УДК 343.13:343.326
DOI https://doi.org/10.24144/2788-6018.2025.02.145

ДОСВІД ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЄС ТА США: ТЕОРЕТИЧНИЙ, ПРАВОВИЙ ТА ОРГАНІЗАЦІЙНИЙ АСПЕКТИ

Герасименко О.М.,
кандидат юридичних наук, докторант,
Національна академія Служби безпеки України
ORCID: 0009-0005-5078-3829

Герасименко О.М. Досвід досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури ЄС та США: теоретичний, правовий, організаційний аспекти.

Стаття присвячена комплексному аналізу досвіду досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в Європейському Союзі та Сполучених Штатах Америки. Досліджено теоретичні засади поняття «критична інфраструктура», розкрито особливості її правового регулювання в США та країнах ЄС. Встановлено, що американський підхід до визначення критичної інфраструктури є широким і охоплює різноманітні сектори, включаючи енергетику, транспорт, телекомунікації, банківську сферу, охорону здоров'я та інші стратегічно важливі об'єкти. Виявлено еволюцію термінології в європейському підході – від концепції «захисту критичної інфраструктури» до концепції «стійкості критично важливих об'єктів», що відображено в зміні основних нормативних документів ЄС.

Проаналізовано правові аспекти досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в США та ЄС, виявлено спільні риси та відмінності в організаційних підходах. Установлено, що в США система досудового розслідування характеризується децентралізованим підходом із чітким розмежуванням повноважень між федеральними та місцевими органами, тоді як у країнах ЄС спостерігається тенденція до централізації та уніфікації процедур. Досліджено особливості міжнародного співробітництва у сфері розслідування транснаціональних злочинів проти критичної інфраструктури, а також роль державно-приватного партнерства у забезпеченні ефективності розслідування.

Визначено ключові проблеми досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури, серед яких: технологічні виклики, правові обмеження, кваліфікація кадрів, атрибуції кібератак та недостатня співпраця між державним і приватним секторами. Окреслено перспективні напрями вдосконалення досудового розслідування таких правопорушень, зокрема: розвиток правової бази, посилення міжнародного співробітництва, впровадження новітніх технологій, розвиток державно-приватного партнерства та інвестиції у підготовку спеціалізованих кадрів.

Обґрунтовано пропозицію переходу від реактивної до проактивної моделі розслідування та впровадження технологій штучного інтелекту для аналізу великих обсягів даних і прогнозування потенційних загроз.

Ключові слова: критична інфраструктура, досудове розслідування, кримінальні правопорушення, кібератаки, Європейський Союз, США, правове регулювання, міжнародне співробітництво, державно-приватне партнерство, об'єкти критичної інфраструктури, атрибуція кібератак, транснаціональні злочини, проактивний підхід, штучний інтелект.

Herasymenko O.M. Experience of pre-trial investigation of criminal offenses at critical infrastructure facilities in the EU and the USA: theoretical, legal, and organizational aspects.

The article is devoted to a comprehensive analysis of the experience of pre-trial investigation of criminal offenses at critical infrastructure facilities in the European Union and the United States of America. The theoretical foundations of the concept of critical infrastructure are studied, and the peculiarities of its legal regulation in the USA and EU countries are revealed. It is established that the American approach to defining critical infrastructure is broad and covers various sectors, including energy, transport, telecommunications, banking, healthcare, and other strategically important facilities. The evolution of terminology in the European approach is revealed – from the concept of «critical infrastructure protection» to the concept of «resilience of critical facilities,» which is reflected in the change of the main EU regulatory documents.

The legal aspects of pre-trial investigation of criminal offenses at critical infrastructure facilities in the USA and EU are analyzed, revealing common features and differences in organizational approaches. It is established that in the USA, the pre-trial investigation system is characterized by a decentralized approach

with a clear delimitation of powers between federal and local authorities, while in EU countries there is a tendency towards centralization and unification of procedures. The peculiarities of international cooperation in the investigation of transnational crimes against critical infrastructure, as well as the role of public-private partnership in ensuring the effectiveness of investigations, are studied.

Key problems of pre-trial investigation of criminal offenses at critical infrastructure facilities are identified, including: technological challenges, legal limitations, personnel qualification, attribution of cyber attacks, and insufficient cooperation between public and private sectors. Promising directions for improving the pre-trial investigation of such offenses are outlined, in particular: development of the legal framework, strengthening international cooperation, implementation of new technologies, development of public-private partnerships, and investment in the training of specialized personnel.

The proposal for a transition from a reactive to a proactive model of investigation and the implementation of artificial intelligence technologies for analyzing large volumes of data and predicting potential threats is substantiated.

Key words: critical infrastructure, pre-trial investigation, criminal offenses, cyber attacks, European Union, USA, legal regulation, international cooperation, public-private partnership, critical infrastructure facilities, attribution of cyber attacks, transnational crimes, proactive approach, artificial intelligence.

Постановка проблеми. Дослідження досвіду досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в ЄС та США є актуальним питанням сучасної юридичної науки з огляду на зростання загроз таким об'єктам в Україні та необхідність удосконалення вітчизняної методології та законодавчого забезпечення організації діяльності у цій сфері. Загрозлива динаміка небезпечного для національної безпеки України характеру заподіяння шкоди об'єктам критичної інфраструктури від скоєних кримінальних посягань, вимагає розробки та впровадження спеціальних, актуальних методик досудового розслідування, які враховували б специфіку таких об'єктів та особливості кримінальних правопорушень, що посягають на охоронювані Кримінальним кодексом України суспільні відносини на них або здійснюються проти них. Особливого значення набуває поглиблене вивчення міжнародного досвіду розслідування таких правопорушень, зокрема досвіду США та держав Європейського Союзу, як провідних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури та протидії кримінальним правопорушенням, що посягають на стабільність їх функціонування.

Враховуючи зазначене, для наукової сфери актуальним завданням є наукова розробка наявних проблем протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури України. Дослідження проблем означеного назвою статті напряму забезпечить умови їх розв'язання і створить теоретичне підґрунтя для практичної реалізації заходів підвищення рівня національної безпеки України.

Зважаючи на важливість визначеної теми для забезпечення національної безпеки України, з урахуванням актуальності обраної теми серед вчених, а також з огляду сучасних потреб практики, є потреба проведення дослідження.

