



УДК 343.3:351.78

[https://doi.org/10.52058/2786-6300-2024-10\(28\)-472-487](https://doi.org/10.52058/2786-6300-2024-10(28)-472-487)

Предместніков Олег Гарійович доктор юридичних наук, професор, заслужений юрист України, завідувач кафедри права Мелітопольського державного педагогічного університету імені Богдана Хмельницького, пр-т Наукове місто, 59, м. Запоріжжя, 69000, <https://orcid.org/0000-0001-8196-647X>

Охман Ольга Василівна кандидат юридичних наук, доцент кафедри права та правоохоронної діяльності, Хмельницький інститут імені Блаженнішого Володимира, Митрополита Київського і всієї України ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», Проспект Миру, 101 А, м. Хмельницький, 29015, <https://orcid.org/0000-0002-9509-5326>

Пархета Вікторія Іванівна доктор філософії зі спеціальності 081 «Право», доцент кафедри соціальних і правових дисциплін, Уманський державний педагогічний університет імені Павла Тичини, вул. Садова, 2, м. Умань, 20300, <https://orcid.org/0000-0003-2774-4790>

ПРОТИДІЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ПРЕДМЕТ НАУКОВОГО ДОСЛІДЖЕННЯ: ТЕОРЕТИЧНИЙ АСПЕКТ

Анотація. Стаття присвячена теоретичному аналізу кримінальних правопорушень та їх протидії на об'єктах критичної інфраструктури в Україні. Актуальність дослідження зумовлена зростаючою загрозою для критичної інфраструктури країни, особливо в умовах війни, а також необхідністю удосконалення правової та організаційної бази для її захисту.

Мета статті – дослідити теоретичні аспекти протидії кримінальним правопорушенням на об'єктах критичної інфраструктури та запропонувати рекомендації для підвищення ефективності цих заходів.

В процесі дослідження використано наступні загальнонаукові методи пізнання: аналіз, синтез, систематизація та порівняння. Для досягнення цілей дослідження виконано низку завдань: визначено сутність поняття «кримінальне правопорушення» та «протидія кримінальним правопорушенням», а також мету та завдання протидії кримінальним правопорушенням; проаналізовано основні ознаки кримінального правопорушення; визначено та систематизовано види кримінальних правопорушень на об'єктах критичної інфраструктури; розглянуто наслідки таких правопорушень для різних секторів критичної інфраструктури; проаналізовано заходи, що вживаються для їх запобігання.



Результати дослідження. За результатами теоретичного та практичного аналізу встановлено, що протидія кримінальним правопорушенням на об'єктах критичної інфраструктури потребує комплексного підходу, який охоплює правові, організаційні, технічні та соціальні аспекти. Зокрема, це налагодження державно-приватного партнерства, посилення місцевої стійкості шляхом розширення повноважень регіональних органів влади, збільшення інвестицій в інфраструктуру кібербезпеки, удосконалення системи моніторингу та раннього виявлення загроз, розробка програм з підготовки кадрів для управління критичними ситуаціями, а також удосконалення законодавства в частині захисту критичної інфраструктури, що включає більш чітке визначення відповідальності за порушення у цій сфері, посилення санкцій за вчинення злочинів проти критичних об'єктів.

Практичне значення дослідження полягає в можливості застосування отриманих результатів для розробки ефективних стратегій захисту критичної інфраструктури України.

Ключові слова: критична інфраструктура, кримінальне правопорушення, злочин, Реєстр об'єктів критичної інфраструктури, Служба безпеки України, терористичний акт, громадська безпека, правосуддя.

Predmestnikov Oleg Gariyovych Doctor of Law, Professor, Honored Lawyer of Ukraine, Head of the Department of Law, Melitopol State Pedagogical University named after Bogdan Khmelnytsky, St. 59 Naukovoje Misto Ave., Zaporizhzhia, 69000, <http://orcid.org/0000-0001-8196-647X>

Okhman Olha Vasylivna Candidate of Legal Sciences, Associate Professor of the Department of Law and Law Enforcement, Khmelnytskyi Institute named after His Beatitude Volodymyr, Metropolitan of Kyiv and all Ukraine PJSC «Interregional Academy of Personnel Management», Prospekt Miru, 101 A, Khmelnytskyi, 29015, <https://orcid.org/0000-0002-9509-5326>

Parkheta Viktoriia Ivanivna PhD in Law, Associate Professor of the Department of Social and Legal Disciplines, Pavlo Tychyna Uman State Pedagogical University, Sadova St., 28, Uman, 20300, <https://orcid.org/0000-0003-2774-4790>

COUNTERING CRIMINAL OFFENSES AT CRITICAL INFRASTRUCTURE FACILITIES AS A SUBJECT OF SCIENTIFIC RESEARCH: THEORETICAL ASPECT

Abstract. The article is devoted to the theoretical analysis of criminal offenses and their counteraction at critical infrastructure facilities in Ukraine. The relevance



of the research is determined by the growing threat to the country's critical infrastructure, especially in wartime conditions, as well as the need to improve the legal and organizational framework for its protection.

The purpose of the article is to explore the theoretical aspects of countering criminal offenses at critical infrastructure facilities and to propose recommendations for enhancing the effectiveness of these measures.

The following general scientific research methods were used: analysis, synthesis, systematization, and comparison. To achieve the research objectives, several tasks were completed: the essence of the concepts of "criminal offense" and "counteraction to criminal offenses" was defined, as well as the goals and objectives of countering criminal offenses; the main characteristics of a criminal offense were analyzed; the types of criminal offenses at critical infrastructure facilities were identified and systematized; the consequences of such offenses for different sectors of critical infrastructure were examined; and the measures taken to prevent them were analyzed.

