ФП 2025-4
ISSN 1995-6134

УДК *343.35:620.9(477)*
DOI: http://doi.org/10.5281/zenodo.17347755

І.В. ЗОЗУЛЯ,
професор кафедри криміналістики та судової експертології Харківського національного університету внутрішніх справ, доктор юридичних наук, професор, м. Харків, Україна; e-mail: journals@meta.ua;
ORCID: http://orcid.org/0000-0002-3507-0012

ПРАВОВІ ТА КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ РЕАЛІЗАЦІЇ ПРОЄКТІВ ЗАХИСТУ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

I.V. ZOZULIA,
Professor, Department of Forensics and Judicial Expertology, Kharkiv National University of Internal Affairs, Doctor of Law, Professor, Kharkiv, Ukraine; e-mail: journals@meta.ua;
ORCID: http://orcid.org/0000-0002-3507-0012

LEGAL AND CRIMINAL LAW ASPECTS OF THE IMPLEMENTATION OF ENERGY INFRASTRUCTURE PROTECTION PROJECTS IN UKRAINE

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEYWORDS)

Постановка проблеми. Реалізація проєктів захисту енергетичної інфраструктури України в умовах воєнного стану та цифровізації супроводжується підвищеними корупційними і кримінальними ризиками. Складність технічних рішень, багаторівневе фінансування та використання цифрових систем створюють специфічне кримінально-правове середовище з фрагментарними та недостатньо уніфікованими підходами до кваліфікації злочинів і оцінювання правового значення фактичних обставин їх вчинення. **Метою** статті є здійснення комплексного кримінально-правового аналізу зловживань у процесі реалізації проєктів захисту енергетичної інфраструктури України з урахуванням галузевого регулювання, організаційно-управлінських механізмів і практики правозастосування, а також визначення проблем кваліфікації відповідних кримінальних правопорушень і меж кримінальної відповідальності. **Методи.** Метод аналізу та синтезу використано для опрацювання норм кримінального, процесуального та галузевого законодавства, а також наукових джерел; формально-логічний метод – для уточнення понятійного апарату та структурування складів злочинів; порівняльно-правовий метод – для зіставлення національних підходів з європейськими стандартами управління в енергетиці; спеціально-юридичний метод – для аналізу правозастосовної практики, виявлення типових правових ризиків та оцінювання ролі експертних висновків у процесі кримінально-правової кваліфікації. **Результати.** Обґрунтовано специфіку проєктів захисту енергетичної інфраструктури як окремого об'єкта кримінально-правового аналізу. Систематизовано типові склади злочинів і проблеми їх кваліфікації у сфері реалізації таких проєктів. Визначено характерні ознаки суспільної небезпечності відповідних діянь з урахуванням технічних, фінансових і цифрових факторів, що впливають на зміст кримінально-правової оцінки. Запропоновано системний підхід до оцінювання кримінально-правового значення відповідних діянь з урахуванням галузевої специфіки. **Висновки.** Ефективна протидія зловживанням у проєктах захисту енергетичної інфраструктури можлива лише за умови послідовного застосування кримінально-правового аналізу, адаптованого до умов функціонування критичної інфраструктури та цифрового середовища. Запропоновані підходи можуть застосовуватись у правозастосовній практиці та слугувати науковим підґрунтям для вдосконалення кримінально-правових механізмів реагування на правопорушення у сфері енергетичної безпеки України.

Ключові слова: *енергетична інфраструктура; проєкти захисту; кримінальні правопорушення; кримінально-правова кваліфікація; зловживання; воєнний стан; цифровізація; експертні висновки*

***

Problem statement. The implementation of projects aimed at protecting Ukraine's energy infrastructure under conditions of martial law and digitalization is accompanied by increased corruption-related and criminal risks. The complexity of technical solutions, multi-level financing, and the use of digital systems create a specific criminal-law environment characterized by fragmented and insufficiently unified approaches to the qualification of crimes and the assessment of the legal significance of the factual circumstances of their commission. The **purpose** of the article is to conduct a comprehensive criminal-

© Зозуля І.В., 2025
Open access under CC BY license

law analysis of abuses occurring in the process of implementing projects for the protection of Ukraine's energy infrastructure, taking into account sectoral regulation, organizational and managerial mechanisms, and law-enforcement practice, as well as to identify problems of qualification of the relevant criminal offenses and the limits of criminal liability. **Methods.** The method of analysis and synthesis was used to examine the provisions of criminal, procedural, and sector-specific legislation, as well as scholarly sources; the formal-logical method was applied to clarify the conceptual framework and structure the elements of criminal offenses; the comparative-law method was employed to compare national approaches with European standards of energy governance; the special legal method was used to analyze law-enforcement practice, identify typical legal risks, and assess the role of expert opinions in the process of criminal-law qualification. **Results.** The specificity of energy infrastructure protection projects is substantiated as a distinct object of criminal-law analysis. Typical elements of crimes and problems of their qualification in the implementation of such projects are systematized. Characteristic features of the social harmfulness of the relevant acts are identified, taking into account technical, financial, and digital factors that influence the substance of criminal-law assessment. A systemic approach to assessing the criminal-law significance of such acts, with due regard to sectoral specifics, is proposed. **Conclusions.** Effective counteraction to abuses in energy infrastructure protection projects is possible only through the consistent application of criminal-law analysis adapted to the conditions of functioning of critical infrastructure and the digital environment. The proposed approaches may be applied in law-enforcement practice and serve as a scholarly basis for improving criminal-law mechanisms for responding to offenses in the field of Ukraine's energy security.

Keywords: *energy infrastructure; protection projects; criminal offenses; criminal-law qualification; abuses; martial law; digitalization; expert opinions*

Постановка проблеми

Повномасштабна війна на території України виявила не лише військово-технічні, а й інституційно-процесуальні вразливості у сфері захисту критичної енергетичної інфраструктури. Відновлення та захист об'єктів енергозабезпечення – електростанцій, підстанцій, магістральних ліній та диспетчерських центрів – супроводжується масовими проєктами з великими обсягами державних і донорських коштів, строками виконання "тут і зараз" і безпрецедентним тиском на операційні та закупівельні ланцюги. У таких умовах зростає ймовірність корупційних схем, технічних фальсифікацій та цифрових маніпуляцій, що робить актуальним дослідження кримінальної складової у справах про зловживання під час реалізації проєктів захисту енергетичної інфраструктури [1, с.17; 2].

До того ж, ситуація ускладняється тим, що у світлі нещодавнього аудиту Рахункової палати щодо реалізації експериментального проєкту із захисту критичної енергетичної інфраструктури актуалізувалося питання не лише управлінських і фінансових порушень, а й можливих кримінальних ризиків, що витікають із них. Звіт Рахункової палати констатував системні недоліки в організації означеного проєкту, непрозорі процедури закупівель, факти завищення цін і часткову неготовність об'єктів до захисту, що створює підґрунтя для кримінально-правової кваліфікації відповідних діянь і визначення їх суспільної небезпечності [3–5]. Аудит і кримінальне переслідування є різними, але взаємопов'язаними процедурами, де аудит фіксує фактичні невідповідності, а результати перевірок можуть слугувати підставою для кримінально-правової оцінки та відкриття кримінальних проваджень.

Різноманітні аспекти захисту об'єктів енергозабезпечення та зловживань у сфері енергетики частково вже досліджувалися науковцями. Зокрема, Ю. Клят із співавторами запропонували класифікацію загроз енергетичній безпеці для виявлення найкритичніших вразливостей у національній енергетичній системі України [6]; Ю.В. Ус і В.О. Литовченко дослідили засади розроблення стратегії управління енергетичною безпекою підприємств в умовах зростаючої нестабільності [7], проте без урахування аспектів саме фізичного захисту об'єктів енергетичної інфраструктури в умовах воєнних дій та руйнувань. Водночас безпосередньо питання безпеки та захисту об'єктів критичної інфраструктури України в умовах воєнних руйнувань були досліджені нами [8], що дозволяє доповнити наявні підходи акцентом на фізичну та організаційно-правову складову захисту. В свою чергу, Ю.О. Ліпін розслідував шляхи заволодіння майном через зловживання службовим становищем у паливно-енергетичному комплексі України [9]; В. Корж надала ознаки характеристики економічних злочинів, скоєних організованими групами з корупційними зв'язками [10]; О.В. Неклеса розглянув окремі аспекти документування злочинів, вчинених у сфері публічних закупівель в умовах воєнного стану [11]. Окреме місце займає дослідження О.С. Гирич щодо кримінальної відповідальності за вчинення правопорушень у сфері енергетичної безпеки за законодавством країн

ISSN 1995-6134

Європейського Союзу [12]. Все це, включаючи й виявлені Рахунковою палатою України системні порушення під час реалізації проєкту із захисту енергетичної інфраструктури, підтверджує значущість теми.