Мета статті – полягає в аналізі досвіду досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в ЄС та США, з урахуванням теоретичних, правових та організаційних аспектів. Завданням є виявлення основних тенденцій, порівняння правових та організаційних моделей, а також визначення ефективних підходів та механізмів, що застосовуються в цих країнах для боротьби з кримінальними правопорушеннями, пов'язаними з критичною інфраструктурою, з метою підвищення ефективності національного досудового розслідування.

Стан опрацювання проблематики. Проведений науковий аналіз досліджень фахівців з кримінального права і процесу, криміналістики, міжнародного права, кібербезпеки та охорони критичної інфраструктури засвідчує, що в межах предметів своїх робіт окремими теоретичними та практичними питаннями досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури ЄС та США займалися такі вчені, як: О.В. Батюк – дослідив криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури, проаналізувавши методи та засоби розслідування таких правопорушень (2021 р.) [1]; Д.С. Бірюков, С.І. Кондратов – розглянули проблеми та перспективи впровадження системи захисту критичної інфраструктури в Україні, звернувши увагу на нормативно-правові та організаційні аспекти (2012 р.) [2]; В.І. Коломієць – дослідив зарубіжний досвід взаємодії між органами досудового розслідування та можливості його адаптації в Україні (2023 р.) [7]; І.І. Маринів – проаналізував боротьбу з тероризмом у контексті актів Європейського Союзу та Ради Європи, дослідивши співвідношення права ЄС із міжнародним правом (2019 р.) [8]; А.А. Саковський, І.М. Єфіменко, О.С. Хоруженко та інші – розробили методичні рекомендації щодо розслідування посягань на об'єкти критичної інфраструктури, висвітливши алгоритми дій правоохоронних органів (2023 р.) [10]; С.С. Теленик – проаналізував досвід правового регулювання системи

захисту критичної інфраструктури в США, окресливши особливості американської моделі у цій сфері (2018 р.) [11]; R. Barnsby – дослідив правові механізми посилення кібербезпеки через державно-приватне партнерство, розглянувши переваги та виклики такого підходу (2020 р.) [15]; S. Carrera, M. Stefan, V. Mitsilegas – розглянули проблематику транскордонного доступу до даних у кримінальних провадженнях та перспективи цифрового правосуддя в ЄС (2020 р.) [16]; M. Kaiafa-Gbandi – дослідила юрисдикційні конфлікти у кримінальних справах у межах наднаціональної правової системи ЄС та можливі шляхи їх врегулювання (2017 р.) [37]; J. Littlewood – проаналізував політику захисту критичної інфраструктури в США за часів адміністрації Президента США Б. Обами, зосередившись на основних реформах та викликах у цій сфері [39]; K.T. Mulyk – дослідила історичні та теоретичні аспекти імплементації норм щодо досудового розслідування у правові системи різних країн (2023 р.) [42].

Утім, попри наявні наукові здобутки за визначеною темою, на теоретичному рівні ці питання ще не систематизовані і розроблені не в повному обсязі. Дискусія щодо правових та організаційних аспектів досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури триває, що зумовлює необхідність подальшого дослідження цієї теми, з урахуванням сучасних викликів безпеки та потреб практики.

Виклад основного матеріалу. У другій половині XX століття сформувалися передумови для трансформації індустріального суспільства в сучасну модель, засновану на інформаційних технологіях. Цей процес суттєво змінив суспільні відносини, зокрема у сфері безпеки критичної інфраструктури, що стало новим викликом для правоохоронних органів. У багатьох країнах, зокрема в ЄС та США, запровадження високотехнологічних рішень в управління об'єктами критичної інфраструктури виявило їхню вразливість до загроз кримінального характеру. Це зумовило необхідність удосконалення теоретичних, правових та організаційних засад досудового розслідування кримінальних правопорушень, пов'язаних із посяганням на такі об'єкти. Враховуючи стратегічне значення останніх для економіки, оборони та національної безпеки, також виникла необхідність розробки ефективних механізмів міжнародної співпраці, гармонізації правових підходів та вдосконалення методів досудового розслідування.

Знані вчені, аналізуючи міжнародний досвід забезпечення безпеки об'єктів критичної інфраструктури, зазначають, що остання потребує належної протидії незаконним посяганням, оскільки стабільність функціонування зазначених об'єктів впливає на життєдіяльність суспільства.

Зокрема вітчизняні учений О.В. Батюк наголошує на можливих катастрофічних наслідках кримінальних правопорушень у цій сфері, зокрема порушенні життєво важливих систем, економічних збитках і загрозі національній безпеці. Для ефективного розслідування таких злочинів він пропонує комплексний підхід, що включає інформаційно-аналітичне, техніко-криміналістичне, тактико-організаційне та методичне забезпечення. Важливу роль, на думку ученого, і це є цілком прийнятним, відіграє взаємодія правоохоронних органів, спецслужб та операторів критичної інфраструктури. До основних принципів досудового розслідування відносить: 1) пріоритетність (ці правопорушення мають бути в центрі уваги правоохоронців); 2) спеціалізацію (участь підготовлених слідчих); 3) координацію (злагодженість усіх залучених суб'єктів) та 4) міжнародне співробітництво (оскільки багато злочинів мають транснаціональний характер) [1].

Вчені А.А. Саковський, І.М. Єфіменко та О.С. Хоруженко та ін., своєю чергою, виокремлюють три основні концептуальні підходи до організації досудового розслідування таких правопорушень: 1) секторальний – базується на специфіці певного сектору критичної інфраструктури (енергетика, транспорт, телекомунікації тощо); 2) ризик-орієнтований – ґрунтується на оцінці ризиків та загроз, що виникають у процесі функціонування об'єктів критичної інфраструктури; 3) інтегрований – поєднує елементи секторального та ризик-орієнтованого підходів і забезпечує комплексний підхід до розслідування [10].

У контексті дослідження проблеми проаналізуємо погляди іноземних дослідників. Так, Роберт Барнсбі (Robert Barnsby) зазначає, що ключовим елементом ефективного розслідування кримінальних правопорушень на об'єктах критичної інфраструктури є застосування проактивного підходу, який передбачає не лише реагування на вже вчинені правопорушення, але й виявлення та нейтралізацію потенційних загроз [15]. Дослідник наголошує, що досудове розслідування має базуватися на моделі постійного моніторингу та аналізу ризиків, тісній співпраці між правоохоронними органами та операторами критичної інфраструктури, а також використанні сучасних технологій для виявлення та фіксації слідів кримінальних правопорушень [15].