The theoretical and practical analysis revealed that countering criminal offenses at critical infrastructure facilities requires a comprehensive approach that encompasses legal, organizational, technical, and social aspects. In particular, this includes establishing public-private partnerships, strengthening local resilience by expanding the powers of regional authorities, increasing investment in cybersecurity infrastructure, improving monitoring and early threat detection systems, developing training programs for managing critical situations, and refining legislation related to critical infrastructure protection, including clearer definitions of liability for violations in this area and tougher sanctions for crimes against critical facilities.

The practical significance of the study lies in the possibility of applying the obtained results to develop effective strategies for protecting Ukraine's critical infrastructure.

Keywords: critical infrastructure, criminal offense, crime, Register of Critical Infrastructure Facilities, Security Service of Ukraine, terrorist act, public safety, justice.

Постановка проблеми. Об'єкти критичної інфраструктури є життєво важливими компонентами соціальної та економічної структури країни, що охоплюють стратегічно важливі підприємства, організації та установи. Ці об'єкти необхідні для підтримки безперервної роботи суспільства, тому їх будь-яке незаплановане відключення, перебої в роботі або повне руйнування може призвести до серйозних наслідків. Такі події можуть загрожувати національній безпеці, послаблювати обороноздатність, завдавати шкоди навколишньому середовищу, наносити матеріальні і фінансові збитки та навіть призводити до людських жертв.



Останніми роками, особливо в умовах війни, що триває, кримінальні правопорушення, спрямовані на об'єкти критичної інфраструктури, стають дедалі частішими та більш витонченими. Вони становлять значний ризик не лише для безпосереднього функціонування постраждалих об'єктів, але й для стабільності та безпеки країни в цілому. З огляду на це, питання забезпечення ефективного захисту об'єктів критичної інфраструктури набуває першочергового значення.

Теоретичне осмислення проблеми дозволить розробити комплексні підходи до протидії таким правопорушенням, що включатимуть не лише заходи безпосередньої охорони, але й удосконалення законодавчої бази, створення системи попередження та мінімізації наслідків можливих атак. Зважаючи на складність і масштабність загроз, що постають перед критичною інфраструктурою, дане дослідження спрямоване на формування науково обґрунтованих рекомендацій для забезпечення ефективного захисту національних інтересів і гарантування стабільності суспільства.

Аналіз останніх досліджень і публікацій. Теоретичні, нормативно-правові, організаційно-управлінські, технічні і практичні аспекти захисту критичної інфраструктури розглядаються у працях таких дослідників, як Тацій В. Я., Пшонка В. П., Борисов В. І., Тютюгін В. І. [2], Александров Ю. В., Антипов В. І., Володько М. В. [3], Конопельський В. Я., Меркулова В. О. [4], Бурдін В. М. [5], Коржанський М. Й. [6], Таран О. В., Сандул О. Г. [7], Афанасенко С. І., Стойков І. М. [11], Мармура О. З., Пасека О. Ф., Примаченко В. Ф., Сабанюк Т. Р. [12], Мозоль С. А. [13], Авраменко О. В., Бурда С. Я., Сас М. В. [14], Тимошенко Н. О. [15], Басараб О. Т. [16], Палюх Л. [17], Федієнко О. [18], Богдан Б. В. [23]. Однак недостатньо дослідженим на сьогоднішній день залишається питання протидії кримінальним правопорушенням на об'єктах критичної інфраструктури та, зокрема, теоретичні основи цього процесу. Так, сутність поняття «протидія кримінальним правопорушенням», мета та завдання протидії кримінальним правопорушенням є предметом дослідження в роботах Бандурки О. М. та Давиденка Л. М. [8], а також Бандурки О. М. та Литвинова О. М. [9]. Втім існує потреба в глибшому аналізі специфіки кримінальних правопорушень, що вчиняються на критичних об'єктах, і в розробці рекомендацій для їх попередження та реагування. Теоретичний аспект дослідження, що охоплює концептуальні підходи до визначення та класифікації таких правопорушень, їх вплив на безпеку і функціонування критичної інфраструктури, а також вивчення взаємодії різних правових і організаційних механізмів, залишається недостатньо дослідженим. Це підкреслює необхідність подальших наукових розробок, спрямованих на формулювання ефективних теоретичних і практичних рекомендацій для захисту критичної інфраструктури від кримінальних загроз.

Мета статті – дослідити теоретичні аспекти протидії кримінальним правопорушенням на об'єктах критичної інфраструктури та запропонувати рекомендації для підвищення ефективності цих заходів.



Виклад основного матеріалу. Враховуючи тему нашого дослідження, вважаємо за необхідне розглянути сутність та особливості кримінальних правопорушень у контексті захисту об'єктів критичної інфраструктури. Однак перш за все, необхідно надати теоретичне визначення цього поняття.

Згідно з Кримінальним кодексом України кримінальні правопорушення визначаються як суспільно небезпечні діяння (дії або бездіяльність), вчинені суб'єктом кримінального правопорушення – фізичною особою, що підлягає кримінальній відповідальності та досягла віку, з якого настає така відповідальність [1].

З визначення даного поняття виокремимо ключові ознаки кримінального правопорушення: наявність діяння, притаманна йому суспільна небезпека, елемент вини, передбаченість чинним Кримінальним кодексом України, наявність конкретного суб'єкта та караність.

Кримінальним кодексом України діяння (дія чи бездіяльність) визнається кримінальним правопорушенням у тому випадку, якщо воно відображає свідому та вольову поведінку особи, яка її вчиняє [2; 3]. Варто зазначити, що Конопельський В. Я. та Меркулова В. О. під діянням розуміють добровільну, свідому поведінку — активну (дію) чи пасивну (бездіяльність), яка спричиняє або створює загрозу заподіяння шкоди охоронюваним кримінальним законом суспільним відносинам [4]. Ми згодні з таким тлумаченням.