Разом із тим, незважаючи на наявність певних напрацювань у цій сфері, залишаються невирішеними питання щодо ефективності існуючих механізмів запобігання зловживанням, а також проблеми недостатньої кримінально-правової оцінки у розслідуванні таких злочинів.

Тому *мета* статті полягає у здійсненні комплексного кримінально-правового аналізу зловживань у процесі реалізації проєктів захисту енергетичної інфраструктури України з урахуванням галузевого регулювання, організаційно-управлінських механізмів і практики правозастосування, а також визначенні проблем кваліфікації відповідних кримінальних правопорушень. *Новизна* статті полягає у вперше здійсненому комплексному розгляді зловживань як самостійного міжгалузевого об'єкта кримінально-правового аналізу з урахуванням безпекових, технічних і фінансово-економічних аспектів. *Завдання* статті включають: дослідження правових засад та особливостей галузевого регулювання; характеристику енергетичної інфраструктури і вразливостей; аналіз стану багаторівневого захисту об’єктів і визначення кримінально-правових особливостей зловживань у реалізації проєктів захисту енергетичної інфраструктури України та проблем їх правової оцінки.

Правові засади та галузеве регулювання реалізації проєктів захисту енергетичної інфраструктури України

Правове забезпечення захисту критичної енергетичної інфраструктури в Україні базується на поєднанні норм цивільного, адміністративного, публічного та кримінального права. Ключову роль у цьому відіграють Закони України "Про критичну інфраструктуру" від 16.11.2021 р. № 1882-IX [13], "Про публічні закупівлі" від 25.12.2015 р. № 922-VIII [14], Кримінальний кодекс України від 05.04.2001 р. № 2341-III [15] та інші нормативно-правові акти. Саме вони визначають коло уповноважених суб’єктів, закріплюють вимоги до процедур управління коштами, закупівель і будівництва, а також передбачають механізми контролю й відповідальності за порушення у сфері реалізації проєктів енергетичної інфраструктури.

Галузеве енергетичне законодавство конкретизує особливості функціонування енергетичного сектору та систему державного нагляду. Так, Закон України "Про ринок електричної енергії" від 13.04.2017 р. № 2019-VIII [16] регулює питання ліцензування, повноваження регулятора та інструменти контролю за діяльністю учасників ринку. Водночас Закон України "Про землі енергетики та правовий режим спеціальних зон енергетичних об’єктів" від 09.07.2010 р. № 2480-VI [17] визначає правовий режим використання земель енергетики, встановлює межі спеціальних зон та передбачає заходи їх охорони.

У практичній площині розслідування кримінальних правопорушень у сфері енергетики нерідко відбувається паралельно з аудитами Рахункової палати, внутрішніми перевірками операторів енергетичного ринку, а також контролем із боку міжнародних донорських організацій, зокрема World Bank, EBRD, USAID. Така ситуація об’єктивно зумовлює потребу в узгодженому застосуванні норм різних галузей права та налагодженні ефективної міжвідомчої взаємодії вже на початкових етапах досудового розслідування.

При цьому зловживання під час реалізації проєктів захисту енергетичної інфраструктури не мають поодинокого характеру. У публічному просторі неодноразово фіксувалися повідомлення про проведення понад 20 обшуків у справах щодо зловживань під час відновлення енергетичної інфраструктури у вересні 2023 р. [18], виявлення зловживань монопольним становищем у сфері енергетичного регулювання у жовтні 2022 р. [19], викриття заволодіння коштами стратегічних підприємств у травні 2018 р. [20], а також затримання заступника Міністра енергетики України за отримання неправомірної вигоди у серпні 2024 р. [21].

У зв’язку з цим *предмет правозастосування у справах про зловживання під час реалізації проєктів захисту енергетичної інфраструктури* охоплює сукупність кримінально-правових норм, спрямованих на виявлення, правову оцінку та доказування суспільно небезпечних діянь. Йдеться про посягання на цільове використання фінансових ресурсів, доброчесність процедур проєктування, закупівель і будівництва, а також на безпеку стратегічно важливих енергетичних об’єктів. У межах такого підходу аналізуються державні й міжнародні проєкти з укріплення енергетичної інфраструктури, рух фінансових потоків, тендерні та підрядні процедури, результати аудиту, службові рішення і їх наслідки для енергетичної безпеки держави. Це створює підґрунтя для своєчасного й адекватного реагу-

ISSN 1995-6134

вання на зловживання, що виникають на етапах проєктування, будівництва, модернізації, фінансування та введення в експлуатацію об'єктів енергетичної інфраструктури.

Енергетична інфраструктура, проєкти її захисту та їхні вразливості як предмет дослідження

Енергетична інфраструктура посідає ключове місце в системі національної безпеки, оскільки саме від її стабільного функціонування залежить робота промисловості, транспорту, комунальної сфери, сектору оборони та повсякденна життєдіяльність населення. Порушення в роботі енергетичних об'єктів мають системний характер і швидко виходять за межі самої галузі, спричиняючи економічні втрати, ускладнення державного управління та зниження загальної стійкості держави [22].

За своєю структурою енергетична інфраструктура є складною багаторівневою системою, що включає *виробничі об'єкти* (теплові, гідро- та атомні електростанції, а також потужності відновлюваної енергетики), *транспортні мережі* (магістральні та розподільчі електромережі, газо- й нафтопроводи), *системи управління та диспетчеризації* (SCADA-рішення, центри моніторингу і балансування), а також *критичні вузлові елементи* – підстанції та критичні точки розподілу, від яких залежить стабільність енергетичних потоків.

З позицій безпеки найбільш уразливими є об'єкти генерації, високовольтні підстанції, диспетчерські центри та кіберфізичні комплекси управління технологічними процесами [23]. В умовах збройної агресії рівень їх уразливості суттєво зростає. За офіційною інформацією Міністерства енергетики України, "за три роки повномасштабної війни було пошкоджено понад 63 тисячі об'єктів енергетичної інфраструктури, а тільки у 2024 році масовані удари та щоденні точкові обстріли об'єктів енергетичної інфраструктури призвели до втрати близько 10 ГВт генеруючої потужності" [24]. Ці дані наочно демонструють масштаб загроз і об'єктивну потребу в цілеспрямованих заходах захисту.

Для кримінально-правового аналізу принципове значення має *розмежування між діючою (експлуатованою) енергетичною інфраструктурою та проєктами її захисту*. Таке розмежування безпосередньо впливає на кваліфікацію діянь, оскільки зловживання у процесі реалізації захисних проєктів мають інший характер суспільної небезпеки, іншу логіку вчинення та специфічні ознаки суспільної небезпечності й відмінні підходи до кримінально-правової оцінки порівняно з посяганнями на об'єкти, що вже перебувають в експлуатації.

Діюча енергетична інфраструктура охоплює сукупність технічних засобів, мереж і систем, які забезпечують безперервне виробництво, передачу та розподіл енергії в режимі реального часу. Натомість *проєкти захисту енергетичної інфраструктури* слід розглядати як комплекс організаційних, інженерних і технологічних заходів, спрямованих на відновлення, модернізацію та підвищення фізичної, кібернетичної й операційної стійкості енергетичних об'єктів. До таких заходів належать постачання та монтаж трансформаторного і високовольтного обладнання, виконання будівельно-монтажних робіт, встановлення систем відеоспостереження й контролю доступу, інтеграція рішень захисту від БПЛА, а також упровадження спеціалізованих модулів безпеки у SCADA, EMS та ERP-системах[1].

