повітряне судно» не виключає можливості існування безпілотних апаратів. Основними ознаками залишаються:

– функціонування у повітряному просторі;

– здатність до керованого польоту;

– технічна придатність до переміщення в атмосфері.

Щодо законодавчого закріплення терміну «повітряне судно», то в цій ситуації, в-першу чергу, мова йде про Повітряний кодекс України. Відповідно до даного нормативно-правового акту, повітряне судно визначається як літальний апарат, що підтримується в атмосфері внаслідок взаємодії з повітрям, відмінної від взаємодії з повітрям, відбитим від земної поверхні [3].

Аналогічні визначення містяться і в підзаконних нормативних актах Державіаслужби України.

Важливим є те, що законодавець не пов'язує поняття повітряного судна із наявністю екіпажу або пілота на борту. Навпаки, у сучасному авіаційному законодавстві дедалі частіше використовуються поняття:

– «безпілотне повітряне судно»;
– «безпілотна авіаційна система»;
– «безпілотний літальний апарат».

У наукових та нормативних джерелах безпілотне повітряне судно (*далі – БПС*) визначається як будь-яке повітряне судно, що експлуатується або розроблене для експлуатації автономно чи яке пілотується дистанційно без пілота на борту [3].

В тому ж нормативно-правовому акті закріплюється і зміст такого поняття як «безпілотна авіаційна система», а саме: безпілотне повітряне судно та обладнання для дистанційного керування ним [3].

Отже, нормативний аналіз підтверджує, що безпілотне повітряне судно є різновидом повітряного судна.

У сучасній юридичній доктрині сформувалося два основні підходи до визначення правової природи безпілотних повітряних суден, а саме: концепція тотожності та концепція функціонального відмежування.

Згідно з цим підходом, безпілотне повітряне судно є різновидом повітряного судна. Представники цього підходу наголошують на функціональній єдності зазначених категорій.

Так, О. О. Квітка прямо вказує на сучасну практичну реальність – зростання використання малогабаритних повітряних суден і безпілотних літальних апаратів (*далі – БЛА*), польоти яких можуть створювати небезпеку для людей. Це є підставою для кримінально-правового аналізу таких випадків у межах ст. 281 КК України [4, с. 145-146].

Аргументами на користь цього підходу є:
– однакове середовище функціонування;
– потенційна небезпека для безпеки польотів;
– підпорядкування авіаційним правилам.

Саме такої позиції дотримуються більшість сучасних дослідників авіаційного права та представники практики Державіаслужби.

Додатковим аргументом є міжнародна практика ІСАО, відповідно до якої *unmanned aircraft* (безпілотний літальний апарат) входить до системи *aircraft* (літак) загалом.

Іншими словами, треба наголошувати на тому, що БПС вважається літальним апаратом, що використовується в повітряному просторі, а отже, на нього поширюються загальні норми повітряного права (наприклад, норми Повітряного кодексу України) [3]. Екіпаж у цьому випадку є «дистанційним» (оператор на землі), але він все одно вважається суб'єктом, що керує повітряним рухом. Ця концепція зручна для інтеграції дронів у єдину систему управління повітряним рухом, оскільки застосовує стандартні вимоги до реєстрації, сертифікації та польотів.

Інший підхід, тобто концепція функціонального відмежування, передбачає диференціацію БПС залежно від їх характеристик. Прихильники цієї концепції вважають, що не всі БПС повинні визнаватися предметом кримінального правопорушення.

Зокрема, пропонується виключати малогабаритні апарати, які використовуються для розваг і не становлять значної загрози для безпеки повітряного руху. Так, наприклад, В. В. Кузнецов та М. В. Сийплокі, наголошують на тому, що межа, нижче якої дрони вважаються «іграшками» або такими, що становлять мінімальний ризик, повинна бути вага 250 г [5, с. 377].

Однак така позиція викликає критику, оскільки навіть малий апарат може створити небезпеку у разі потрапляння у зону польотів повітряних суден.

Зокрема, пропонується відмежовувати:
– професійні та сертифіковані БПС;
– побутові дрони малої ваги;

– іграшкові літальні пристрої.

Прихильники цього підходу наголошують, що малогабаритні дрони не завжди становлять реальну загрозу безпеці польотів цивільної авіації, а тому не повинні автоматично визнаватися предметом кримінального правопорушення, передбаченого ст. 281 КК України.