Суспільна небезпека, як здатність заподіяти серйозну та істотну шкоду встановленому правопорядку або об'єктам, що перебувають під кримінально-правовою охороною, є однією з найважливіших ознак кримінального правопорушення. Поняття суспільної небезпеки є основним критерієм відмежування кримінальних правопорушень від інших видів правопорушень. Суспільна небезпека є основною матеріальною ознакою будь-якого кримінального правопорушення, що розкриває його соціальну сутність. На думку Бурдіна В. М., вона виражається у яскраво вираженій антисоціальній спрямованості правопорушення, яке не тільки суперечить правовим нормам, а й протистоїть загальноприйнятим стандартам поведінки, внаслідок чого заподіюється або створюється загроза заподіяння істотної шкоди законним інтересам особи, суспільства, держави [5].

Вина є ще однією істотною ознакою кримінального правопорушення. Це обов'язкова ознака будь-якого злочину, яка відображає внутрішній психологічний стан винного — його психічне ставлення до вчиненого діяння та його наслідків, що виражається як умислом, так і необережністю. Як зазначає Коржанський М. Й., зазначена характеристика підкреслює важливий конституційний принцип суб'єктивної відповідальності, коли відповідальність можлива лише за наявності вини, як це закріплено Конституцією України та Кримінальним кодексом [6].



Протиправність, як юридичний прояв суспільної небезпечності кримінального правопорушення, встановлена Кримінальним кодексом України. В ньому зазначено, що діяння має бути передбачене цим законодавчим актом, тобто його вчинення прямо заборонено кримінальним законом, який є єдиним джерелом кримінальної відповідальності [1].

Крім того, кримінальне правопорушення характеризується його караністю. Кримінальним кодексом визначено суспільно небезпечні діяння, які є кримінальними правопорушеннями та покарання, що застосовуються до осіб, що їх вчинили [1].

Кримінальне правопорушення повинно мати суб'єкт, оскільки наявність кримінального правопорушення не може бути визнана без його участі. Відповідно до чинного Кримінального кодексу України суб'єктом кримінального правопорушення є фізична підсудна особа, яка вчинила кримінальне правопорушення та досягла віку, з якого настає кримінальна відповідальність відповідно до цього законодавчого акту [1; 4].

Отже, кримінальні правопорушення визначаються законодавцем та вітчизняними науковцями як суспільно небезпечні діяння, передбачені чинним Кримінальним кодексом України, що мають певний суб'єкт, характеризуються виною та караністю, а також включають як дії, так і бездіяльність, які порушують правопорядок і завдають шкоди охоронюваним інтересам.

В умовах війни і політичної нестабільності такі діяння набувають нових масштабів. Зловмисники використовують сучасні технології і методи для проникнення в критичні системи, що значно ускладнює їх виявлення і запобігання. Кримінальні правопорушення, орієнтовані на об'єкти критичної інфраструктури, масштабний вплив, порушуючи функціонування економічних і соціальних систем, створюючи загрозу для життя і здоров'я людей, а також завдаючи значних матеріальних збитків [7]. У цьому контексті дослідження кримінальних правопорушень на об'єктах критичної інфраструктури та протидія таким правопорушенням набуває особливого значення. Визначимо сутність протидії кримінальним правопорушенням та об'єкти інфраструктури, щодо яких вони здійснюються.

Бандурка О. М. та Давиденко Л. М. зазначають, що в кримінологічній теорії та правозастосовній практиці поняття «протидія кримінальним правопорушенням» часто ототожнюється з терміном «боротьба зі злочинністю» [8]. Нерідко ці терміни вживаються як синоніми, що відображає не тільки їх принципову схожість, а й збіг за змістом. У багатьох наукових працях, правових документах та методичних рекомендаціях вони розглядаються як взаємозамінні. Однак науковці висловлюють думку, що термін «протидія кримінальним правопорушенням» охоплює також і запобігання таким правопорушенням [8].



На думку Бандурки О. М. та Литвинова О. М., під протидією кримінальним правопорушенням слід розуміти складну, багаторівневу систему соціального управління, яка передбачає скоординовану діяльність різних суб'єктів, таких як державні та недержавні органи, установи, громадські організації, окремі громадяни [9]. Ці суб'єкти взаємодіють через мережу різноманітних заходів, спрямованих на пошук ефективних методів, інструментів і стратегій впливу на злочинність. Метою протидії кримінальним правопорушенням є зниження інтенсивності дії факторів, що криміногенно впливають на злочинність, нейтралізація причин і умов, що їй сприяють, обмеження злочинної активності до рівня, який є соціально прийнятним [9].

Завданнями протидії кримінальним правопорушенням є:

- виявлення першопричин злочинної поведінки та умов, що їй сприяють;
- здійснення заходів, що усувають або нейтралізують ці причини та умови;
- виявлення осіб, протиправна поведінка яких має тенденцію до переростання у злочинні діяння;
 - застосування до цих осіб заходів виправного впливу з метою запобігання вчиненню кримінальних правопорушень у майбутньому за допомогою цілеспрямованих превентивних стратегій;
 - зменшення ризику для громадян стати жертвами злочинів;
 - обмеження негативних наслідків і процесів, пов'язаних зі злочинністю;
 - мобілізація всіх позитивних сил суспільства на формування середовища нульової толерантності до злочинної поведінки;
 - усунення та виправлення недоліків у діяльності суб'єктів запобігання злочинності;
 - підвищення загальної ефективності зусиль щодо запобігання кримінальним правопорушенням [9].

Постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 9.10.2020 р. № 1109 затверджено «Порядок віднесення об'єктів до критичної інфраструктури», який містить перелік секторів критичної інфраструктури. Відповідно до нього, до об'єктів критичної інфраструктури відносяться підприємства, установи, організації незалежно від форми власності, які проводять діяльність та надають послуги в таких секторах як оборона, паливна енергетика, цифрові технології, фінанси, харчова промисловість, агропромисловий комплекс, охорона здоров'я, громадська безпека, транспорт, правосуддя, державна влада та місцеве самоврядування, а також в інших життєво важливих сферах [10].

Кримінальні правопорушення вчиняються у всіх без виключення секторах, визначених у Переліку. Проте, вони відрізняються за способом вчинення, наслідками та відповідальністю (Таблиця 1).



Таблиця 1.

**Види кримінальних правопорушень та способи їх вчинення на
об'єктах критичної інфраструктури [1]**

Види кримінальних правопорушень	Способи вчинення
Проти основ національної безпеки	Колабораційна діяльність; диверсія; шпигунство
Проти власності	Крадіжка; грабіж; розбій; викрадення води, електричної або теплової енергії шляхом її самовільного використання; вимагання; шахрайство; привласнення, розтрата майна та заволодіння таким майном шляхом зловживання службовим становищем; знищення або пошкодження майна, здійснене умисно, пошкодження електроенергетичних об'єктів
Проти громадської безпеки	Створення, керівництво злочинною спільнотою чи організацією, а також участь у ній; сприяння учасникам злочинних організацій; бандитизм; теракт; фінансування тероризму; утворення воєнізованих або збройних формувань, не передбачених законодавством; напад на об'єкти, на яких знаходяться предмети, небезпечні для оточення; знищення або пошкодження об'єктів житлово-комунального-господарства умисного характеру
Проти безпеки руху та експлуатації транспорту	Пошкодження шляхів сполучення і транспортних засобів; угон або захоплення залізничного рухомого складу, повітряного, морського чи річкового судна; блокування транспортних комунікацій; захоплення транспортних підприємств; пошкодження об'єктів магістральних або промислових нафто-, газо-, конденсато- та нафтопродуктопроводів
Проти авторитету органів державної влади, органів місцевого самоврядування	Захоплення державних або громадських будівель чи споруд; умисне пошкодження або руйнування телекомунікаційної мережі
У сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку	Незаконне втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних, електронних комунікаційних мереж; створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, їх розповсюдження або реалізація; незаконний збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; незаконні дії з інформацією, яка оброблюється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї
Проти правосуддя	Незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя; дії, які дезорганізують роботу установ виконання покарань та інші

Примітка: систематизовано авторами



Наслідки вчинення зазначених правопорушень залежать від сектора критичної інфраструктури, в якому вони вчиняються. Як зазначають в своїй роботі Афанасенко С. І. та Стойков І. М., правопорушення проти основ національної безпеки, такі як колабораційна діяльність, диверсії та шпигунство, завдають істотну шкоду безпеці держави та суспільства [11]. Вони можуть призвести до серйозного підриву обороноздатності країни, втрати стратегічної інформації та послаблення позицій на міжнародній арені. Це спричиняє втрату довіри до органів влади та зростання ризиків для національної безпеки.

Мармура О. З., Пасека О. Ф., Примаченко В. Ф., Сабанюк Т. Р. наголошують на тому, що злочини проти власності, включаючи крадіжки, грабїж та пошкодження майна, здатні спричинити значні матеріальні збитки, порушення постачання важливих ресурсів, таких як електроенергія чи вода, та збої у функціонуванні об'єктів критичної інфраструктури. В свою чергу, це може призвести до економічних втрат, затримок у роботі підприємств і загрози для життєдіяльності населення [12].

Кримінальні правопорушення проти громадської безпеки, такі як теракти та фінансування тероризму, можуть спричинити масові жертви, паніку серед населення, руйнування об'єктів житлово-комунального господарства, а також дестабілізацію суспільного порядку, порушення комунікацій та зниження довіри до органів влади [13].

Злочини проти безпеки руху та експлуатації транспорту, такі як угони транспортних засобів та пошкодження шляхів сполучення, здатні порушити логістичні ланцюги, спричинити аварії та створити серйозні загрози для життя і здоров'я людей [14].

Правопорушення проти авторитету органів державної влади та місцевого самоврядування, наприклад, захоплення державних будівель та руйнування телекомунікаційної мережі, можуть призвести до дезорганізації роботи органів влади, зниження довіри населення до державних інституцій та сприяти загостренню соціальної напруженості [15].

У сфері використання електронно-обчислювальних машин та комп'ютерних мереж незаконне втручання в роботу інформаційних систем і розповсюдження шкідливих програм можуть порушити функціонування критично важливих сервісів, таких як зв'язок та банківські операції, що може призвести до значних економічних збитків і створити загрозу національній безпеці [16].

Кримінальні правопорушення проти правосуддя, зокрема незаконне втручання в роботу автоматизованих систем, можуть дезорганізувати судову систему, спричиняючи затримки у здійсненні правосуддя, зниження ефективності судових процесів та підрив довіри до правової системи [17].



Відповідальність за вчинення зазначених кримінальних правопорушень передбачена Кримінальним кодексом України і варіюється від штрафу до позбавлення волі, залежно від тяжкості злочину та наслідків для суспільства.

Перелік кримінальних правопорушень та способів їх вчинення на об'єктах критичної інфраструктури, наведений в Таблиці 1, не є вичерпним. Однак, проаналізувавши його, можна зробити висновок про різноманітність і багатовимірність таких правопорушень. Це підкреслює необхідність всебічного підходу до протидії злочинам на об'єктах критичної інфраструктури.