Саме ці проєкти формують окреме коло вразливостей, які можна розглядати як самостійні криміногенні вузли. На етапі *закупівель* ризики пов'язані з використанням термінових процедур, дробленням контрактів, надмірно закритими або штучно звуженими технічними вимогами, а також можливими змовами між учасниками торгів [25]. На стадії виконання та приймання робіт проблеми *в контролі якості та прийманні робіт* часто виникають через відсутність повноцінних випробувань, неналежну фото- чи відеофіксацію, ігнорування лабораторних тестів, що створює передумови для фіктивного або часткового виконання зобов'язань. Такі обставини істотно ускладнюють подальшу кримінально-правову оцінку та доказування.

Додаткові ризики формуються у *ланцюгах постачання,* де залучення транзитних компаній, непрозорих субпідрядників і складна логістика можуть призводити як до втрати обладнання, так і до реалізації схем відмивання коштів. Особливе місце займає *кіберкомпонент*. Лог-фай-

[1] SCADA (Supervisory Control and Data Acquisition) – це система диспетчерського керування та збору даних; використовується для моніторингу й контролю технологічних процесів в енергетиці (мережі, підстанції, обладнання); EMS (Energy Management System) – система керування енергосистемою; оптимізує виробництво, розподіл, балансування, прогнозування навантажень; ERP (Enterprise Resource Planning) – система планування ресурсів підприємства; охоплює управління персоналом, фінансами, закупівлями, логістикою, техобслуговуванням.

ISSN 1995-6134

ли SCADA та ICS-систем (журнали технологічних операцій), дані ERP (про управління ресурсами, закупівлі та платежі) щодо закупівель і платежів, а також інформація з систем електронного документообігу мають істотне значення для встановлення фактичних обставин і кримінально-правової оцінки відповідних діянь. Їх неналежне збереження або контроль створює ризики спотворення або втрати інформації, що може ускладнювати кримінально-правову оцінку відповідних правопорушень [26]. Окремим криміногенним чинником виступає *масштабність фінансування* таких проєктів, що підвищує ймовірність завищення вартості робіт, дублювання платежів чи використання фіктивних підрядних структур.

Таким чином, у центрі кримінального аналізу перебуває *неправомірна поведінка, спрямована на отримання незаконної вигоди або зловживання службовим становищем у процесі реалізації проєктів захисту енергетичної інфраструктури,* а також кримінально-правові механізми реагування на неправомірну поведінку у сфері реалізації проєктів захисту енергетичної інфраструктури.

Окремої уваги потребує експериментальний характер таких проєктів. У Звіті Рахункової палати зазначається реалізація "експериментального проєкту із захисту критичної інфраструктури паливно-енергетичного сектору" [3]. Відповідний статус закріплений Постановою Кабінету Міністрів України від 07.02.2025 р. № 142, якою запроваджено спеціальний режим для нового будівництва, реконструкції, капітального ремонту, технічного переоснащення та впровадження інженерно-технічних рішень із захисту об'єктів критичної інфраструктури енергетики, залізничного транспорту та систем життєзабезпечення [27].

До повномасштабної війни експериментальні режими в енергетиці України застосовувалися переважно у сфері ринку електроенергії, цифровізації обліку, розвитку "розумних мереж" і впровадження європейського енергетичного acquis. Йшлося про пілотні проєкти смарт-мереж, окремі кіберініціативи за участі USAID, NREL чи ENTSO-E, а також експерименти з інтеграції відновлюваних джерел енергії. Водночас не існувало державних експериментальних проєктів, спрямованих саме на комплексну інтеграцію фізичного захисту, протиповітряної оборони, кібербезпеки, систем раннього виявлення та моделей безперервності енергопостачання в умовах реальних бойових дій.

У сучасному контексті *експериментальність таких проєктів є якісно новим явищем,* пов'язаним із трансформацією сектору безпеки та необхідністю тестування інтегрованих рішень захисту енергетики в умовах війни. *Експериментальний проєкт у цій сфері слід розглядати як спеціальний правовий режим, створений для апробації комплексних інженерних, кібернетичних і організаційних рішень на конкретних об'єктах.* Він передбачає обмежений масштаб упровадження, спрощені процедури закупівель, прискорене погодження технічних рішень і поєднання різнорівневих систем безпеки. У результаті держава отримує емпіричну та аналітичну базу, необхідну для формування національних стандартів багаторівневого захисту енергетичної інфраструктури та їх подальшого масштабування.

Стан реалізації багаторівневого захисту енергетичних об'єктів України: організаційні, управлінські та практичні аспекти

В умовах повномасштабної збройної агресії російської федерації питання захисту енергетичної інфраструктури набуло для України не лише галузевого, а й загальнодержавного значення. Формування та впровадження системи багаторівневого захисту енергетичних об'єктів фактично стало одним із ключових напрямів державної політики у сфері національної безпеки, оскільки стабільне функціонування енергосистеми безпосередньо впливає на обороноздатність держави, життєзабезпечення населення та економічну стійкість країни.

За *інформацією, оприлюдненою Державним агентством відновлення та розвитку інфраструктури* 20 листопада 2023 року, комплекс заходів із фізичного укріплення енергетичних об'єктів було вибудувано за трирівневою моделлю. Перший рівень передбачає використання відносно простих і швидких у реалізації інженерних рішень, зокрема спорудження габіонів та захисних бар'єрів із біг-бегів. Такі конструкції дозволили знизити ризики ураження об'єктів уламками ракет і безпілотних літальних апаратів. Загалом у межах цього рівня було укріплено 90 енергетичних об'єктів у 21 області.

Другий рівень захисту орієнтований на протидію більш цілеспрямованим атакам, зокрема застосуванню дронів-камікадзе та БпЛА типу "шахед". Починаючи з березня 2023 року, навколо критично важливих елементів мережі НЕК "Укренерго" розпочалося зведення спеціальних бетонних конструкцій. У результаті таких робіт захист було забезпечено для 22 підстанцій та 63 автотрансформаторів у 14 областях України.

ISSN 1995-6134

Третій рівень передбачає реалізацію найбільш складних інженерних рішень, розрахованих на протидію прямим ракетним ударам. Відповідні роботи здійснюються на 22 підстанціях, при цьому всі проєктні рішення підлягають обов'язковому погодженню з Генеральним штабом Збройних Сил України та Державною службою України з надзвичайних ситуацій. До підготовки й оцінювання таких проєктів залучалися матеріали та технічні рекомендації фахівців Великої Британії та США [28].

Відповідно до відкритих даних того ж державного органу, перший рівень укриттів станом на відповідний період було реалізовано на всіх об'єктах енергетичної системи України. Заходами другого рівня охоплено 84 ключові об'єкти НЕК "Укренерго", які було розподілено на три черги реалізації. У межах першої черги 69 об'єктів уже повністю укріплено, ще на 13 об'єктах роботи перебувають на завершальній стадії. Паралельно розпочато впровадження елементів третього рівня захисту – довготривалих інженерних укриттів, здатних витримувати ракетні удари, які мають забезпечити додаткову безпеку 22 підстанцій [29].

Разом із тим, попри масштабність і публічну демонстрацію здійснюваних заходів, питання реальної ефективності їх багаторівневого захисту залишається дискусійним і потребує комплексної правової оцінки з урахуванням фактичних результатів, рівня використання бюджетних коштів та відповідності обраних механізмів заявленим цілям забезпечення енергетичної безпеки.

Показовим у цьому контексті є ракетний обстріл у ніч на 8 листопада 2025 року, внаслідок якого було зупинено роботу двох теплоелектростанцій державної компанії "Центренерго" – Зміївської ТЕС у Харківській області та Трипільської ТЕС у Київській області [30]. Цей факт переконливо свідчить про те, що навіть за наявності системи укріплень енергетичні об'єкти залишаються вразливими до ударів високої інтенсивності. Зазначене актуалізує питання реальної ефективності багаторівневого захисту, запровадження якого раніше було задекларовано на державному рівні як інноваційного механізму мінімізації наслідків ворожих атак на цивільну енергетичну інфраструктуру [31].

Подальший розвиток цієї політики був закріплений рішенням Ради національної безпеки і оборони України від 17 жовтня 2023 року, яке Президент України увів у дію. Цим рішенням Кабінет Міністрів України було зобов'язано у стислі строки забезпечити належний інженерний та фізичний захист об'єктів критичної інфраструктури, збільшити кількість і посилити спроможність вогневих груп Сил оборони, що здійснюють їх прикриття та охорону, створити умови для захисту персоналу і проведення евакуаційних заходів, сформувати резерви обладнання та запасних частин для оперативного відновлення, а також забезпечити збереження документації на унікальне обладнання й архівування критичних баз даних [31]. У сукупності ці заходи формують системний підхід до підвищення стійкості енергетичної інфраструктури в умовах воєнних дій.