Подібний підхід частково підтверджується законодавством України, яке звільняє від державної реєстрації окремі безпілотні повітряні судна масою до 20 кг, що використовуються для спортивних або розважальних цілей (п. 4 ч. 8 ст. 39 Повітряний кодекс України) [3].

Однак навіть відсутність реєстрації не означає, що такий апарат перестає бути повітряним судном за своєю юридичною природою.

Сучасна наукова дискусія зосереджена навколо питання: чи може БПС визнаватися предметом складу кримінального правопорушення, передбаченого ст. 281 КК України. Іншими словами існує протиставленням вузького та широкого підходів до тлумачення поняття «повітряне судно» в межах предмету кримінального правопорушення.

Прихильники широкого підходу (зокрема, О. О. Квітка) обґрунтовують необхідність включення безпілотних повітряних суден до предмета кримінального правопорушення передбаченого ст. 281 КК України, виходячи з функціонального критерію. Тобто мова йде про те, що тлумачення ознак даного складу кримінального правопорушення повинно відбуватись з урахуванням розвитку новітніх авіаційних технологій. Дослідники наголошують на тому, що традиційне розуміння повітряного судна як виключно пілотованого апарата є застарілим.

Натомість окремі автори вказують на проблему правової невизначеності. Вони підкреслюють, що КК України був прийнятий у 2001 році, коли масове використання дронів фактично ще не існувало. Відтак диспозиція ст. 281 КК України формувалася виходячи з класичного розуміння авіації.

При цьому слід враховувати принцип юридичної визначеності кримінального закону. Надмірно широке тлумачення поняття «повітряне судно» може створювати ризики необґрунтованої криміналізації.

Разом із тим переважаючою в сучасній доктрині є позиція про те, що БПС можуть бути предметом кримінального правопорушення, передбаченого ст. 281 КК України, якщо:
– вони є повітряними суднами за технічними характеристиками;
– їх експлуатація регламентується авіаційними правилами;
– порушення правил їх використання створює небезпеку для безпеки польотів.

На нашу думку, БПС може визнаватися предметом кримінального правопорушення, передбаченого ст. 281 КК України.

Такий висновок обґрунтовується наступним: 1) законодавче визначення повітряного судна не містить ознаки обов’язкової присутності пілота на борту; 2) БПС функціонують у повітряному просторі та здатні створювати загрозу безпеці авіації; 3) сучасне авіаційне право прямо використовує категорію «безпілотне повітряне судно»; 4) метою ст. 281 КК України є охорона безпеки польотів, а не лише безпека експлуатації пілотованої авіації; 5) виключення БПС із предмета даного кримінального правопорушення створювало б небезпечну прогалину у кримінально-правовому захисті повітряного простору.

Водночас доцільним видається нормативне уточнення диспозиції ст. 281 КК України шляхом прямого закріплення в ній положення про безпілотні повітряні судна. Це сприяло б дотриманню принципу правової визначеності та усуненню суперечностей у правозастосуванні.

**Висновки.**

Предметом складу кримінального правопорушення, передбаченого ст. 281 КК України, є повітряне судно як технічний засіб здійснення польоту у повітряному просторі.

Етимологічний, філологічний та нормативний аналіз поняття «повітряне судно» свідчить про те, що воно не обмежується лише пілотованими літальними апаратами. Сучасне законодавство України та міжнародна практика визнають БПС різновидом повітряних суден. Саме тому БПС можуть розглядатися як предмет кримінального правопорушення, передбаченого ст. 281 КК України, за умови створення ними загрози безпеці польотів. Наукова полеміка щодо цього питання демонструє необхідність подальшого вдосконалення кримінального та авіаційного законодавства України з урахуванням стрімкого розвитку безпілотних технологій.