Зі свого боку М. Кайафи-Ґбанді (M. Kaiafa-Gbandi) наполягає на комплексному підході до організації досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури, який включає як ефективну міжнародну співпрацю й чітке врегулювання юрисдикційних питань, так і суворе дотримання стандартів захисту фундаментальних прав осіб на стадії досудового провадження. Розглядаючи юрисдикційні конфлікти у кримінальних справах у межах наднаціональної правової системи Європейського Союзу та можливі шляхи їх врегулювання, вчена відзначила, що однією з ключо-

вих проблем досудового розслідування кримінальних правопорушень, зокрема тих, що посягають на критичну інфраструктуру у країнах ЄС, є конфлікти юрисдикцій між правоохоронними органами різних держав-членів ЄС. На її думку, такі конфлікти виникають через відмінності в національних правових системах, що призводить до ускладнень у зборі доказів, обміні інформацією та координації слідчих дій. Вчена акцентує на необхідності створення чітких правових механізмів для узгодження юрисдикційних питань та уникнення конфліктів між державами-членами ЄС [37].

Дещо схожу позицію висловлюють і група європейських дослідників на чолі з С. Каррера, М. Стефан і В. Міцілегас (Carrera S., Stefan M., Mitsilegas V.), які пропонують принципово новий підхід до розуміння транскордонного характеру таких правопорушень. Вчені наголошують, що сучасна парадигма досудового розслідування повинна виходити за межі традиційних територіальних кордонів, адже кібернетичні загрози для критичної інфраструктури мають глобальний характер [16]. Підкреслено необхідність створення транскордонної моделі розслідування, яка базується на поєднанні національних юрисдикційних повноважень із наднаціональними механізмами координації.

Значну увагу вони приділяють механізмам електронного правосуддя та транскордонного збору доказів. Критична інфраструктура в цифрову епоху вимагає трансформації процесуальних інструментів збору та обміну електронними доказами, які часто розпорошені між різними юрисдикціями. Згадані науковці наполягають на багаторівневій системі досудового розслідування, що передбачає: 1) гармонізацію національних процесуальних норм у сфері електронних доказів; 2) створення єдиної європейської платформи для безпечного обміну цифровими доказами; 3) розробку спільних стандартів автентифікації та верифікації електронних доказів; 4) впровадження прискорених процедур транскордонного доступу до даних у випадках загроз критичній інфраструктурі [16].

Вчений Ж. Літтлвуд (J. Littlewood), досліджуючи захист критичної інфраструктури США за часів адміністрації Б. Обами, зазначав, що захист критичної інфраструктури вимагає довгострокового підходу та стійкої прихильності, яка має тривати роками та поколіннями. Дослідник звертає увагу на те, що захист критичної інфраструктури США базується на посиленні державного управління ризиками, розширенні партнерства між державними установами та приватним сектором, а також активному використанні інформаційних технологій для попередження загроз [39]. Таким чином американська система захисту критичної інфраструктури передбачає комплексний підхід, який включає виявлення вразливостей, оцінку ризиків і впровадження адаптивних механізмів реагування.

Отже, порівнюючи позиції вищезазначених науковців, можна зробити поточний висновок, що найбільш перспективним є саме інтегрований підхід, запропонований вітчизняними науковцями – А.А. Саковським, І.М. Єфіменко та О.С. Хоруженко, оскільки він забезпечує комплексність та системність розслідування, враховуючи як секторальну специфіку об'єктів критичної інфраструктури, так і оцінку потенційних ризиків та загроз. Водночас, доцільно доповнити цей підхід елементами проактивної моделі, запропонованої Р. Барнсбі (Robert Barnsby), що дозволить не лише ефективно розслідувати вже вчинені правопорушення, але й запобігати потенційним атакам на об'єкти критичної інфраструктури.

Продовжуючи, слід зазначити, що дослідження проблематики досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури ЄС та США вимагає з'ясування його частин: визначення поняття «критична інфраструктура», об'єкта забезпечення безпеки, загроз та особливостей досудового розслідування кримінальних правопорушень.

Так, у Сполучених Штатах Америки, які мають найбільший досвід нормативно-правового регулювання та правозастосовної практики у сфері захисту критичної інфраструктури, поняття «критична інфраструктура» (далі – KI) було закріплено в Директиві про рішення Президента № 63 «Про захист критичної інфраструктури» від 1998 року [47]. Згідно з цим документом критична інфраструктура розглядається як фізичні та кіберсистеми, необхідні для мінімального забезпечення операцій економіки й уряду. Вони містять, однак не обмежуються такими компонентами як: телекомунікації, енергетика, банківська справа і фінанси, транспорт, водні системи та служби екстреної допомоги (як державні, так і приватні) [47]. У цьому визначенні привертає увагу акцент на функціональному призначенні критичної інфраструктури – забезпеченні мінімальних операцій економіки та уряду, що підкреслює її стратегічне значення для нормального функціонування держави.

Американський підхід до визначення критичної інфраструктури є доволі широким і охоплює різноманітні сектори. У США до об'єктів критичної інфраструктури, що підлягають захисту, належать: сільське господарство і продовольство (ферми, підприємства з виробництва продовольчих продуктів); водні ресурси (федеральні резервуари, очисні споруди, водопроводи); охорона здоров'я (лікарні, банки крові, лабораторії); служби екстреної допомоги (медична, поліцейська, пожежна); оборонно-промислова база (дослідження, розробка, науково-виробничі підприємства); інформаційні технології (інтернет, програмне забезпечення, центри обробки й зберігання даних); телекомунікації (супутники, наземні станції, магістральні лінії зв'язку, центри комутації); енергетика (нафто- й газопроводи, електричні підстанції, атомні електростанції); транспорт (аеропорти, шляхи, порти, громадський тран-

спорт); банки і фінанси (інститути кредитування, банки, інформаційні мережі); пошта і доставлення (сортувальні центри, транспорт); національні пам'ятки і символи (статуя Свободи, Вашингтонський монумент); хімічний сектор (заводи, лабораторії, науково-дослідні розробки); комерційні об'єкти (торгові центри, бізнес-центри, розважальні комплекси) [39]. Такий широкий перелік свідчить про всеосяжний підхід до формування системи захисту критичної інфраструктури в США.