Як зазначається, з технічного погляду *трирівнева система захисту* ґрунтується на положеннях профільних нормативних актів і стандартів. Перший рівень передбачає застосування тимчасових конструкцій, які здатні частково захистити об'єкти від уламків ракет і поодиноких непрямих ударів безпілотників. Другий рівень охоплює інженерні споруди, розраховані на витримування прямих влучань дронів-камікадзе та непрямих ракетних ударів. Третій рівень представлений спеціальними сталебетонними спорудами бункерного типу, зазвичай заглибленими або напівзаглибленими, які призначені для захисту від прямих ракетних ударів. Такі об'єкти є складними й тривалими у будівництві, тому переважно застосовуються для нових або переміщуваних енергетичних станцій і на теперішній час здебільшого перебувають на стадії спорудження [32; 33].

Для більш повного розуміння специфіки українського підходу доцільно звернутися до зарубіжного досвіду захисту критичної інфраструктури. У Європейському Союзі діє регуляторна модель, закріплена в EU Directive 2008/114/EC, яка встановлює загальні підходи до ідентифікації, класифікації та захисту об'єктів критичної інфраструктури, а також передбачає обов'язкове оцінювання ризиків і налагодження міжвідомчої координації [34]. У Сполучених Штатах Америки функціонує система стандартів NERC CIP, спрямована на забезпечення як фізичної, так і кібербезпеки енергетичних систем, зокрема шляхом регулювання доступу, захисту мережевої інфраструктури та чіткого реагування на інциденти [35]. Ізраїль застосовує інтегровану модель захисту енергетики, що поєднує системи протиповітряної оборони, засоби раннього виявлення загроз і комплексну кібербезпеку. Такий підхід дозволяє оперативно реагувати як на повітряні атаки, так і на кіберінциденти, підт-

ISSN 1995-6134

римуючи стабільність енергетичного сектору в умовах постійної загрози [36].

Узагальнення наведених даних дає змогу оцінити масштаб і складність впровадження в Україні багаторівневих систем захисту енергетичної інфраструктури. Водночас воно переконливо демонструє, що попри активні зусилля з модернізації, результативність таких систем значною мірою залежить від якості технологічних рішень, рівня інтеграції фізичних і кіберкомпонентів, швидкості реагування на загрози та відповідності міжнародним стандартам. За цих умов удосконалення підходів до проєктування й оцінювання захисних систем набуває особливого значення для забезпечення енергетичної стійкості держави, що є особливо актуальним з огляду на виявлені Рахунковою палатою істотні порушення у реалізації проєктів із захисту об'єктів критичної енергетичної інфраструктури [3–5].

Саме тому в зазначеному контексті зростає актуальність аналізу кримінально-правових аспектів реалізації проєктів захисту енергетичної інфраструктури України. Правові ризики можливих зловживань безпосередньо впливають не лише на ефективність впроваджених інженерних рішень, а й на загальний рівень безпеки енергетичного сектору. Перехід до цього виміру дослідження дає змогу виявити типові злочинні прояви, окреслити межі відповідальності та сформувати практичні орієнтири для їх правильної правової кваліфікації.

Кримінально-правові аспекти реалізації проєктів захисту енергетичної інфраструктури України: типові склади злочинів і практика кваліфікації

Правова оцінка дій, пов'язаних із реалізацією проєктів захисту енергетичної інфраструктури України, завжди ґрунтується на аналізі реального змісту цих дій, їх суб'єктивної сторони, зокрема наявності умислу та мотивів, а також на масштабі й характері наслідків, яких вони спричинили. Водночас кримінально-правовий аналіз у цій сфері неможливий без урахування її технічної специфіки. Кожне рішення щодо закупівлі обладнання, виконання монтажних робіт чи інтеграції захисних систем повинно відповідати вимогам технічних регламентів, галузевих стандартів НКРЕКП, положенням ДСТУ, стандартам IEC, а також правилам фізичного та кібернетичного захисту. Відхилення від цих вимог у багатьох випадках стає первинним сигналом можливого кримінального правопорушення та зумовлює необхідність залучення спеціальних технічних і галузевих експертиз у межах досудового розслідування.

Загалом досудові розслідування у сфері енергетики охоплюють широкий спектр протиправних діянь. Йдеться не лише про розкрадання палива чи зловживання під час здійснення державних закупівель, а й про саботаж, корупційні практики на об'єктах критичної інфраструктури, а також кіберзлочини, кількість яких істотно зросла після початку повномасштабної збройної агресії. Розслідування таких правопорушень здійснюють різні правоохоронні органи залежно від суб'єктного складу та характеру злочину: Державне бюро розслідувань – у справах щодо посадових осіб, Національне антикорупційне бюро України – у провадженнях корупційної спрямованості, Національна поліція України – у справах про крадіжки, шахрайства та інші загальнокримінальні правопорушення.

Найбільш поширеними у практиці правоохоронних органів злочинами, пов'язаними з реалізацією енергетичних проєктів, залишаються діяння, передбачені статтею 191 Кримінального кодексу України [15]. Йдеться про привласнення або розтрату майна, що, як правило, проявляється у нецільовому використанні чи фактичному привласненні бюджетних коштів, виділених на відновлення або захист енергетичної інфраструктури. Типовими доказами у таких кримінальних провадженнях є виведення коштів на фіктивні або транзитні компанії, відсутність реального виконання робіт, а також маніпуляції під час закупівлі обладнання чи проведення модернізаційних робіт на підстанціях і захисних спорудах. У подібних ситуаціях слідчі, як правило, ставлять перед експертами питання щодо відповідності договірної вартості фактичним обсягам робіт, а також щодо наявності ознак умисного завищення цін.

Окремої уваги потребують корупційні ризики у сфері військово-енергетичних закупівель, коли захисні системи встановлюються в умовах обмеженого часу та термінового фінансування. У таких випадках особливого значення набуває правильне врахування специфіки спрощених процедур закупівель і спеціального порядку контролю, оскільки саме в цих умовах зловживання можуть маскуватися під об'єктивні потреби воєнного часу, що ускладнює їх правову оцінку.

Стаття 364 Кримінального кодексу України, яка передбачає відповідальність за зловживання владою або службовим становищем, застосовується у випадках, коли посадові особи формально погоджують проєктну документацію, свідомо ігнорують зауваження, виявлені під час

ISSN 1995-6134

технічних перевірок, або укладають договори з підрядниками, які не мають необхідних технічних ресурсів і компетенцій. Унаслідок таких дій затверджуються технічні рішення, що не відповідають вимогам безпеки, або приймаються роботи, які фактично не забезпечують належного рівня захисту енергетичних об'єктів. Подібна практика може мати тяжкі наслідки: у 2022–2023 роках фіксувалися випадки, коли окремі енергетичні об'єкти отримували офіційне погодження щодо незавершених або неправильно змонтованих охоронних систем, що створювало реальні ризики диверсійного впливу або техногенних аварій.

Для належної правової кваліфікації таких діянь принципово важливою є взаємодія слідчих органів із технічними регуляторами та системними операторами енергоринку, зокрема з НЕК "Укренерго" та Міністерством енергетики України. Саме ці суб'єкти можуть надати фахові роз'яснення щодо технологічної коректності виконаних робіт, відповідності встановлених систем чинним стандартам і реального рівня їх ефективності.

Стаття 367 Кримінального кодексу України, яка встановлює відповідальність за службову недбалість, охоплює випадки неналежного виконання службових обов'язків, що призвело до порушення роботи об'єктів критичної інфраструктури або створило загрозу безпеці держави. У межах відповідних кримінальних проваджень слідчі з'ясовують, чи відповідали дії або бездіяльність посадових осіб, відповідальних за встановлення, налаштування та експлуатацію захисних систем, вимогам технічних і нормативних документів.

У сфері кібербезпеки особливої актуальності набуває застосування статті 361 Кримінального кодексу України, яка передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних систем. Такі правопорушення можуть полягати у зламі SCADA-комплексів, модифікації сигналів моніторингу або отриманні доступу до критичних даних без відповідного дозволу. У цих випадках слідчий встановлює не лише сам факт несанкціонованого доступу, а й його вплив на стабільність і безпеку функціонування енергетичного об'єкта.