**Список використаних джерел:**


1. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III. // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 23.04.2016)
2. Кримінальне право України. (Особлива частина): підручник / Кол. авторів А. В. Байлов, О. А. Васильєв, О. О. Житний, та ін.; за заг. ред. О. М. Литвинова; наук. ред. серії О. М. Бандурка. – Харків: Вид-во ХНУВС, 2011. – 572 с.
3. Повітряний кодекс України: закон України від 19.05.2011 № 3393-VI. // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3393-17 (дата звернення: 24.04.2016)
4. Квітка О. О. Щодо діяння як ознаки складу злочину, передбаченого ст. 281 КК України. *Вісник асоціації кримінального права*. 2020. № 1 (13). С. 145–162.
5. Кузнецов В. В., Сийплокі М. В. Правове регулювання використання безпілотних повітряних суден: окремі аспекти імплементації досвіду ЄС // Науковий вісник Ужгородського Національного Університету, 2026. Серія ПРАВО. Випуск 93: частина 5. С. 373-380. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/356175/342058

https://doi.org/10.5281/zenodo.20498373

***Наталія ФІЛІПЕНКО,***
*докторка юридичних наук, професорка,*
*професорка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*
*ORCID: https://orcid.org/0000-0001-9469-3650*
*e-mail: n.filipenko@khai.edu*

***Сергій ЛУКАШЕВИЧ,***
*кандидат юридичних наук, доцент,*
*професор кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету*
*«Харківський авіаційний інститут»*
*ORCID: https://orcid.org/0000-0001-8386-6237*
*e-mail: s.lukashevych@khai.edu*

***Володимир ТРОФИМЕНКО,***
*доктор юридичних наук, професор,*
*заступник Голови Державної служби спеціального зв'язку*
*та захисту інформації України*
*ORCID: https://orcid.org/0000-0001-6032-5550*
*e-mail: tvm.stolica@gmail.com*

## ЗМІНА ПАРАДИГМАЛЬНИХ ПІДХОДІВ ДО КІБЕРБЕЗПЕКИ УКРАЇНИ

Здійснено комплексний аналіз трансформації національної архітектури кібербезпеки України – від традиційної моделі «кіберзахисту», що ґрунтувалася на статичних бар'єрах та процедурі атестації, до сучасної концепції кіберрезильєнтності. Розкрито кризу моделі комплексної системи захисту інформації (КСЗІ), яка в умовах швидкої еволюції загроз виявилася надмірно формалізованою та неспроможною забезпечити належний рівень цифрової стійкості. Правові засади переходу визначені Законом України № 4336-IX, що гармонізує національне законодавство з вимогами Директиви ЄС 2022/2555 (NIS2) та інтегрує міжнародний досвід (ISO/IEC 27001, NIST). Особливу увагу приділено впровадженню системи профілів безпеки, механізмам авторизації та новим підходам до управління ризиками. Показано роль новітніх технологій — штучного інтелекту та концепції Zero Trust – у забезпеченні цифрової стійкості критичної інфраструктури та формуванні «форензічної готовності» систем. Зроблено висновок, що трансформація архітектури кібербезпеки України є стратегічною імплементацією міжнародних стандартів, яка дозволяє перейти від бюрократичної статичності до технологічної резильєнтності, забезпечуючи національну безпеку та відповідність європейським вимогам.

**Ключові слова:** кібербезпека, кіберрезильєнтність, критична інфраструктура, профілі безпеки, авторизація, Zero Trust, штучний інтелект, NIS2, ISO/IEC 27001, NIST.

## SHIFTING PARADIGMATIC APPROACHES TO CYBERSECURITY IN UKRAINE

A comprehensive analysis of the transformation of Ukraine's national cybersecurity architecture has been carried out – from the traditional "cyber defense" model, based on static barriers and certification procedures, to the modern concept of cyber resilience. The crisis of the Comprehensive Information Protection System (CIPS) model is revealed, which, under conditions of rapid threat evolution, proved excessively formalized and incapable of ensuring an adequate level of digital resilience. The legal foundations of the transition are defined by the Law of Ukraine No. 4336-IX, which harmonizes national legislation with the requirements of the EU Directive 2022/2555 (NIS2) and integrates international experience (ISO/IEC 27001, NIST). Particular attention is paid to

the implementation of the system of security profiles, authorization mechanisms, and new approaches to risk management. The role of emerging technologies – artificial intelligence and the Zero Trust concept – is highlighted in ensuring the digital resilience of critical infrastructure and in shaping systems' "forensic readiness." It is concluded that the transformation of Ukraine's cybersecurity architecture represents a strategic implementation of international standards, enabling the shift from bureaucratic static approaches to technological resilience, thereby ensuring national security and compliance with European requirements.

**Keywords**: cybersecurity, cyber resilience, critical infrastructure, security profiles, authorization, Zero Trust, artificial intelligence, NIS2, ISO/IEC 27001, NIST.