Протидія кримінальним правопорушенням на об'єктах критичної інфраструктури є одним із першочергових завдань, які постають перед Україною під час війни. Україна докладає значних зусиль для ефективного вирішення цієї проблеми. Хоча підтримка західних партнерів є вирішальною у цих починаннях, значна частина відповідальності лежить на українській владі. У цій сфері вже досягнуто значного прогресу.

Як слушно зауважує О. В. Таран та О. Г. Сандул, наразі немає єдиного підходу щодо протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. Насамперед складнощі виникають у відсутності у вітчизняному законодавстві переліку об'єктів критичної інфраструктури. Разом із тим доопрацювання потребує й ККУ України. На думку авторів, удосконалення полягає в запровадженні окремих норм, які б чітко встановлювали особливості протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. І хоча, на думку авторів, у ККУ не доцільно наводити повний перелік об'єктів критичної інфраструктури через їх значний обсяг та потребу у частих змінах, які, як наслідок, потребуватимуть коригування кодексу, все ж таки необхідно поміркувати над тим, щоб чинне законодавство вмещувало відповідні норми у різних розділах ККУ. Наразі залишається необхідність у доповненні існуючих норм у запровадженні відповідних норм у розділі I Особливої частини ККУ «Злочини проти основ національної безпеки України» [7].

Розглядаючи питання протидії кримінальним правопорушенням на об'єктах критичної інфраструктури, неможна обійти увагою і суб'єктів, які займаються цим. Вітчизняний дослідник В. В. Крикун наголошує на тому, що Служба безпеки України в межах виконання основних завдань здійснює захист об'єктів критичної інфраструктури шляхом запобігання та протидії найрізноманітнішим протиправним посяганням на об'єкти критичної інфраструктури. Тобто в якості окремого напрямку діяльності Служби безпеки України як суб'єкта захисту об'єктів критичної інфраструктури є забезпечення кібербезпеки об'єктів критичної інфраструктури. Автор підкреслює й те, що одним з провідних суб'єктів захисту об'єктів критичної інфраструктури є Служба безпеки України, яка, реалізуючи свій правовий статус, виконує в цьому напрямку значну кількість завдань [18].



Оскільки питання протидії кримінальним правопорушенням на об'єктах критичної інфраструктури має комплексний характер сформований із методів і принципів діяльності окремих суб'єктів, вітчизняний дослідник Б. В. Богдан наголошує на тому, що варто зосереджуватися саме на протидії – як завданні правоохоронних органів, що здійснюють захист об'єктів критичної інфраструктури. Автор зазначає, що наразі державою здійснено низку заходів, які спрямовані на протидію кримінальним правопорушенням однак для повної гармонізації цього питання необхідно привести вітчизняні норми у відповідність до норм законодавства Європейського Союзу окремі норми-дефініції у сфері захисту об'єктів критичної інфраструктури, визначивши сектори та категоризацію об'єктів на законодавчому рівні [19].

Група вітчизняних дослідників Я. Р. Машталяр, В. А. Козачок, З. М. Бржевська, О. М. Богданов (2023) відзначають, що протидія кіберзагрозам на об'єктах критичної інфраструктури потребує не лише технічних інновацій, але й стратегічного перегляду підходів до кіберзахисту. Кібербезпека вимагає постійного еволюційного підходу для ефективного протидії як сучасним, так і майбутнім кіберзагрозам, що є особливо актуальним для об'єктів критичної інфраструктури. Складність та обсяг кіберзагроз постійно зростають, що вимагає не лише технічних інновацій, таких як штучний інтелект і блокчейн, але й стратегічного перегляду підходів до захисту критичних систем. Успіх у кіберзахисті можливий лише через комплексний підхід, що охоплює технічні, організаційні та людські аспекти, з активною співпрацею між державними органами, приватним сектором і громадянським суспільством. Освіта та підвищення обізнаності у сфері кіберзахисту є вирішальними для забезпечення безпеки об'єктів критичної інфраструктури, адже усвідомлення та навички всіх працівників підвищують загальний рівень кібербезпеки [20].

Напередодні війни було зроблено кілька важливих кроків. Прийняття закону «Про критичну інфраструктуру» заклало правову основу для захисту ключових об'єктів [21]. Крім того, уряд затвердив Національний план захисту та стабільності об'єктів критичної інфраструктури, ініціатором якого є Держспецзв'язку (уповноважений орган з координації захисту критичної інфраструктури). Ця служба відповідає за координацію діяльності суб'єктів системи захисту країни та забезпечення ефективної реалізації державної політики щодо критичної інфраструктури [22; 23].

Створено комплексний Реєстр об'єктів критичної інфраструктури. Суб'єктам, включеним до цього реєстру, надається пріоритетний доступ до таких ресурсів, як електроенергія, експертні рекомендації щодо заходів безпеки та спрощені процеси закупівель для їх потреб у захисті [24].



Необхідно відзначити зусилля Служби безпеки України, яка приділяє особливу увагу контррозвідувальному захисту об'єктів енергетики, транспортної інфраструктури та інших стратегічно важливих секторів. Це є критично важливим для запобігання спробам ворожого агентурного проникнення на ці об'єкти та його намірам здійснити диверсії [25].