Стаття 366 Кримінального кодексу України застосовується у справах, пов'язаних зі службовим підробленням технічних паспортів, актів виконаних робіт, сертифікатів якості та іншої документації. Наявність такого правопорушення, як правило, підтверджується експертними висновками, які фіксують розбіжності між заявленими характеристиками та фактичним станом обладнання [37]. До цієї ж категорії належать і кіберзлочини, пов'язані з підробленням або видаленням лог-файлів у системах SCADA чи ERP, що можуть кваліфікуватися як неправомірний доступ до інформації або її знищення.

Окрему групу становлять злочини, передбачені статтями 111–114 Кримінального кодексу України, зокрема державна зрада, диверсія та інші посягання на обороноздатність. Вони застосовуються у тих випадках, коли дії службових осіб або пов'язаних із ними суб'єктів об'єктивно сприяють ворогові або створюють загрозу енергопостачанню військових частин і об'єктів критичної інфраструктури. В умовах воєнного стану окремі посягання можуть кваліфікуватися як диверсійні залежно від спрямованості умислу, характеру дій та тяжкості наслідків.

Важливою складовою кримінально-правового аналізу є встановлення повного складу злочину у випадках, коли дії фізичних осіб або підрядних організацій призвели до матеріальних збитків або створили реальну загрозу функціонуванню об'єктів критичної інфраструктури. У таких провадженнях до суду подаються клопотання про призначення комплексних експертиз із метою визначення розміру шкоди, встановлення причинно-наслідкового зв'язку між діями обвинувачених і заподіяними наслідками, а також оцінки ступеня їхньої вини.

Ефективне застосування норм кримінального права у цій сфері можливе лише за умови поєднання різних видів доказів, зокрема результатів фінансово-економічних, технічних і кіберекспертиз, показань працівників, аналізу первинної документації та результатів аудиту контрактів. Сукупність таких доказів формує повноцінну доказову базу, яка дозволяє правильно кваліфікувати правопорушення та забезпечити захист державних інтересів у сфері енергетичної безпеки [15; 38].

Разом із тим, на практиці слідчі органи стикаються з двома системними проблемами. По-перше, це складність доведення умислу у специфічних господарських відносинах, де необхідно чітко відмежувати допустимий економічний ризик від кримінально караного порушення. По-друге, це проблема збереження цифрових доказів, зокрема логів і метаданих, які нерідко модифікуються або знищуються ще до офіційного початку досудового розслідування.

Додатковий виклик пов'язаний із кримінально-правовою оцінкою використання міжнародної

ISSN 1995-6134

технічної допомоги та обладнання, переданого Україні для підвищення енергетичної стійкості. У випадках нецільового використання такого обладнання або його неналежного монтажу відповідальність може наставати не лише за злочини проти власності чи службові правопорушення, а й за порушення міжнародних зобов'язань, що потребує залучення донорських структур і міжнародних аудиторів.

Отже, кримінально-правовий вимір реалізації проєктів захисту енергетичної інфраструктури охоплює цілу сукупність правопорушень: від економічних злочинів, пов'язаних із нецільовим використанням бюджетних коштів, до службово-технічних порушень правил встановлення та експлуатації захисних систем, а також кіберзагроз, що полягають у несанкціонованому втручанні в системи управління. Такий комплексний підхід дозволяє сформувати дієві механізми реагування й запобігання зловживанням, мінімізуючи ризики для об'єктів критично важливої енергетичної інфраструктури.

Висновки

1. Проведене дослідження підтверджує, що захист критичної енергетичної інфраструктури України в умовах повномасштабної збройної агресії є комплексним міждисциплінарним завданням, яке виходить за межі технічних і організаційних рішень та формує специфічні кримінально-правові ризики, пов'язані з реалізацією масштабних проєктів захисту в умовах воєнного стану. Реалізація масштабних проєктів захисту в умовах воєнного стану, поєднана зі значними фінансовими ресурсами, спрощеними процедурами та цифровізацією, об'єктивно підвищує ймовірність зловживань і ускладнює їх виявлення та доказування.

2. Установлено, що правове регулювання у сфері захисту енергетичної інфраструктури має багаторівневий і міжгалузевий характер, а його ефективність значною мірою залежить від узгодженого застосування норм різних галузей права та належної міжвідомчої взаємодії. Проєкти захисту енергетичних об'єктів формують самостійний криміногенний простір, у межах якого концентрація ризиків відбувається на етапах планування, закупівель, виконання та приймання робіт.

3. Доведено, що кримінально-правова характеристика зловживань у цій сфері охоплює широкий спектр злочинів – від корупційних і майнових до службових і кіберзлочинів, а їх належна кваліфікація потребує врахування технічної специфіки об'єктів, особливостей воєнного режиму та застосування комплексної кримінально-правової оцінки з урахуванням технічної специфіки об'єктів і умов воєнного режиму.

4. Встановлено, що основними практичними проблемами розслідування є складність доведення умислу в технічно складних процесах, обмеженість контрольних процедур в умовах воєнного стану та ризики втрати або спотворення цифрових доказів, що зумовлює необхідність раннього залучення галузевих фахівців та застосування сучасних експертних методів.

5. Практична значущість дослідження полягає у формуванні комплексного кримінально-правового підходу до аналізу зловживань у проєктах захисту енергетичної інфраструктури України, який може бути використаний у правозастосовній практиці та слугувати підґрунтям для подальшого розвитку методик розслідування злочинів у сфері енергетичної безпеки.

Конфлікт інтересів

Автор заявляє про відсутність потенціального конфлікту інтересів, пов'язаного з його обов'язками як члена редколегії, що могло би стати причиною упередженості дослідження. Стаття піддана незалежному рецензуванню відповідно до правил журналу. При підготовці статті цифрові редакторські засоби використовувалися винятково для стилістичного редагування без втручання в науковий зміст.

Вираз вдячності

Дослідження виконано відповідно до планів науково-дослідних робіт Харківського національного університету внутрішніх справ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ефективність діяльності Національного антикорупційного бюро України: Звіт за результатами зовнішньої незалежної оцінки (аудиту). 02.05.2025. 99 с. https://www.kmu.gov.ua/storage/app/sites/1/otsinka_nabu/finalnyi-zvit-ukr.pdf
2. Білоус О. Ключові судові рішення у сфері енергетики. 18.07.2024. https://lcf.ua/thought-leadership/litigation/klyuchovi-sudovi-rishennya-u-sferi-energetiki/
3. Рахункова палата України. *Звіт за результатами аудиту: Реалізація експериментального проєкту із захисту критичної інфраструктури паливно-енергетичного сектору.* 15.10.2025. https://rp.gov.ua/PressCenter/News/?id=2804 (дата звернення: 15.10.2025).