У країнах Європейського Союзу поняття критичної інфраструктури також отримало нормативне закріплення, але з певними особливостями. Як зазначається у дослідженні Національного інституту стратегічних досліджень України [9], під критичною інфраструктурою розуміють об'єкти та системи, настільки важливі для забезпечення життєдіяльності людей і держави, дестабілізація роботи яких, не кажучи вже про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків [11]. Таке визначення наголошує на потенційних наслідках порушення функціонування об'єктів критичної інфраструктури, що є важливим для розуміння суспільної небезпечності кримінальних правопорушень, які вчиняються на таких об'єктах.

Цікаво, що в європейському підході спостерігається еволюція термінології – від концепції «захисту критичної інфраструктури» до концепції «стійкості критично важливих об'єктів». Це відображено у зміні основного нормативного документа ЄС у цій сфері – з Директиви ЕСІ 2008 року «Про ідентифікацію та призначення об'єктів європейської критичної інфраструктури та оцінку необхідності поліпшення їхнього захисту» [6; 20] на Директиву CER 2022 року «Про стійкість критично важливих об'єктів» [28]. Наведене свідчить про розширення підходу до проблеми і розвиток від суто захисних заходів до підвищення загальної стійкості від загроз систем критичної інфраструктури. Отже, розкриємо особливості досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури США та ЄС крізь призму правового та організаційного аспектів.

Так, нормативно-правова база США у цій сфері є розгалуженою та динамічною, вона постійно вдосконалюється з урахуванням нових викликів та загроз. Американська модель правового регулювання у цій сфері ґрунтується на поєднанні законів, підзаконних актів, президентських директив та стратегій, що забезпечує гнучкість та адаптивність до нових викликів та загроз. Основоположним законом у сфері захисту критичної інфраструктури в США є Закон про безпеку критичної інфраструктури (Critical Infrastructure Security Act) 2001 року [56], прийнятий після терористичних атак 11 вересня. Законом вперше на законодавчому рівні було визначено поняття критичної інфраструктури, встановлено механізми її захисту та визначено повноваження федеральних органів у сфері розслідування кримінальних правопорушень на таких об'єктах.

У 2002 році було прийнято Закон про внутрішню безпеку (Homeland Security Act) [35], який створив Міністерство внутрішньої безпеки США (Department of Homeland Security) та наділив його повноваженнями щодо координації захисту критичної інфраструктури. Відзначимо, що цей закон встановив основні засади співпраці між федеральними агенціями, органами штатів та приватним сектором у сфері захисту критичної інфраструктури та розслідування правопорушень.

Важливе значення для правового регулювання розслідування кібернетичних атак на об'єкти критичної інфраструктури має Закон про кібербезпеку та захист критичної інфраструктури (Cybersecurity and Critical Infrastructure Protection Act) 2015 року [21]. Він встановив механізми обміну інформацією про кіберзагрози між державним та приватним секторами, а також визначив повноваження правоохоронних органів щодо розслідування кібератак на об'єкти критичної інфраструктури.

У 2019 році було прийнято Закон про захист енергетичної інфраструктури (Protecting and Securing Chemical Facilities from Terrorist Attacks Act) [18], який встановив підвищені вимоги до безпеки об'єктів енергетичної інфраструктури та визначив процедури розслідування правопорушень на таких об'єктах. Законом передбачено створення спеціалізованих підрозділів у структурі Федерального бюро розслідувань (FBI) та Агенції з охорони навколишнього середовища (EPA), які відповідають за розслідування правопорушень на об'єктах енергетичної інфраструктури.

Крім законів, важливу роль у правовому регулюванні досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в США відіграють президентські директиви та виконавчі накази. Зокрема, згадана раніше Президентська Директива з політики національної безпеки 21 (Presidential Policy Directive 21) «Про захист критичної інфраструктури та стійкість» 2013 року [48] встановлює стратегічні рамки для посилення безпеки та стійкості критичної інфраструктури країни.

Виконавчий наказ № 13636 «Про покращення кібербезпеки критичної інфраструктури» 2013 року [30] встановлює механізми обміну інформацією про кіберзагрози між урядом та приватним сектором, а також визначає процедури реагування на інциденти. Ним передбачено створення рамкової програми з кібербезпеки (Cybersecurity Framework), яка включає стандарти, методології, процедури та процеси для ідентифікації, захисту, виявлення, реагування та відновлення після кібератак на об'єкти критичної інфраструктури [44].

У 2021 році був виданий Виконавчий наказ № 14028 «Про покращення національної кібербезпеки» [31], який встановлює нові вимоги до безпеки федеральних інформаційних систем та об'єктів кри-

тичної інфраструктури, а також визначає механізми координації розслідування кібератак. Цей наказ передбачає створення Ради з кібербезпеки (Cyber Safety Review Board) [58], яка відповідає за аналіз значних кіберінцидентів та надання рекомендацій щодо вдосконалення механізмів розслідування.

Важливе значення для забезпечення ефективного розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в США мають також галузеві нормативні акти, такі як Закон про модернізацію енергетичної інфраструктури (Energy Infrastructure Modernization Act) 2020 року [29], Закон про безпеку трубопроводів (Pipeline Security Act) 2021 року [46], Закон про захист водної інфраструктури (Water Infrastructure Protection Act) 2018 року [14] та ін.

Така послідовність правових документів зумовлена метою забезпечення контролю та моніторингу ситуації щодо змін і ризиків у системі КІ з відповідним коригуванням секторальних планів, програмних елементів, концепцій тощо. Тобто кожен наступний документ розробляли відповідно до поточного стану й актуальних проблем захисту КІ, що дало змогу проаналізувати й оцінити ефективність різних заходів, своєчасно реагувати на актуальні запити та потреби секторів і системи загалом, визначати сферу й напрями правового регулювання [55]. Гнучкість у правовому регулюванні є важливою перевагою американської моделі, оскільки дозволяє оперативно реагувати на зміни у сфері загроз критичній інфраструктурі.

Специфічним елементом американської системи захисту критичної інфраструктури є й активна участь приватного сектору. Приватні суб'єкти мають ширші можливості для визначення та реалізації стратегій зниження ризиків і роботи з різними збоями. Державні установи можуть надавати важливі консультації та підтримку [55]. Така модель державно-приватного партнерства у сфері захисту критичної інфраструктури є ефективною, оскільки дозволяє об'єднати ресурси та експертизу обох секторів.