**Вступ**.

Сучасний глобальний цифровий простір перебуває у стані перманентної трансформації, де кіберзагрози еволюціонували від поодиноких актів хакерства до стратегічних інструментів міждержавного протистояння. Для України, яка перебуває в стані першої в історії відкритої кібервійни, розбудова ефективної архітектури кібербезпеки є питанням національного виживання. Традиційна парадигма «кіберзахисту», зосереджена на створенні периметральних бар'єрів, поступово поступається місцем концепції кіберрезильєнтності (cyber resilience). Цей перехід передбачає зміщення акцентів із запобігання інцидентам на здатність системи витримувати атаки, мінімізувати їхні наслідки та оперативно відновлюватися в умовах агресивного середовища.

**Викладення основного матеріалу**.

Протягом десятиліть основою захисту інформації в Україні залишалася модель комплексної системи захисту інформації (КСЗІ), яка будувалася на процедурі атестації. Така модель була «статичною за дизайном» — орієнтованою на фіксацію стану системи на момент перевірки з видачею атестата терміном до п'яти років. Це створювало ілюзію стабільності, проте фактично обмежувало здатність системи реагувати на нові загрози. Ключовими вадами КСЗІ стали надмірний формалізм, фокус на паперовій відповідності та неможливість оперативно реагувати на нові вразливості, що постійно мутують. В умовах використання супротивником складних тактик — таких як Living-off-the-Land (LotL) та вайпери для знищення даних – статичні бар'єри виявилися недостатніми.

Фундаментальний зсув у вітчизняній архітектурі кіберзахисту закріплений Законом України від 27 березня 2025 р. № 4336-IX. Цей акт гармонізує українське законодавство з вимогами Директиви ЄС 2022/2555 (NIS2) – що є критично важливим для євроінтеграції та формування лідируючої позиції України в регіоні. Імплементація положень NIS2 означає перехід від формальної атестації до ризик-орієнтованої моделі, яка відповідає європейським стандартам управління кіберризиками. Нова правова рамка вводить термін «авторизація з безпеки» – управлінське рішення щодо можливості функціонування системи на основі її відповідності профілям безпеки протягом усього життєвого циклу. На відміну від атестації, авторизація базується на принципах динамічності, де залишкові ризики ідентифікуються та визнаються прийнятними для власника системи.

Різниця між статичною робастністю (міцністю) та динамічною резильєнтністю (стійкістю) є ідеологічною основою реформи. Робастність намагається «витримати удар» без руйнувань та відновитись. Резильєнтність же базується на принципі «Assume Breach» — тобто припущенні про компрометацію — і включає чотири функції: передбачення, витримування, відновлення та адаптація. Динамічна резильєнтність розглядається як безперервний, керований даними процес, що забезпечує стабільність навіть у разі успішного зламу окремих елементів.

Заміна КСЗІ реалізується через впровадження системи профілів безпеки згідно з Постановою КМУ № 712. Профіль безпеки – це структурований документ, що містить ієрархію вимог:

– Базовий профіль безпеки (БПБ): уніфікований мінімальний стандарт від Держспецзв'язку, обов'язковий для всіх;

– Галузевий профіль безпеки (ГПБ): набір вимог, що враховує специфіку конкретних сфер, наприклад, захист SCADA-систем в енергетиці чи цілісність транзакцій у банках;

– Цільовий профіль безпеки (ЦПБ): кінцевий операційний документ конкретної системи, що розробляється її власником на основі оцінки ризиків.

Авторизація систем, де не обробляється державна таємниця, тепер здійснюється за декларативним принципом — що значно зменшує бюрократичне навантаження та відповідає європейській практиці.

Закон № 4336-IX суттєво розширює роль ключових суб'єктів: НКЦК при РНБО здійснює стратегічну координацію, Держспецзв'язку стає уповноваженим органом з формування національної політики в сфері кібербезпеки, а CERT-UA виконує роль центральної групи реагування, підтримуючи мережу галузевих та регіональних CSIRT — що прямо відповідає моделі, закріпленій у ЄС. Важливим нововведенням є інституціоналізація посад керівників із кіберзахисту, погодження їх призначення з регулятором, а також створення системи професійних кваліфікацій і залучення ветеранів до навчання кіберфахівців.