ISSN 1995-6134

4. Yur-gazeta. *Рахункова палата виявила системні порушення під час реалізації проєкту із захисту енергетичної інфраструктури.* 13.10.2025. https://yur-gazeta.com/golovna/rahunkova-palata-viyavila-sistemni-porushennya-pid-chas-realizaciyi-proektu-iz-zahistu-energetichnoy.html (дата звернення: 15.10.2025).
5. Delo.ua. *Захист енергетичної інфраструктури: аудит Рахункової палати виявив недоліки експериментального проєкту.* 13.10.2025. https://delo.ua/news/zaxist-energeticnoyi-infrastrukturi-audit-raxunkovoyi-palati-viyaviv-nedoliki-eksperimentalnogo-projektu-453843/ (дата звернення: 15.10.2025).
6. Клят Ю., Соломицький О., Семененко О., Водчиць О., Войцеховський Р., Поливода М. Визначення та класифікація загроз енергетичній безпеці України в сучасних умовах військових викликів. *Social Development and Security.* 2024. Vol. 14. No. 2. С. 272-285. https://doi.org/10.33445/sds.2024.14.2.22
7. Ус Ю. В., Литовченко В. О. Реалізація стратегії управління енергетичною безпекою підприємств в умовах зростаючої нестабільності: організаційний аспект. *Бізнес-інформ.* 2024. № 9. С. 314-320. https://doi.org/10.32983/2222-4459-2024-9-313-320
8. Зозуля І. В. Безпека та захист об'єктів критичної інфраструктури України в умовах воєнних руйнувань. *Оперативно-бойова діяльність сил сектору безпеки і оборони в умовах воєнного стану:* матеріали Всеукраїнської наук.-практ. конф., (м. Київ, 30 жовт. 2025 р.). Київ: НА СБУ, 2025. Вип. 2. С. 91-94.
9. Ліпін Ю. О. Розслідування заволодіння майном шляхом зловживання службовим становищем у паливно-енергетичному комплексі України: дис. … докт. філос.: 081-Право. Київ, 2021. 302 с. https://elar.navs.edu.ua/items/e86f603d-ec4a-409c-9bb2-131b978866a5
10. Корж В. Криміналістична характеристика економічних злочинів, скоєних організованими групами з корупційними зв'язками. *Теорія та практика судової експертизи і криміналістики.* 2024. Вип. 2 (35). С. 44-57. https://doi.org/10.32353/khrife.2.2024.04
11. Неклеса О. В. Окремі аспекти документування злочинів вчинених у сфері публічних закупівель в умовах воєнного стану. *Протидія організованій злочинності: проблеми теорії та практики:* матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 09 грудня 2022 р.). Дніпро: ДДУВС, 2022. С. 63-65. https://er.dduvs.edu.ua/handle/123456789/15411
12. Гирич О. С. Кримінальна відповідальність за вчинення правопорушень у сфері енергетичної безпеки за законодавством країн Європейського Союзу. *Юридичний науковий електронний журнал.* 2024. № 9. С. 293-295. https://doi.org/10.32782/2524-0374/2024-9/69
13. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України.* 2023. № 5. Ст. 13. https://zakon.rada.gov.ua/laws/show/1882-20#Text
14. Про публічні закупівлі: Закон України від 25.12.2015 № 922-VIII. *Відомості Верховної Ради України.* 2016. № 9. ст. 89. https://zakon.rada.gov.ua/laws/show/922-19#Text
15. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25-26. Ст. 131. https://zakon.rada.gov.ua/laws/show/2341-14/conv#Text
16. Про ринок електричної енергії: Закон України від 13.04.2017 № 2019-VIII. *Відомості Верховної Ради України.* 2017. № 27-28. Ст. 312. https://zakon.rada.gov.ua/laws/show/2019-19#Text
17. Про землі енергетики та правовий режим спеціальних зон енергетичних об'єктів: Закон України від 09.07.2010 № 2480-VI. *Відомості Верховної Ради України.* 2011. № 1. ст. 1. https://zakon.rada.gov.ua/laws/show/2480-17#Text
18. В Україні відбувається понад 20 обшуків у справі про зловживання на відновленні енергетичної інфраструктури – СБУ. 05.09.2023. https://ua.interfax.com.ua/news/general/932989.html?utm_source=chatgpt.com
19. Трохимець О. Судові спори в сфері енергетики. Роттердам+. 27.10.2022. https://unba.org.ua/publications/print/7663-sudovi-spori-v-sferi-energetiki-rotterdam.html?utm_source=chatgpt.com
20. Заволодіння коштами ДП "СхідГЗК" та НАЕК "Енергоатом". 23.05.2018. https://nabu.gov.ua/news/novyny-zavolodinnya-koshtamy-dp-shidgzk-ta-naek-energoatom/?utm_source=chatgpt.com
21. СБУ та НАБУ за сприяння Міністра енергетики України затримали його заступника на хабарі у пів мільйона доларів (відео). 12.08.2024. https://ssu.gov.ua/novyny/sbu-ta-nabu-za-spryiannia-ministra-enerhetyky-ukrainy-zatrymaly-yoho-zastupnyka-na-khabari-u-piv-miliona-dolariv-video
22. Зозуля, І. В. (2024). Правові підходи до організації ліквідації наслідків спричиненого воєнними діями руйнування інфраструктури та її відновлення. *Форум Права, 80*(3), 91–109. http://doi.org/10.5281/zenodo.12591874
23. European Union Agency for Cybersecurity (ENISA). *Cybersecurity of Critical Sectors.* ENISA, 2025.

ISSN 1995-6134

https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors
24. Стабільне проходження минулої зими – перемога для всієї енергетичної галузі. 09.04.2025. https://mev.gov.ua/novyna/stabilne-prokhodzhennya-mynuloyi-zymy-peremoha-dlya-vsiyeyi-enerhetychnoyi-haluzi
25. U.S. Agency for International Development, Office of Inspector General. (2025). Action Needed to Enhance Oversight of Energy Procurements: Ukraine Response (Audit Report 8-121-25-002-P). 28.03.2025. https://oig.usaid.gov/sites/default/files/2025-04/Final%20Audit%20Report%20-%20Ukraine%20Response__Action%20Needed%20to%20Enhance%20Oversight%20of%20Energy%20Procurements%20-%208-121-25-002-P.pdf
26. Study on Cybersecurity in the energy sector of the Energy Community – Final Report Document no.: FINR-CS-EC-121019. Blueprint Energy Solutions GmbH December 2019. https://www.energy-community.org/dam/jcr%3Adb8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf
27. Про реалізацію експериментального проекту щодо нового будівництва, реконструкції, капітального ремонту, ремонту та інших інженерно-технічних заходів із захисту об'єктів критичної інфраструктури паливно-енергетичного сектору, підсектору залізничного транспорту сектору транспорту і пошти, сектору систем життєзабезпечення критичної інфраструктури: Постанова Кабінету Міністрів України від 07.02.2025 № 142. https://zakon.rada.gov.ua/laws/show/142-2025-п#Text
28. Васьків О. Енергооб'єкти в Україні отримали три рівні захисту від ракет і дронів. 20.11.2023. https://suspilne.media/621497-energoobekti-v-ukraini-otrimali-tri-rivni-zahistu-vid-raket-i-droniv/
29. Абакумова Ю., Тибінь Г. Сергій Сухомлин, голова Агентства відновлення. Будівництво Миколаївського водогону обійдеться на понад 3 мільярди гривень дешевше. 13.02.2025. https://www.ukrinform.ua/rubric-vidbudova/3959493-sergij-suhomlin-golova-agentstva-vidnovlenna.html
30. Михайлов Д. Усі теплоелектростанції Центренерго зупинилися після ударів РФ. 08.11.2025. https://suspilne.media/1159716-usi-teploelektrostancii-centrenergo-zupinilisa-pisla-udariv-rf/
31. Богданьок О. Україна перша у світі запроваджує багаторівневий захист цивільної енергетичної інфраструктури – Галущенко. 30.10.2023. https://suspilne.media/605847-ukraina-persa-u-sviti-zaprovadzue-bagatorivnevij-zahist-civilnoi-energeticnoi-infrastrukturi-galusenko/
32. Гудкова С. Як можна захистити ТЕС, якщо жодна ППО у світі не працює на 100 %? Виявляється, рішення вже є. 18.04.2024. https://zaborona.com/yak-mozhna-zahystyty-tes-rishennya-vzhe-ye/
33. Зюбанова Е. Я., Кальченко Я. Ю. Аналіз методів захисту енергетичного комплексу України від обстрілів: *Оперативно-бойова діяльність сил сектору безпеки і оборони в умовах воєнного стану:* матеріали Всеукр. наук.-практ. конф., (м. Київ, 30 жовт. 2025 р.). Київ: НА СБУ, 2025. Вип. 2. С. 94-97.
34. Directive 2008/114/EC of the Council of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (2008). *Official Journal of the European Union, L 345/75.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114
35. Iii, Guillermo & El-Sheikh, Eman. (2022). NERC CIP Standards: Review, Compliance, and Training. In book: Global Perspectives on Information Security Regulations (pp.48-71). http://doi.org/10.4018/978-1-7998-8390-6.ch003
36. Kummerow, A., Williams, R. P., Sen, Ö., & Poblocka-Dirakis, A. (2025, June). *Digitalisation and cyber security in the energy sector: A comparative analysis between Germany and Israel* (German-Israeli Energy Partnership). Deutsche Energie-Agentur (dena). https://energypartnership-israel.org/fileadmin/israel/newsroom/Digitalisation_and_Cyber_Security_in_the_Energy_Sector.pdf
37. Зозуля І. Судово-експертна діяльність як ключовий елемент захисту критичної інфраструктури у секторі безпеки та оборони України. *Актуальні питання розвитку українського простору судово-експертної діяльності:* матеріали доповідей Міжнародної наук.-практ. конф. (м. Київ, 31 січня 2025 р.). Львів-Торунь: Liha-Pres, 2025. С. 92-99.
38. Про основні засади забезпечення функціонування критичної інфраструктури: Закон України від 15.07.2021 № 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20