Щодо досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури, то у США цей процес ґрунтується на особливостях, що зумовлені федеративним устроєм держави та специфікою розподілу повноважень між різними рівнями влади.

Особливістю американської правової бази у сфері досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури є наявність спеціалізованих процесуальних норм, які враховують специфіку таких розслідувань та забезпечують баланс між ефективністю розслідування та захистом прав і свобод громадян.

Так, досудове розслідування у США здійснюється відповідно до Кримінального кодексу США. Цей кодекс визначає правові засади досудового розслідування, зокрема, порядок його проведення, повноваження слідчих та права підозрюваних [7].

Тобто американська система досудового розслідування характеризується децентралізованим підходом, де розслідуванням можуть займатися як федеральні агентства, так і правоохоронні органи штатів та місцевого рівня. Для розслідування особливо складних або резонансних злочинів часто створюються спільні слідчі групи, до складу яких входять представники федеральних та місцевих органів. Слідчі у США мають широкі повноваження, в тому числі право на обшук, затримання та допит підозрюваних [7]. Така гнучка структура дозволяє ефективно розподіляти ресурси та оперативно реагувати на різні типи загроз.

Американська правова система передбачає спеціальні процедури для таких випадків, включаючи терміновий звіт до керівництва Департаменту юстиції у випадках: значного пошкодження або суттєвої втрати функціональності федерального, державного, місцевого чи територіального урядового органу; значного пошкодження інфраструктури іноземної держави; злочинів, пов'язаних із іноземним зловмисним впливом; атак на критичну інфраструктуру [60].

Федеральне бюро розслідувань (FBI) також відіграє ключову роль у розслідуванні кримінальних правопорушень на об'єктах критичної інфраструктури, особливо коли йдеться про загрози національного масштабу або кібератаки. Департамент внутрішньої безпеки (DHS) відповідає за координацію діяльності різних агентств та рівнів влади щодо захисту критичної інфраструктури [25]. У структурі DHS функціонує Агентство з кібербезпеки та безпеки інфраструктури (CISA) [22], яке спеціалізується на захисті федеральної інфраструктури від кібератак.

Особливу увагу в американській системі приділено захисту інформації, пов'язаної з критичною інфраструктурою. Програма захищеної інформації критичної інфраструктури (Protected Critical Infrastructure Information Program, PCII) забезпечує метод для власників критичної інфраструктури добровільно подавати інформацію федеральному уряду, до якої уряд інакше не мав би доступу [52]. Ця програма має унікальний характер, оскільки передбачає захист поданої інформації від розголошення згідно із законами про свободу інформації та від використання у цивільних судових процесах або для регуляторних цілей.

Важливою рисою американської системи досудового розслідування є координація діяльності різних органів. Так, у системі досудового розслідування США взаємодія між державними і приватними структурами відіграє визначальну роль. Урядові агентства активно співпрацюють з приватними підприєм-

ствами, які володіють або керують критичною інфраструктурою, що дозволяє значно підвищити рівень безпеки та оперативності реагування на загрози. Така модель сприяє швидкому збору інформації, виявленню загроз та запобіганню потенційним атакам на стратегічно важливі об'єкти. Крім того, ключовим є активне залучення до розслідувань експертних груп та використання передових технологій, включаючи штучний інтелект та аналіз великих даних, що дозволяє правоохоронцям США оперативно виявляти та нейтралізовувати потенційні загрози критичній інфраструктурі.

Крім того, у США діє система досудового обслуговування (Pretrial Services) [49]. Відповідно до інформації з офіційного сайту судів США, співробітники досудового обслуговування слугують вхідними дверима до кримінального судочинства у федеральній судовій системі. Розташовані в кожному окружному суді США, співробітники досудового обслуговування працюють з людьми, яким висунуто звинувачення у федеральних злочинах і які очікують на суд, допомагаючи забезпечити повернення підсудних до суду для запланованих виступів і не становлять небезпеки для громади [50]. Ця система є важливим складником кримінального процесу в США, забезпечуючи належне функціонування судової системи та захист прав підозрюваних.

Особливу увагу в американській моделі досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури приділяють міжнародному співробітництву. Це обумовлено транснаціональним характером багатьох загроз критичній інфраструктурі, зокрема в кіберпросторі. США активно розвивають міжнародні інструменти співпраці, що дозволяють правоохоронним органам збирати докази та обмінюватися інформацією з партнерами за кордоном (уже згадане Агентство кібербезпеки та безпеки інфраструктури (CISA), яке координує зусилля різних відомств у сфері захисту критичної інфраструктури [22]).

Одним із таких інструментів є також «CLOUD Act» (Clarifying Lawful Overseas Use of Data Act) [19] який дозволяє правоохоронним органам США отримувати доступ до даних, що зберігаються за кордоном, для розслідування серйозних злочинів, включаючи злочини проти критичної інфраструктури [36]. Однак, як зазначається у дослідженні CEPS (Центр європейських політичних досліджень) [17], такі інструменти можуть створювати конфлікти юрисдикцій та потенційно порушувати суверенітет інших держав. Конфлікти законів можуть лише посилюватися інструментами, які сприяють прямому й неопосередкованому екстериторіальному здійсненню кримінальної юрисдикції. Це особливо справедливо, коли такі інструменти використовуються органами, що діють у різних системах кримінального правосуддя, з різними традиціями [37]. Ця критика є важливою для розуміння обмежень та потенційних проблем, пов'язаних з міжнародним співробітництвом у сфері розслідування злочинів проти критичної інфраструктури.

Правове регулювання захисту критичної інфраструктури та досудового розслідування правопорушень на її об'єктах у Європейському Союзі теж має свої особливості, які відрізняють його від американської моделі. Ці особливості обумовлені специфікою правової системи ЄС, яка поєднує наднаціональне регулювання з національними правовими системами держав-членів.

ЄС розробив комплексну правову базу для захисту критичної інфраструктури, яка включає і аспекти досудового розслідування кримінальних правопорушень на відповідних об'єктах. Основним документом ЄС у сфері захисту критичної інфраструктури довгий час була згадана раніше Директива ECI 2008 року «Про ідентифікацію та призначення об'єктів європейської критичної інфраструктури та оцінку необхідності поліпшення їхнього захисту» [6; 20]. Однак у 2022 році її замінила Директива CER «Про стійкість критично важливих об'єктів» [5; 28]. Цей документ встановлює загальні принципи та підходи до захисту критичної інфраструктури, включаючи аспекти розслідування.