На відміну від «разової» атестації КСЗІ, нова процедура авторизації базується на принципах безперервності. Вона включає щорічне самооцінювання, зовнішнє оцінювання (аудит) не рідше ніж раз на два роки та постійний моніторинг. Така система перетворює кібербезпеку зі статичного стану на процес постійного вдосконалення – що відповідає міжнародним стандартам ISO/IEC 27001 та практикам NIST.

Нова архітектура спирається також на стандарт Zero Trust – який вимагає безперервної автентифікації кожної транзакції. У цьому алгоритмі штучний інтелект (ШІ) відіграє роль інструменту проактивного виявлення аномалій, що дозволяє скоротити час реагування на інциденти. ШІ стає критичним елементом переходу від реактивного до проактивного захисту, забезпечуючи передбачення та адаптацію системи до змін у ландшафті загроз у режимі реального часу. Крім того, ШІ може стати основою для створення автономних систем, здатних функціонувати навіть у разі деградації можливостей – здійснюючи автоматичну діагностику та усунення вразливостей без втручання оператора. Для об'єктів критичної інфраструктури вводиться концепція «форензічної готовності» (digital resilience) – налаштування систем для гарантованого збереження цифрових доказів навіть у разі деструктивних атак.

**Висновки**.

Отже, можна констатувати, що трансформація архітектури кібербезпеки України – це перехід від бюрократичної статичності до технологічної резильєнтності, яка відповідає сучасним міжнародним стандартам. Імплементація досвіду Європейського Союзу – зокрема положень Директиви NIS2, практик ISO/IEC 27001 та рекомендацій NIST – дозволяє перенести акцент із формальної відповідності на реальне управління ризиками та безперервний моніторинг. Впровадження профілів безпеки замість КСЗІ створює основу для інтеграції принципів Zero Trust та використання штучного інтелекту як інструменту проактивного захисту. Майбутнє системи полягає у перетворенні критичної інфраструктури на «живий організм» – здатний до самовідновлення, адаптації та безперервного функціонування під впливом будь-яких загроз, що забезпечує цифрову стійкість України та її відповідність європейським вимогам.

**Список використаних джерел:**

1. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 березня 2025 р. № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text .

2. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : Постанова Кабінету Міністрів України від 18 червня 2025 р. № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text .

3. Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 31 грудня 2025 р. № 1799. URL: https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF#Text .

4. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*. 2025. № 2 (42). С. 164–171. DOI: https://doi.org/10.35774/app2025.02.164 .

5. Філіпенко Н., Харченко В., Лукашевич С. (2025) Еволюція безпекової політики Європейського союзу і контексті нових кіберзагроз: від директиви nis1 до директиви nis2 (оглядова стаття). Пропілеї права та безпеки, 2025. № 8. С. 34-42. DOI: https://doi.org/10.32620/pls.2025.8.03

6. Лукашевич С., Степанюк А. Захист та стійкість як визначальні категорії безпеки критичної інфраструктури : Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану [Електронний ресурс]: тези доповідей науково-практичної конференції, 8 листопада 2023 р., Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут». – Харків : ХАІ, 2023. – 184 с. DOI: https://doi.org/10.32620/SSDCICML.23

7. Резнікова О. О. *Національна стійкість в умовах мінливого безпекового середовища : монографія*. Київ : НІСД, 2022. 532 с. URL: https://niss.gov.ua/sites/default/files/2022-06/reznikova_book_web.pdf .

8. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2 Directive). URL: https://www.nis-2-directive.com/#:~:text=NIS%202%20(Directive%20(EU),for%20network%20and%20information%20systems.

https://doi.org/10.5281/zenodo.20499128

***Ігор ХМИРОВ,***
*доктор наук з державного управління, доцент,*
*доцент кафедри управління у сфері цивільного захисту*
*навчально-наукового інституту цивільного захисту*
*Національного університету цивільного захисту України,*
*ORCID: https://orcid.org/0000-0002-7958-463X*
*e-mail: khmyrov7771@gmail.com.ua*

***Анастасія ХМИРОВА,***
*кандидатка наук з державного управління,*
*старший викладач-методист навчально-наукового інституту*
*оперативно-рятувальних сил*
*Національного університету цивільного захисту України,*
*ORCID: https://orcid.org/0000-0002-0680-7505*
*e-mail: khmyrova.anast@gmail.com*

***Михайло ВОЛКОВ,***
*здобувач першого (бакалаврського) рівня вищої освіти*
*групи ЦЗк-23-1*
*Національного університету цивільного захисту України,*
*e-mail: mikhail9944@gmail.com*

# УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО РЕГУЛЮВАННЯ УТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ШТАБУ З ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

**Анотація.** Досліджено теоретичні та практичні аспекти державного регулювання механізмів утворення та функціонування штабу з ліквідації наслідків надзвичайних ситуацій як ключового елементу системи забезпечення національної безпеки. Проаналізовано нормативно-правове забезпечення діяльності штабу, його організаційну структуру, функції та інформаційне забезпечення. Визначено роль штабу як координаційного органу, що забезпечує взаємодію органів державної влади, органів місцевого самоврядування та сил цивільного захисту. Виявлено проблемні аспекти діяльності штабів, зокрема недостатню узгодженість міжвідомчої взаємодії, складність інформаційного обміну, домінування паперового документообігу та недостатній рівень підготовки персоналу. Запропоновано напрями вдосконалення механізмів державного регулювання, зокрема цифровізацію управлінських процесів, уніфікацію інформаційного обміну та адаптацію нормативної бази до сучасних викликів.

**Ключові слова:** державне регулювання, надзвичайна ситуація, штаб з ліквідації наслідків НС, цивільний захист, національна безпека, міжвідомча взаємодія, інформаційне забезпечення, управлінські рішення.

# IMPROVEMENT OF STATE REGULATION MECHANISMS FOR THE ESTABLISHMENT AND FUNCTIONING OF EMERGENCY RESPONSE HEADQUARTERS WITHIN THE NATIONAL SECURITY SYSTEM

**Abstract.** Theoretical and practical aspects of state regulation mechanisms for the establishment and functioning of emergency response headquarters as a key element of the national security system have been studied. The regulatory and legal framework governing the activities of the headquarters, its organizational structure, functions, and information support have been analyzed. The role of the headquarters as a coordination body ensuring interaction between state authorities, local self-government bodies, and civil protection forces has been defined. Problematic aspects of headquarters activities have been identified, in

particular insufficient interagency coordination, complexity of information exchange, dominance of paper-based documentation, and an insufficient level of personnel training. Directions for improving state regulation mechanisms have been proposed, including the digitalization of management processes, standardization of information exchange, and adaptation of the regulatory framework to modern challenges.

**Keywords:** state regulation, emergency situation, emergency response headquarters, civil protection, national security, interagency coordination, information support, management decisions.

**Вступ.**

Сучасне безпекове середовище характеризується зростанням кількості та складності надзвичайних ситуацій різного походження, що в умовах воєнного стану набувають комплексного характеру. Це обумовлює підвищені вимоги до ефективності державного регулювання у сфері цивільного захисту та реагування на надзвичайні ситуації. Одним із ключових елементів цієї системи є штаб з ліквідації наслідків надзвичайних ситуацій, діяльність якого забезпечує координацію дій усіх залучених суб'єктів.

**Викладення основного матеріалу.**

Нормативно-правове регулювання утворення та функціонування штабу базується на положеннях Кодексу цивільного захисту України та відповідних підзаконних актах. Вони визначають порядок створення штабу, його структуру, функції, повноваження та механізми інформаційного забезпечення. Такий підхід забезпечує правову визначеність, уніфікацію управлінських процедур та підвищення узгодженості дій органів влади під час ліквідації наслідків надзвичайних ситуацій.

Штаб з ліквідації наслідків надзвичайних ситуацій є тимчасовим органом управління, який формується для координації діяльності органів державної влади, органів місцевого самоврядування, сил цивільного захисту та інших суб'єктів реагування. Його діяльність ґрунтується на принципах централізованого управління, єдиноначальності та безперервності управлінського процесу.

Основними завданнями штабу є оцінювання обстановки в зоні надзвичайної ситуації, організація взаємодії між учасниками реагування, підготовка та доведення управлінських рішень, а також контроль за їх виконанням. Управлінський процес реалізується через послідовний цикл: збір інформації, її аналіз, прийняття рішень, організація виконання та оцінювання результатів. Важливе місце у діяльності штабу займає інформаційне забезпечення, що реалізується через систему оперативно-технічної та звітної документації. Вона дозволяє забезпечити безперервність управління, фіксувати зміни обстановки, контролювати виконання завдань та формувати аналітичну основу для прийняття рішень. Уніфікація форм документації сприяє стандартизації управлінських процесів і покращенню взаємодії між суб'єктами. Разом із тим, практична діяльність штабів виявляє низку проблем. Серед них – недостатня узгодженість міжвідомчої взаємодії, складність інформаційного обміну, нечіткість розмежування повноважень, а також перевантаженість паперовим документообігом. Це знижує оперативність управління та ускладнює адаптацію до швидкозмінної обстановки, особливо в умовах воєнного стану.