REFERENCES

1. *Efektyvnist diialnosti Natsionalnoho antykoruptsiinoho biuro Ukrainy* [Efficiency of the National Anti-Corruption Bureau of Ukraine: Report on the Results of the External Independent Evaluation (Audit)]. Zvit za rezultatamy zovnishnoi nezalezhnoi otsinky (audytu). (2025, May 2). https://www.kmu.gov.ua/storage/app/sites/1/otsinka_nabu/finalnyi-zvit-ukr.pdf (in Ukr.).
2. Bilous, O. (2024, July 18). *Kliuchovi sudovi rishennia u sferi enerhetyky* [Key court decisions in the energy sector]. LCF Law Group. https://lcf.ua/thought-leadership/litigation/klyuchovi-sudovi-rishennya-u-sferi-

energetiki/ (in Ukr.).
3. Accounting Chamber of Ukraine. (2025, October 15). *Zvit za rezultatamy audytu: Realizatsiia eksperymentalnoho proiektu iz zakhystu krytychnoi infrastruktury palyvno-enerhetychnoho sektoru* [Audit report: Implementation of the pilot project on protection of critical infrastructure of the fuel and energy sector]. https://rp.gov.ua/PressCenter/News/?id=2804 (in Ukr.).
4. Yur-Gazeta. (2025, October 13). *Rakhunkova palata vyiavyla systemni porushennia pid chas realizatsii proiektu iz zakhystu enerhetychnoi infrastruktury* [The Accounting Chamber revealed systemic violations during the implementation of the energy infrastructure protection project]. https://yur-gazeta.com/golovna/rahunkova-palata-viyavila-sistemni-porushennya-pid-chas-realizaciyi-proektu-iz-zahistu-energetichnoy.html (in Ukr.).
5. Delo.ua. (2025, October 13). *Zakhyst enerhetychnoi infrastruktury: audyt Rakhunkovoi palaty vyiavyv nedoliky eksperymentalnoho proiektu* [Protection of energy infrastructure: audit of the Accounting Chamber revealed shortcomings of the pilot project]. https://delo.ua/news/zaxist-energeticnoyi-infrastrukturi-audit-raxunkovoyi-palati-viyaviv-nedoliki-eksperimentalnogo-projektu-453843/ (in Ukr.).
6. Kliat, Yu., Solomytskyi, O., Semenenko, O., Vodchyts, O., Voitsekhivskyi, R., & Polyvoda, M. (2024). Vyznachennya ta klasyfikatsiya zahroz enerhetychniy bezpetsi Ukrayiny v suchasnykh umovakh viyskovykh vyklykiv [Identification and classification of threats to Ukraine's energy security under modern military challenges]. *Social Development and Security, 14*(2), 272–285. https://doi.org/10.33445/sds.2024.14.2.22
7. Us, Yu. V., & Lytovchenko, V. O. (2024). Realizatsiia stratehii upravlinnia enerhetychnoiu bezpekoiu pidpryiemstv v umovakh zrostaiuchoi nestabilnosti: orhanizatsiinyi aspekt [Implementation of the enterprise energy security management strategy under increasing instability: organizational aspect]. *Biznes-Inform,* (9), 314–320. https://doi.org/10.32983/2222-4459-2024-9-313-320 (in Ukr.).
8. Zozulia, I. V. (2025). Bezpeka ta zakhyst obiektiv krytychnoi infrastruktury Ukrainy v umovakh voiennykh ruinuvan [Security and protection of critical infrastructure facilities of Ukraine under conditions of wartime destruction]. In: *Operational and combat activities of the security and defense sector forces under martial law* (pp. 91–94). Kyiv: National Academy of the Security Service of Ukraine (in Ukr.).
9. Lipin, Yu. O. (2021). *Rozsliduvannia zavolodinnia mainom shliakhom zlovzhyvannia sluzhbovym stanovyshchem u palyvno-enerhetychnomu kompleksi Ukrainy* [Investigation of misappropriation of property through abuse of official position in the fuel and energy complex of Ukraine] (Doctoral dissertation). Kyiv. https://elar.navs.edu.ua/items/e86f603d-ec4a-409c-9bb2-131b978866a5 (in Ukr.).
10. Korzh, V. (2024). Kryminalistychna kharakterystyka ekonomichnykh zlochyniv, skoienykh orhanizovanymy hrupamy z koruptsiinymy zviazkamy [Forensic characteristics of economic crimes committed by organized groups with corrupt ties]. *Theory and Practice of Forensic Science and Criminalistics, 2*(35), 44–57. https://doi.org/10.32353/khrife.2.2024.04 (in Ukr.).
11. Neklesa, O. V. (2022). Okremi aspekty dokumentuvannia zlochyniv, vchynenykh u sferi publichnykh zakupivel v umovakh voiennoho stanu [Certain aspects of documenting crimes committed in the field of public procurement under martial law]. In: *Counteraction to organized crime: theory and practice* (pp. 63–65). Dnipro: DDUVS. https://er.dduvs.edu.ua/handle/123456789/15411 (in Ukr.).
12. Hyrych, O. S. (2024). Kryminalna vidpovidalnist za vchynennia pravoporushen u sferi enerhetychnoi bezpeky za zakonodavstvom krain Yevropeiskoho Soiuzu [Criminal liability for offenses in the field of energy security under EU legislation]. *Legal Scientific Electronic Journal,* (9), 293–295. https://doi.org/10.32782/2524-0374/2024-9/69 (in Ukr.).
13. Pro krytychnu infrastrukturu [On Critical Infrastructure]. Law of Ukraine (16.11.2021 No. 1882-9). *Vidomosti Verkhovnoi Rady Ukrainy*, 2023, (5), 13. https://zakon.rada.gov.ua/laws/show/1882-20#Text (in Ukr.).
14. Pro publichni zakupivli [On Public Procurement]. Law of Ukraine (25.12.2015 No. 922-8). *Vidomosti Verkhovnoi Rady Ukrainy*, 2016, (9), 89. https://zakon.rada.gov.ua/laws/show/922-19#Text (in Ukr.).
15. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]. Law of Ukraine (05.04.2001 No. 2341-3). *Vidomosti Verkhovnoi Rady Ukrainy,* 2001, (25–26), 131. https://zakon.rada.gov.ua/laws/show/2341-14/conv#Text (in Ukr.).
16. Pro rynok elektrychnoi enerhii [On the Electricity Market]. Law of Ukraine (13.04.2017 No. 2019-8). *Vidomosti Verkhovnoi Rady Ukrainy,* 2017, (27–28), 312. https://zakon.rada.gov.ua/laws/show/2019-19#Text (in Ukr.).
17. Pro zemli enerhetyky ta pravovyi rezhym spetsialnykh zon enerhetychnykh obiektiv [On Energy Lands and the Legal Regime of Special Zones of Energy Facilities]. Law of Ukraine (09.07.2010 No. 2480-6). *Vidomosti Verkhovnoi Rady Ukrainy,* 2011, (1), 1. https://zakon.rada.gov.ua/laws/show/2480-