І, як зазначено, ця зміна відображає еволюцію підходів ЄС до проблеми – від концепції захисту до концепції стійкості, від поняття критичної інфраструктури до поняття «критично важливого об'єкта». Стійкість у цьому контексті слід розуміти як здатність об'єкта не лише витримувати атаки та інші негативні впливи, але й швидко відновлюватися після них, продовжуючи виконувати свої функції. Така концепція, на наш погляд, є більш комплексною та відповідає сучасним викликам у сфері безпеки критичної інфраструктури.

У 2016 році було прийнято Директиву ЄС 2016/1148 «Про заходи щодо забезпечення високого рівня безпеки мережевих та інформаційних систем у Союзі» (NIS Directive) [4; 26], яка розширила сферу захисту критичної інфраструктури, включивши до неї цифрові послуги та інформаційні системи. NIS Directive встановлює механізми співпраці між державами-членами ЄС у сфері кібербезпеки, визначає вимоги до національних стратегій кібербезпеки, а також встановлює обов'язки операторів основних послуг та постачальників цифрових послуг щодо управління ризиками та звітування про інциденти.

У грудні 2020 року Європейська Комісія представила пропозицію щодо нової Директиви NIS 2 [51], яка має замінити наявну Директиву NIS та посилити вимоги до кібербезпеки критичної інфраструктури. NIS 2 розширює сферу застосування попередньої директиви, включаючи нові сектори та послуги, посилює вимоги до безпеки та звітності, а також передбачає більш суворі заходи нагляду та правозастосування.

У контексті розслідування кримінальних правопорушень на об'єктах критичної інфраструктури особливе значення має Директива ЄС 2017/541 «Про боротьбу з тероризмом» [27], яка встановлює мінімальні стандарти щодо визначення терористичних злочинів та покарання за них, включаючи атаки на критичну інфраструктуру. Як зазначає І.І. Маринів, ця Директива вперше на рівні ЄС криміналізує атаки на інформаційні системи критичної інфраструктури, що використовуються для надання основних послуг населенню [8].

Не менш важливим документом є Регламент (ЄС) 2016/679 «Про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних» (GDPR) [53], який встановлює правила обробки персональних даних, у тому числі в контексті розслідування кримінальних правопорушень. GDPR передбачає особливий режим обробки персональних даних правоохоронними органами, що має важливе значення для розслідування кіберзлочинів на об'єктах критичної інфраструктури.

На рівні держав-членів ЄС також прийнято спеціальні закони, що регулюють захист критичної інфраструктури та розслідування правопорушень у цій сфері. Наприклад, у Німеччині діє Закон про безпеку інформаційних технологій (IT Security Act) [54], який встановлює посилені вимоги до безпеки критичної інформаційної інфраструктури та надає Федеральному управлінню з інформаційної безпеки (BSI) повноваження щодо моніторингу та реагування на інциденти. У Франції діє Закон про військове програмування (Loi de programmation militaire) [40], який містить положення щодо захисту критичної інфраструктури та встановлює повноваження Національного агентства з безпеки інформаційних систем (ANSSI) [24].

Загалом європейська правова база у сфері захисту критичної інфраструктури та розслідування кримінальних правопорушень характеризується комплексним підходом, який поєднує як загальні принципи та стандарти на рівні ЄС, так і специфічні механізми їх імплементації на національному рівні держав-членів. Особливістю європейського підходу є акцент на державно-приватному партнерстві та залученні операторів критичної інфраструктури до процесів забезпечення її захисту та розслідування інцидентів.

Досвід окремих європейських країн у сфері правового регулювання захисту критичної інфраструктури також представляє значний інтерес. Окрім згаданих Німеччини та Франції, у нормативно-правовій базі Республіки Польща (Закон про управління кризовими ситуаціями) [61] введено термін «захист критичної інфраструктури», під яким розуміються всі зусилля, спрямовані на забезпечення функціональності, неперервності та цілісності критично важливих об'єктів інфраструктури в цілях запобігання загрозам, ризикам і вразливості та обмеження, а також нейтралізації їх наслідків і швидкого оновлення інфраструктури у випадку відмов, атак та інших випадків, що порушують її належне функціонування [2]. Це визначення є досить широким і охоплює різні аспекти захисту критичної інфраструктури – від запобігання загрозам до відновлення після інцидентів.

В Угорщині своєю чергою у 2012 р. прийнятий Закон щодо захисту критичної інфраструктури [12], в якому визначається порядок та принципи визначення об'єктів КІ, що мають бути віднесені до загальноєвропейської КІ. Окрім цього в законі визначені загальні правила щодо реєстрації об'єктів КІ, забезпечення їх безпеки, проведення інспекцій тощо. Також розробляються нормативно-правові акти, що регулюють окремі сектори КІ. Такий секторальний підхід дозволяє враховувати специфіку різних галузей критичної інфраструктури та розробляти відповідні заходи захисту.

Щодо досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури, в ЄС приділяється велика увага транскордонному співробітництву. Це обумовлено тим, що багато об'єктів критичної інфраструктури мають транскордонний характер або їх функціонування залежить від об'єктів, розташованих в інших державах-членах ЄС. У рамках ЄС діє Європейське бюро розслідувань (далі – ЕРРО), яке контролює та організовує досудове розслідування, вирішує, які заходи необхідно прийняти, та делегує їх ЄПРД держави-члена, в якій вони повинні бути виконані [45; 57]. ЕРРО є наднаціональним органом, який координує розслідування та переслідування злочинів, що посягають на фінансові інтереси ЄС. У контексті захисту критичної інфраструктури цей орган може відігравати важливу роль, оскільки багато об'єктів критичної інфраструктури фінансуються з бюджету ЄС.

Водночас особливістю європейської моделі досудового розслідування є система взаємного визнання судових рішень. ЄС обладнав себе набором внутрішньоєвропейських та міжнародних інструментів співпраці, що дозволяють судовим органам збирати та обмінюватися різними категоріями даних, що потрібні як докази у кримінальних провадженнях і зберігаються постачальниками послуг за кордоном [16]. Така система дозволяє ефективно співпрацювати правоохоронним органам різних держав-членів ЄС під час розслідування транскордонних злочинів.