Враховуючи ці події, очевидно, що Україна заклала надійну основу для захисту своєї критичної інфраструктури та протидії кримінальним порушенням на її об'єктах. Однак потрібні постійні зусилля для зміцнення цієї основи. Рухаючись вперед, вкрай важливо визначити пріоритети в кількох ключових сферах: посилення співпраці між державою та приватним сектором, посилення місцевої стійкості шляхом розширення повноважень регіональних органів влади, збільшення інвестицій в інфраструктуру кібербезпеки, удосконалення системи моніторингу та раннього виявлення загроз, розробка програм з підготовки кадрів для управління критичними ситуаціями, а також удосконалення законодавства в частині захисту критичної інфраструктури, що включає більш чітке визначення відповідальності за порушення у цій сфері, посилення санкцій за вчинення злочинів проти критичних об'єктів [19]. Все це дозволить забезпечити не лише надійний захист, але й стійкість критичної інфраструктури перед будь-якими загрозами, забезпечуючи стабільність і безпеку країни в умовах безперервних викликів.

Висновки. Україна створила міцну основу для захисту своєї критичної інфраструктури від злочинних правопорушень. Незважаючи на ці зусилля, залишається нагальна потреба постійно покращувати та вдосконалювати цю основу для ефективної протидії загрозам, що розвиваються. Серед ключових сфер, які потребують удосконалення, — сприяння міцному державно-приватному партнерству, посилення місцевої стійкості за рахунок розширення повноважень регіональних органів влади та збільшення інвестицій в інфраструктуру кібербезпеки. Крім того, важливими кроками є удосконалення систем моніторингу для раннього виявлення загроз, розробка комплексних навчальних програм для управління критичними ситуаціями та просування законодавчих ініціатив для кращого визначення відповідальності та посилення покарання за злочини проти критичної інфраструктури.

Практичне значення цього дослідження полягає в його потенціалі для розробки більш ефективних стратегій захисту критичної інфраструктури України. Впроваджуючи рекомендації, отримані в результаті цього дослідження, політики та зацікавлені сторони зможуть краще усунути поточні вразливості та підвищити загальну стійкість критичної інфраструктури проти злочинних загроз.



Література:

1. Кримінальний кодекс України: Закон України № 2341-ІІ від 5.04.2001 р. ВРУ. 2024. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
2. Тацій В. Я., Пшонка В. П., Борисов В. І., Тютюгін В. І. Кримінальний кодекс України. Науково-практичний коментар: у 2 т. Загальна частина. Т. 1. Харків: Право, 2013. 376 с.
3. Александров Ю. В., Антипов В. І., Володько М. В. Кримінальне право України. Загальна частина: Підручник. (Вид. 3-тє, переробл. та допов.) Київ: Юридична думка, 2004. 352 с.
4. Конопельський В. Я., Меркулова В. О. Кримінальне право України. Загальна частина: підручник. Одеса, ОДУВС, 2021. 452 с.
5. Бурдін В. М. Закінчений злочин: спірні проблеми розуміння. Науковий Вісник Львівського державного університету внутрішніх справ. 2013. № 3. С. 292-303.
6. Коржанський М. Й. Кримінальне право і законодавство України. Частина Загальна. Курс лекцій. Київ: Атіка, 2001. 432 с.
7. Таран О. В., Сандул О. Г. Проблеми кримінальної відповідальності за посягання на об'єкти критичної інфраструктури в ядерній енергетиці. Ядерна та радіаційна безпека. 2019. 3 (83). С. 58-67. URL: <https://nuclear-journal.com/index.php/journal/article/view/177/172>
8. Бандурка О. М., Давиденко Л. М. Злочинність в Україні: причини та протидія: Монограф. Харків, 2003
9. Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів: Монограф. Харків, 2011
10. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України № 1109 від 9.10.2020 р. ВРУ. 2024. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>
11. Афанасенко С. І., Стойков І. М. Злочини проти основ національної безпеки України, що посягають на відносини в політичній сфері. Правова система: теорія і практика. 2015. С. 54-56. URL: <http://www.sulj.oduvs.od.ua/archive/2015/3/18.pdf>
12. Мармура О. З., Пасека О. Ф., Примаченко В. Ф., Сабанюк Т. Р. Кримінально-правова характеристика злочинів проти власності: навч. посібник у схемах. Львів, 2019. 44 с.
13. Мозоль С. А. Стан і тенденції злочинів проти громадської безпеки під час воєнного стану в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. Харків, 2019. С. 143-146. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/66.pdf
14. Авраменко О. В., Бурда С. Я., Сас М. В. Кримінально-правова характеристика злочинів проти безпеки руху та експлуатації транспорту: навч. посібник у схемах. Львів: Львівський державний університет внутрішніх справ, 2019. 36 с.
15. Тимошенко Н. О. Кримінально-правова характеристика підроблення документів, печаток, штампів та бланків, їх збуту та використання: дис. ... канд. юрид. наук: 12.00.08. Донецьк, 2009. 234 с.
16. Басараб О. Т. Кримінально-правовий аналіз несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-телекомунікаційних систем та електронних комунікаційних мереж. Юридичний науковий електронний журнал. 2024. № 2. С. 319-322. URL: http://www.lsej.org.ua/2_2024/79.pdf
17. Палюх Л. Класифікація злочинів проти правосуддя. Кримінальне право. 2018. № 2. С. 176-181. URL: <http://pgp-journal.kiev.ua/archive/2018/2/33.pdf>