17#Text (in Ukr.).
18. Interfax-Ukraine. (2023, September 5). *V Ukraini vidbuvaietsia ponad 20 obshukiv u spravi pro zlovzhyvannia na vidnovlenni enerhetychnoi infrastruktury* [More than 20 searches are taking place in Ukraine in the case of abuses in the restoration of energy infrastructure – SBU]. https://ua.interfax.com.ua/news/general/932989.html (in Ukr.).
19. Trokhymets, O. (2022, October 27). *Sudovi spory v sferi enerhetyky. Rotterdam+.* [Court disputes in the energy sector. Rotterdam+]. Ukrainian National Bar Association. https://unba.org.ua/publications/print/7663-sudovi-spori-v-sferi-energetiki-rotterdam.html (in Ukr.).
20. National Anti-Corruption Bureau of Ukraine. (2018, May 23). Zavolodinnia koshtamy DP "SkhidHZK" ta NAEK "Enerhoatom" [Misappropriation of funds of SE "SkhidGZK" and NNEGC "Energoatom"]. https://nabu.gov.ua/news/novyny-zavolodinnya-koshtamy-dp-shidgzk-ta-naek-energoatom/ (in Ukr.).
21. Security Service of Ukraine. (2024, August 12). *SBU ta NABU za spryiannia Ministra enerhetyky Ukrainy zatrymaly yoho zastupnyka Na khabari u piv miliona dolariv* [The SBU and NABU, with the assistance of the Minister of Energy of Ukraine, detained his deputy for a bribe of half a million dollars (video)]. https://ssu.gov.ua/novyny/sbu-ta-nabu-za-spryiannia-ministra-enerhetyky-ukrainy-zatrymaly-yoho-zastupnyka-na-khabari-u-piv-miliona-dolariv-video (in Ukr.).
22. Zozulia, I. V. (2024). Pravovi pidkhody do orhanizatsiyi likvidatsiyi naslidkiv sprychynenoho voyennymy diyamy ruynuvannya infrastruktury ta yiyi vidnovlennya [Legal Approaches to Organizing the Liquidation of Consequences of Infrastructure Destruction Caused by Military Actions and Its Restoration]. *Forum Prava, 80*(3), 91–109. https://doi.org/10.5281/zenodo.12591874 (in Ukr.).
23. European Union Agency for Cybersecurity. (2025). *Cybersecurity of critical sectors*. ENISA. https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors
24. Ministry of Energy of Ukraine. (2025, April 9). *Stabilne prokhodzhennia mynuloi zymy – peremoha dlia vsiiei enerhetychnoi haluzi* [Stable passage of last winter is a victory for the entire energy sector]. https://mev.gov.ua/novyna/stabilne-prokhodzhennya-mynuloyi-zymy-peremoha-dlya-vsiyeyi-enerhetychnoyi-haluzi (in Ukr.).
25. U.S. Agency for International Development, Office of Inspector General. (2025, March 28). *Action needed to enhance oversight of energy procurements: Ukraine response* (Audit Report No. 8-121-25-002-P). https://oig.usaid.gov/sites/default/files/2025-04/Final%20Audit%20Report%20-%20Ukraine%20Response__Action%20Needed%20to%20Enhance%20Oversight%20of%20Energy%20Procurements%20-%208-121-25-002-P.pdf
26. Blueprint Energy Solutions GmbH. (2019). *Study on cybersecurity in the energy sector of the Energy Community – Final report* (FINR-CS-EC-121019). https://www.energy-community.org/dam/jcr%3Adb8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf
27. [*Pro realizatsiiu eksperymentalnoho proektu shchodo novoho budivnytstva, rekonstruktsii, kapitalnoho remontu…* [On the implementation of an experimental project on new construction, reconstruction, overhaul, repair and other engineering and technical measures to protect critical infrastructure facilities]. Resolution of the Cabinet of Ministers of Ukraine (07.02.2025 No. 142). https://zakon.rada.gov.ua/laws/show/142-2025-п#Text (in Ukr.).
28. Vaskiv, O. (2023, November 20). *Enerhoobiekty v Ukraini otrymaly try rivni zakhystu vid raket i droniv* [Energy facilities in Ukraine received three levels of protection against missiles and drones]. https://suspilne.media/621497-energoobekti-v-ukraini-otrimali-tri-rivni-zahistu-vid-raket-i-droniv/ (in Ukr.).
29. Abakumova, Yu., & Tybin, H. (2025, February 13). *Serhii Sukhomlyn, holova Ahentstva vidnovlennia. Budivnytstvo Mykolaivskoho vodohonu obiidetsia na ponad 3 miliardy hryven deshevshe* [Serhii Sukhomlyn, head of the Recovery Agency: construction of the Mykolaiv water pipeline will cost more than three billion hryvnias less]. https://www.ukrinform.ua/rubric-vidbudova/3959493-sergij-suhomlin-golova-agentstva-vidnovlenna.html (in Ukr.).
30. Mykhailov, D. (2025, November 8). *Usi teploelektrostantsii Tsentrenerho zupynylysia pislia udariv RF* [All thermal power plants of Centrenergo stopped after Russian strikes]. https://suspilne.media/1159716-usi-teploelektrostancii-centrenergo-zupinilisa-pisla-udariv-rf/ (in Ukr.).
31. Bohdaniok, O. (2023, October 30). *Ukraina persha u sviti zaprovadzhuie bahatorivnevyj zakhyst tsyvilnoi enerhetychnoi infrastruktury – Halushchenko* [Ukraine is the first in the world to introduce multi-level protection of civilian energy infrastructure – Halushchenko]. https://suspilne.media/605847-ukraina-persa-u-sviti-zaprovadzue-bagatorivnevij-zahist-civilnoi-energeticnoi-infrastrukturi-galusenko/ (in Ukr.).
32. Hudkova, S. (2024, April 18). *Yak mozhna zakhystyty TES, yakshcho zhodna PPO u sviti ne pratsiuie na 100 %? Vyiavliaietsia, rishennia vzhe ye* [How can TPPs be protected if no air defense system in the world works 100 %? It turns out solutions already exist]. https://zaborona.com/yak-mozhna-zahystyty-

tes-rishennya-vzhe-ye/ (in Ukr.).
33. Ziubanova, E. Ya., & Kalchenko, Ya. Yu. (2025). Analiz metodiv zakhystu enerhetychnoho kompleksu Ukrainy vid obstriliv [Analysis of methods for protecting Ukraine's energy complex from shelling]. In: *Operatyvno-boiova diialnist syl sektoru bezpeky i oborony v umovakh voiennoho stanu* (Vol. 2, pp. 94–97). Kyiv: National Academy of the Security Service of Ukraine (in Ukr.).
34. Council of the European Union. (2008). *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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114
35. Guillermo, I. I. I., & El-Sheikh, E. (2022). NERC CIP standards: Review, compliance, and training. In: *Global perspectives on information security regulations* (pp. 48–71). https://doi.org/10.4018/978-1-7998-8390-6.ch003
36. Kummerow, A., Williams, R. P., Sen, Ö., & Poblocka-Dirakis, A. (2025). *Digitalisation and cyber security in the energy sector: A comparative analysis between Germany and Israel*. Deutsche Energie-Agentur (Dena). https://energypartnership-israel.org/fileadmin/israel/newsroom/Digitalisation_and_Cyber_Security_in_the_Energy_Sector.pdf
37. Zozulia, I. (2025). Sudovo-ekspertna diialnist yak kliuchovyi element zakhystu krytychnoi infrastruktury u sektori bezpeky ta oborony Ukrainy [Forensic expert activity as a key element of critical infrastructure protection in Ukraine's security and defense sector]. In: *Aktualni pytannia rozvytku ukrainskoho prostoru sudovo-ekspertnoi diialnosti* (pp. 92–99). Lviv–Torun: Liha-Pres (in Ukr.).
38. Verkhovna Rada of Ukraine. (2021). *Pro osnovni zasady zabezpechennia funktsionuvannia krytychnoi infrastruktury* [On the basic principles of ensuring the functioning of critical infrastructure]. Zakon Ukrainy. (15.07.2021 No. 1882-9). https://zakon.rada.gov.ua/laws/show/1882-20 (in Ukr.).

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права: 84 pp. 106–119 (4).

Related identifiers:
10.5281/zenodo.17347755

http://forumprava.pp.ua/files/106-119-2025-4-FP-Zozulia_15.pdf

http://nbuv.gov.ua/UJRN/FP_index.htm_2025_4_15.pdf

License (for files):
Creative Commons Attribution 4.0 International

Received: 31.10.2025
Accepted: 24.11.2025
Published: 28.11.2025
Available online: 28.11.2025

Cite as:

Зозуля, І. В. (2025). Правові та кримінально-правові аспекти реалізації проєктів захисту енергетичної інфраструктури України. *Форум Права, 84*(4), 106-119. http://doi.org/10.5281/zenodo.17347755

Zozulia, I. V. (2025). Pravovi ta kryminalno-pravovi aspekty realizatsiyi proyektiv zakhystu enerhetychnoyi infrastruktury Ukrayiny [Legal and Criminal Law Aspects of the Implementation of Energy Infrastructure Protection Projects in Ukraine]. *Forum Prava, 84*(4), 106–119. http://doi.org/10.5281/zenodo.17347755