Окремою проблемою є недостатній рівень підготовки персоналу до роботи в штабному форматі, що впливає на якість прийняття управлінських рішень. Відсутність єдиних підходів до навчання та тренування персоналу знижує ефективність координації та взаємодії між різними службами.

Удосконалення механізмів державного регулювання діяльності штабів має здійснюватися комплексно. Важливими напрямами є цифровізація управлінських процесів, впровадження електронного документообігу, уніфікація інформаційних потоків та створення єдиних стандартів обміну даними. Також необхідно адаптувати нормативно-правову базу до умов воєнного стану та підвищити рівень професійної підготовки персоналу. Реалізація зазначених заходів дозволить підвищити оперативність прийняття рішень, покращити координацію між суб'єктами реагування та забезпечити ефективне використання ресурсів під час ліквідації наслідків надзвичайних ситуацій.

**Висновки.**

Державне регулювання механізмів утворення та функціонування штабу з ліквідації наслідків надзвичайних ситуацій є важливим елементом системи забезпечення національної безпеки. Чинна нормативно-правова база створює основу для координації дій суб'єктів реагування, однак потребує подальшого вдосконалення з урахуванням сучасних викликів. Основними напрямами вдосконалення є цифровізація управління, підвищення ефективності інформаційного обміну,

удосконалення міжвідомчої взаємодії та підвищення рівня підготовки персоналу. Реалізація цих заходів сприятиме підвищенню ефективності функціонування штабів та зміцненню національної безпеки України.

**Список використаних джерел:**


1. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17
2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
3. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19
4. Про затвердження Положення про штаб з ліквідації наслідків надзвичайної ситуації : Наказ МВС України від 26.12.2014 № 1406. URL: https://zakon.rada.gov.ua/laws/show/z0047-15
5. Вавренюк С.А., Хмиров І.М., Хряпинський А. П., Григор'ян М. Б., Власенко О. В. Державне регулювання механізму утворення та роботи штабу з ліквідації наслідків надзвичайних ситуацій як чинник забезпечення національної безпеки // Інвестиції: практика та досвід. 2026. № 4. С. 301–305. DOI: 10.32702/2306-6814.2026.4.301
6. Хмиров І. М., Хмирова А. О., Фурманов О. Публічне управління та адміністрування логістичним забезпеченням спільних дій сил безпеки при реагуванні на надзвичайні ситуації // Пропілеї права та безпеки. 2025. № 8. DOI: https://doi.org/10.32620/pls.2025.8.80
7. Хмиров І. М. Особливості правового регулювання відшкодування шкоди, завданої Державною службою України з надзвичайних ситуацій при гасінні пожеж // Вісник НУЦЗУ. Серія "Державне управління". – 2022. – Вип. 1 (16). – С. 314-320.

## УЧАСНИКИ КОНФЕРЕНЦІЇ

**НАУКОВЕ ВИДАННЯ**

**ПРАВОВІ ЗАСАДИ СТІЙКОСТІ ТА СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВ АВІАЦІЙНОЇ ГАЛУЗІ ТА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**
**Тези доповідей Всеукраїнської науково-практичної конференції (м. Харків, 30 квітня 2026 року) Електронне видання.**

**LEGAL PRINCIPLES OF SUSTAINABILITY AND SUSTAINABLE DEVELOPMENT OF AVIATION INDUSTRY ENTERPRISES AND CRITICAL INFRASTRUCTURE FACILITIES**

**Theses of the All-Ukrainian Scientific and Practical Conference**

**Відповідальний за випуск Н. Є. Філіпенко**
**Технічний редактор Т. М. Лазарева**
**Комп'ютерне складання та верстання Т. М. Лазарева**

**Адреса редакційної колегії:**
**61070, м. Харків, вул. Манька, 17**
**Національний аерокосмічний університет**
**«Харківський авіаційний інститут»**
**тел. +38 (067) 575 83 94**

**Підписано до видання 27.05.2026**
**Ум. друк. арк. 8,37. Обл.-вид. арк. 5,5. Електронний ресурс**