18. Крикун В.В. Правоохоронні органи як суб'єкти захисту об'єктів критичної інфраструктури в Україні. Юридична наука, №4 (94). 2019. С. 143-152. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/550fd44f-fd22-4966-8c07-3dfab33272a3/content>
19. Богдан Б. В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2022. № (6). <https://doi.org/10.54929/2786-5746-2022-6-01-09> 23
20. Машталяр Я.Р., Козачок В. А., Бржезьська З. М., Богданов О. М. Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка. №2 (22), 2023. С. 156-165 URL: https://www.researchgate.net/publication/377421360_RESEARCH_OF_DEVELOPMENT_AND_INNOVATION_OF_CYBER_PROTECTION_AT_CRITICAL_INFRASTRUCTURE_FACILITIES
21. Федієнко О. Державно-приватне партнерство: єдиний механізм для захисту критичної інфраструктури. Мінд. 2023. URL: <https://mind.ua/openmind/20261400-derzhavno-privatne-partnerstvo-edinij-mehanizm-dlya-zahistu-kritichnoyi-infrastrukturi18>
22. Уряд затвердив Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури. КМУ. 2023. URL: <https://www.kmu.gov.ua/news/uriad-zatverdvy-natsionalnyi-plan-zakhystu-ta-zabezpechennia-bezpeky-ta-stiikosti-krytychnoi-infrastruktury19>
23. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України № 825-р. від 19.09.2023 р. ВРУ. 2023. URL: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text20>
24. Об'єкти критичної інфраструктури України: все, що варто знати. Київpost. 2024. URL: <https://www.kyivpost.com/uk/post/28283> 21
25. Захист об'єктів критичної інфраструктури. СБУ. 2024. URL: <https://ssu.gov.ua/zakhyst-obiektiv-krytychnoi-infrastruktury> 22

References:

1. Kryminal'nyy kodeks Ukrayiny: Zakon Ukrayiny № 2341-II vid 5.04.2001 r. (2024). [Criminal Code of Ukraine: Law of Ukraine No. 2341-II dated April 5, 2001 of the VRU]. VRU. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> [in Ukrainian].
2. Tatsiy, V. YA., Pshonka, V. P., Borysov, V. I., Tyutyuhin, V. I. (2013). Kryminal'nyy kodeks Ukrayiny. Naukovo-praktychnyy komentar: u 2t. Zahal'na chastyna [Criminal Code of Ukraine. Scientific and practical commentary: in 2 volumes. General part]. T. 1. Kharkiv: Pravo, 376 [in Ukrainian].
3. Aleksandrov, YU. V., Antypov, V. I., Volod'ko, M. V. (2004). Kryminal'ne pravo Ukrayiny. Zahal'na chastyna: Pidruchnyk. (Vyd. 3-tye, pererobl. ta dopov.) [Criminal Law of Ukraine. General part: Textbook. (3rd ed., revised and supplemented)]. Kyiv: Yurydychna dumka, 352 [in Ukrainian].
4. Konopel's'kyu, V. YA., Merkulova, V. O. (2021). Kryminal'ne pravo Ukrayiny. Zahal'na chastyna: pidruchnyk [Criminal law of Ukraine. General part: textbook]. Odesa, ODUVS, 452 [in Ukrainian].
5. Burdin, V. M. (2013). Zakinchenyy zlochyn: spil'ni problemy rozuminnya [The finished crime: common problems of understanding]. Naukovyy Visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav, 3, 292-303 [in Ukrainian].
6. Korzhans'kyu, M. Y. (2001). Kryminal'ne pravo i zakonodavstvo Ukrayiny. Chastyna Zahal'na. Kurs leksiy [Criminal law and legislation of Ukraine. General part. Course of lectures]. Kyiv: Atika, 432 [in Ukrainian].



7. Taran, O. V., Sandul, O. H. (2019). Problemy kryminal'noyi vidpovidal'nosti za posyahannya na ob'ekty krytychnoyi infrastruktury v yaderniy enerhetytsi [Problems of criminal liability for encroachment on critical infrastructure objects in nuclear energy]. *Yaderna ta radiatsiyana bezpeka*, 3 (83), 58-67. Retrieved from: <https://nuclear-journal.com/index.php/journal/article/view/177/172> [in Ukrainian].
8. Bandurka, O. M., Davydenko, L. M. (2003). *Zlochynnist' v Ukrayini: prychny ta protydiya: Monohraf* [Crime in Ukraine: causes and countermeasures: Monograph]. Kharkiv [in Ukrainian].
9. Bandurka, O. M., Lytvynov, O. M. (2011). *Protydiya zlochynnosti ta profilaktyka zlochyniv: Monohraf* [Crime prevention and crime prevention: Monograph]. Kharkiv [in Ukrainian].
10. Deyaki pytannya obyektiv krytychnoyi infrastruktury: Postanova Kabinetu Ministriv Ukrayiny № 1109 vid 9.10.2020 r. (2024). [Some issues of critical infrastructure objects: Resolution of the Cabinet of Ministers of Ukraine No. 1109 of October 9, 2020 of the VRU]. VRU. Retrieved from: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text> [in Ukrainian].
11. Afanasenko, S. I., Stoykov, I. M. (2015). *Zlochyny proty osnov natsional'noyi bezpeky Ukrayiny, shcho posyahayut' na vidnosyny v politychniy sferi* [Crimes against the foundations of Ukraine's national security that encroach on relations in the political sphere]. *Pravova systema: teoriya i praktyka*, 54-56. Retrieved from: <http://www.sulj.oduvs.od.ua/archive/2015/3/18.pdf> [in Ukrainian].
12. Marmura, O. Z., Pasyeka, O. F., Prymachenko, V. F., Sabanyuk, T. R. (2019). *Kryminal'no-pravova kharakterystyka zlochyniv proty vlasnosti: navch. posibnyk u skhemakh* [Criminal law characteristics of crimes against property: education. manual in diagrams]. L'viv, 44 [in Ukrainian].
13. Mozol', S. A. (2019). *Stan i tendentsiyi zlochyniv proty hromads'koyi bezpeky pid chas voyennoho stanu v Ukrayini* [State and trends of crimes against public safety during martial law in Ukraine]. *Kryminal'no-pravovi ta kryminolohichni zasoby protydyi zlochynam proty hromads'koyi bezpeky ta publichnoho porядku*. Kharkiv, 143-146. Retrieved from: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/66.pdf [in Ukrainian].
14. Avramenko, O. V., Burda, S. YA., Sas, M. V. (2019). *Kryminal'no-pravova kharakterystyka zlochyniv proty bezpeky rukhu ta ekspluatatsiyi transportu: navch. posibnyk u skhemakh* [Criminal and legal characteristics of crimes against traffic safety and operation of transport: training. manual in diagrams]. L'viv: L'vivs'kyy derzhavnyy universytet vnutrishnikh sprav, 36 [in Ukrainian].
15. Timoshenko, N. O. (2019). *Kryminal'no-pravova kharakterystyka pidroblennya dokumentiv, pechatok, shtampiv ta blankiv, yikh zbutu ta vykorystannya: dys. ... kand. yuryd. nauk: 12.00.08.* [Criminal and legal characteristics of forgery of documents, seals, stamps and forms, their sale and use: dissertation. ... candidate law Sciences: 12.00.08.]. Donetsk, 234 [in Ukrainian].
16. Basarab, O. T. (2024). *Kryminal'no-pravovyy analiz nesanktsionovanoho vtruchannya v robotu informatsiynykh (avtomatyzovanykh), elektronnykh komunikatsiynykh, informatsiyno-telekomunikatsiynykh system ta elektronnykh komunikatsiynykh merezh* [Criminal law analysis of unauthorized interference in the work of information (automated), electronic communication, information and telecommunication systems and electronic communication networks]. *Yurydychnyy naukovyy elektronnyy zhurnal*, 2, 319-322. Retrieved from: http://www.lsej.org.ua/2_2024/79.pdf [in Ukrainian].
17. Palyukh, L. (2018). *Klasyfikatsiya zlochyniv proty pravosuddya* [Classification of crimes against justice]. *Kryminal'ne pravo*, 2, 176-181. Retrieved from: <http://pgp-journal.kiev.ua/archive/2018/2/33.pdf> [in Ukrainian].