Система судового співробітництва ЄС у сфері транскордонного збору доказів також ґрунтується на системі взаємної «перевірки» рішень у сфері кримінального судочинства. Така система призначена для забезпечення послідовного та ефективного застосування acquis ЄС у сфері кримінального судочинства та захисту даних і водночас для збереження суверенітету держав та конституційної цілісності.

Вона є важливою гарантією дотримання прав людини та принципів верховенства права під час досудового розслідування.

Отже, організаційний аспект досудового розслідування злочинів проти критичної інфраструктури в країнах ЄС та США, як бачимо, має низку спільних рис і відмінностей. У більшості держав-членів ЄС існує централізований підхід до координації зусиль правоохоронних органів у сфері захисту критичної інфраструктури. Наприклад, у Німеччині створено Федеральне відомство із захисту інформаційних технологій (BSI) [34], яке, у тісній взаємодії з Федеральним відомством з кримінальних справ (далі – BKA) [33], забезпечує методичну й оперативну підтримку розслідувань. У Франції функціонує Національне агентство з безпеки інформаційних систем (ANSSI), [13] що співпрацює з жандармерією та іншими спецслужбами щодо інцидентів, пов'язаних із кібератаками на важливі об'єкти. У Великій Британії питанням протидії нападів на критичну інфраструктуру займається National Cyber Security Centre (далі – NCSC) [43], що тісно координує зусилля зі Скотленд-Ярдом [41] та британськими розвідувальними службами. Водночас у кожній країні є своя особливість щодо юрисдикції та розподілу повноважень між поліцією, жандармерією, контррозвідувальними агентствами та прокуратурою.

Для США характерним є багаторівневий підхід, де координаційний центр на федеральному рівні поєднується із залученням локальних і штатних правоохоронних органів. Так, CISA при Міністерстві внутрішньої безпеки США відповідає за вироблення єдиної політики безпеки критичної інфраструктури, а також за централізований обмін інформацією про загрози між штатом і приватним сектором [22]. Однак безпосередні функції досудового розслідування здебільшого лежать на FBI і, за потреби, на інших федеральних агентствах, таких як Secret Service [59]. У випадку загроз із використанням кіберзлочинних технологій великого значення набуває підрозділ Cyber Division у складі FBI, де зосереджені вузькоспеціалізовані фахівці з цифрової криміналістики [32]. На рівні штатів також існують спеціалізовані підрозділи, що взаємодіють із федеральними органами за чітко визначеними протоколами.

Важливо зазначити, що обидві моделі – і європейська, і американська – передбачають змішаний характер взаємодії між державними структурами та приватним сектором. Це пояснюється тим, що більшість об'єктів критичної інфраструктури перебувають у приватній власності, і без їхньої активної співпраці правоохоронні органи не можуть ефективно збирати докази про вчинене правопорушення. Саме тому спеціальні угоди про обмін даними, механізми повідомлення про інциденти, розробка спільних стандартів безпеки й регулярні навчання стали обов'язковими елементами організаційного підходу до захисту та розслідування на критичних об'єктах. І ключовим викликом на цьому шляху є захист комерційної таємниці й конфіденційності користувачів. Тому розробляються спеціальні процедури, які збалансовують інтереси національної безпеки та інтереси приватних компаній, що можуть постраждати від розкриття конфіденційних даних.

Таким чином у державах ЄС відчувається тенденція до уніфікації та централізації зусиль задля підвищення ефективності координації між національними та європейськими структурами. У США ж модель базується на федеративному принципі, де кожен штат може мати власні нюанси регулювання, але водночас існує потужний федеральний центр у формі DHS, FBI та інших відомств, які задають загальну політику і методологію. Утім, обидва підходи ефективні за умови прозорої взаємодії, доступності ресурсів і чіткої регламентації дій кожного учасника процесу.

Аналіз практичних аспектів досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в ЄС та США дозволяє виявити низку проблем та окреслити перспективи вдосконалення цієї діяльності. Так, ключовими проблемами є: 1) технологічні виклики, пов'язані з постійним розвитком та ускладненням методів атак; 2) правові обмеження, які ускладнюють збирання електронних доказів та проведення транскордонних розслідувань; 3) недостатня кваліфікація слідчих у сфері високих технологій; 4) складнощі у встановленні балансу між забезпеченням безпеки та захистом прав і свобод громадян; 5) проблеми координації між різними органами та агенціями, залученими до розслідування.

Водночас слід звернути увагу на проблему атрибуції кібератак, адже одним з найскладніших завдань у розслідуванні кримінальних правопорушень на об'єктах критичної інфраструктури є встановлення джерела атаки та ідентифікація конкретних осіб, відповідальних за її здійснення, оскільки зловмисники використовують різноманітні методи маскування своєї діяльності, такі як проксі-сервери, VPN, Tor, ботнети. Особливо складною є атрибуція атак, спонсорованих державами (state-sponsored attacks), оскільки такі атаки здійснюються з використанням найсучасніших технологій та методів, а також мають високий рівень організації та ресурсного забезпечення.

Підкреслимо й проблему нестачі кваліфікованих кадрів. Як в ЄС, так і в США спостерігається дефіцит слідчих, які мають достатні знання та навички у сфері високих технологій для ефективного розслідування кібератак на об'єкти критичної інфраструктури. Ситуація ускладнюється високою конкуренцією з приватним сектором, який пропонує кращі умови праці та вищу оплату для фахівців з кібербезпеки.

Не менш значущою є проблема недостатньої співпраці між державним та приватним секторами, адже ефективне розслідування кримінальних правопорушень на об'єктах критичної інфраструктури

вимагає тісної співпраці між правоохоронними органами та операторами критичної інфраструктури, однак на практиці така співпраця часто обмежується через недовіру, конфлікт інтересів, а також правові та організаційні бар'єри.

У контексті аналізу досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури відзначимо, що в ЄС діє принцип субсидіарності, згідно з яким питання організації розслідування належать до компетенції держав-членів. Проте, на рівні ЄС створені механізми співпраці правоохоронних органів та обміну інформацією, зокрема, через Європол та Євроюст.