18. Krykun V.V. (2019) Pravoohoronni orhany yak sub"yekty zakhystu ob"yektiv krytychnoyi infrastruktury v Ukrayini [Law enforcement agencies as subjects of protection of critical infrastructure objects in Ukraine] Yurydychna nauka, №4 (94). Retrieved from: <https://dspace.univd.edu.ua/server/api/core/bitstreams/550fd44f-fd22-4966-8c07-3dfab33272a3/content> [in Ukrainian].

19. Bohdan, B. V. (2022). Aktual'ni pytannya normatyvno-pravovoho rehulyuvannya zakhystu krytychnoyi infrastruktury v umovakh voyennoho stanu v Ukrayini [Current issues of normative and legal regulation of critical infrastructure protection in the conditions of martial law in Ukraine]. Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya, 6. <https://doi.org/10.54929/2786-5746-2022-6-01-09> [in Ukrainian].

20. Mashtalyar YA.R., Kozachok V. A., Brzhevs'ka Z. M., Bohdanov O. M. (2023) Doslidzhennya rozvytku ta innovatsiyi kiberzakhystu na obyektakh krytychnoyi infrastruktury. [Research on the development and innovation of cyber protection at critical infrastructure facilities] Kiberbezpeka: osvita, nauka, tekhnika. №2 (22). Retrieved from: https://www.researchgate.net/publication/377421360_RESEARCH_OF_DEVELOPMENT_AND_INNOVATION_OF_CYBER_PROTECTION_AT_CRITICAL_INFRASTRUCTURE_FACILITIES [in Ukrainian].

21. Fediyenko, O. (2023). Derzhavno-pryvatne partnerstvo: yedynny mekhanizm dlya zakhystu krytychnoyi infrastruktury [Public-private partnership: a single mechanism for the protection of critical infrastructure]. Mind. Retrieved from: <https://mind.ua/openmind/20261400-derzhavno-pryvatne-partnerstvo-edynij-mekhanizm-dlya-zahystu-krytychnoyi-infrastruktury> [in Ukrainian].

22. Uryad zatverdyv Natsional'nyy plan zakhystu ta zabezpechennya bezpeky ta stiykosti krytychnoyi infrastruktury. (2023). [The Government approved the National Plan for the Protection and Ensuring the Safety and Stability of Critical Infrastructure]. KМУ. Retrieved from: <https://www.kmu.gov.ua/news/uriad-zatverdyv-natsionalnyi-plan-zakhystu-ta-zabezpechennia-bezpeky-ta-stiykosti-krytychnoi-infrastruktury> [in Ukrainian].

23. Pro zatverdzhennya Natsional'noho planu zakhystu ta zabezpechennya bezpeky ta stiykosti krytychnoyi infrastruktury: Rozporyadzhennya Kabinetu Ministriv Ukrayiny № 825-r. vid 19.09.2023 r. (2023). [On the approval of the National Plan for the Protection and Ensuring the Safety and Stability of Critical Infrastructure: Order of the Cabinet of Ministers of Ukraine No. 825-r. dated September 19, 2023]. VRU. Retrieved from: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text> [in Ukrainian].

24. Ob'yekty krytychnoyi infrastruktury Ukrayiny: vse, shcho varto znaty. (2024). [Objects of critical infrastructure of Ukraine: everything worth knowing]. Kievpost. Retrieved from: <https://www.kyivpost.com/uk/post/28283> [in Ukrainian].

25. Zakhyst ob"yektiv krytychnoyi infrastruktury. (2024). [Protection of critical infrastructure facilities]. SBU. Retrieved from: <https://ssu.gov.ua/zakhyst-obiektiv-krytychnoi-infrastruktury> [in Ukrainian].