Відповідно, постає проблема балансу між відкритістю та конфіденційністю інформації, адже розслідування кримінальних правопорушень на об'єктах критичної інфраструктури часто вимагає доступу до конфіденційної інформації, яка може стосуватися питань національної безпеки, комерційної таємниці, персональних даних. Забезпечення належного захисту такої інформації при одночасному забезпеченні ефективності розслідування є складним завданням.

Тому перспективами вдосконалення досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури вважаємо наступні напрями: 1) розвиток правової бази, яка б враховувала специфіку таких правопорушень та забезпечувала баланс між ефективністю розслідування та захистом прав і свобод громадян; 2) посилення міжнародного співробітництва, в тому числі через гармонізацію законодавства, укладення міжнародних договорів, створення спільних слідчих груп; 3) впровадження новітніх технологій, таких як штучний інтелект, машинне навчання, автоматизований аналіз даних; 4) розвиток державно-приватного партнерства у сфері розслідування правопорушень на об'єктах критичної інфраструктури; 5) інвестиції у підготовку спеціалізованих кадрів для правоохоронних органів.

Необхідним є також розвиток проактивного підходу до розслідування. Зокрема вдосконалення досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури вимагає переходу від реактивної моделі, орієнтованої на реагування на вже вчинені правопорушення, до проактивної моделі, спрямованої на раннє виявлення загроз, профілактику правопорушень та мінімізацію їх наслідків. Саме такий підхід, на нашу думку, передбачає розвиток систем моніторингу та раннього попередження, проведення випереджувальних оперативно-розшукових заходів, а також тісну співпрацю з операторами критичної інфраструктури.

Що стосується використання технологій штучного інтелекту у досудовому розслідуванні, то штучний інтелект та машинне навчання відкривають нові можливості для автоматизації аналізу великих обсягів даних, виявлення аномалій у функціонуванні систем, прогнозування потенційних загроз, атрибуції атак та підтримки прийняття рішень слідчими. Особливо перспективним є використання технологій штучного інтелекту для аналізу поведінкових шаблонів зловмисників та прогнозування їх дій. На наш погляд, необхідно створити певну систему кримінально-правових засобів, до яких слід включити кримінально-правові норми (заборонні, роз'яснювальні, заохочувальні та обмежувальні) та методи кримінально-правової політики (криміналізація та декриміналізація, пеналізація та депеналізація), за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин.

Важливим аспектом досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури є робота з електронними доказами. Станом на сьогодні, крім кіберзлочинів, електронні докази активно використовуються для розслідування традиційних злочинів. У ЄС понад половина всіх кримінальних розслідувань нині включають транскордонні запити на доступ до електронних доказів, таких як текстові повідомлення, електронні листи або програми обміну повідомленнями.

І нарешті, враховуючи транснаціональний характер багатьох кібератак на об'єкти критичної інфраструктури, ключовим напрямом вдосконалення розслідування є посилення механізмів міжнародної співпраці, включаючи обмін інформацією про загрози, спільні операції, взаємну правову допомогу, екстрадицію. Особливо важливим є розвиток регіональних та глобальних мереж співпраці між правоохоронними органами, такими як Європол, Інтерпол, FBI, а також спеціалізованими підрозділами з кібербезпеки різних держав.

Таким чином досвід ЄС і США демонструє важливість комплексного підходу до досудового розслідування кримінальних правопорушень на об'єктах КІ. Україні доцільно адаптувати найкращі практики цих країн із врахуванням специфіки національного законодавства та сучасних викликів.

Висновки. Дослідження досвіду досудового розслідування кримінальних правопорушень на об'єктах критичної інфраструктури в ЄС та США засвідчило значну увагу до питань правового, організаційного та методологічного забезпечення цього процесу. Проаналізовані підходи свідчать про важливість комплексної стратегії захисту критичної інфраструктури, що передбачає як попередження, так і оперативне реагування на них.

Правове регулювання досудового розслідування в США та ЄС суттєво відрізняється. Американська система характеризується гнучкістю, що забезпечується поєднанням федеральних і штатних законодавчих актів, активним залученням приватного сектору та значними повноваженнями правоохорон-

них органів, зокрема ФБР та Міністерства внутрішньої безпеки (DHS). Водночас у ЄС діє уніфікований підхід із впровадженням директив, спрямованих на гармонізацію розслідувань між державами-членами, та активною роллю Європолу й Євроюсту. Важливою особливістю європейської моделі є орієнтація на підвищення стійкості критично важливих об'єктів, а не лише на їхній захист.

Методологічні аспекти досудового розслідування в США та ЄС мають як спільні, так і відмінні риси. В обох системах велика увага приділяється впровадженню проактивного підходу, що передбачає раннє виявлення загроз та запобігання кримінальним посяганням, використанню сучасних технологій для аналізу загроз і забезпечення кібербезпеки, а також розвитку співпраці між державним і приватним секторами. Водночас у США спостерігається більший рівень децентралізації та координації між федеральними і локальними структурами, тоді як ЄС акцентує на транскордонній співпраці та централізації відповідних механізмів.

Значну роль у досудовому розслідуванні кримінальних правопорушень на обєктах критичної інфраструктури відіграють інформаційні технології та штучний інтелект. Використання алгоритмів машинного навчання, автоматизованого аналізу даних та поведінкових моделей злочинців є перспективним напрямом удосконалення слідчих методик. Особливої уваги потребує проблема атрибуції кіберзлочинів, що ускладнює встановлення винних осіб та притягнення їх до відповідальності. Досвід ЄС та США демонструє, що для ефективного розслідування важливе впровадження єдиних стандартів збору та використання електронних доказів, а також посилення співпраці між державами.

Перспективи подальших досліджень полягають у розробці правових механізмів удосконалення досудового розслідування шляхом гармонізації законодавства, інтеграції новітніх криміналістичних технологій, посилення державно-приватного партнерства та підготовки висококваліфікованих фахівців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Батюк О.В. Криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури: монографія. Луцьк: Волиньполіграф, 2021. 455 с.
2. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналіт. доп. Київ : НІСД, 2012. 57 с. URL: https://niss.gov.ua/sites/default/files/2012-09/zah_ynfrastr-b98c0.pdf (дата звернення: 04.03.2025).
3. Герасименко О.М. Організаційно-правові засади захисту критичної інфраструктури: міжнародний досвід та перспективи для України. *Юридичний науковий електронний журнал.* 2024. № 10. С. 68–72. URL: http://www.lsej.org.ua/10_2024/16.pdf (дата звернення: 04.03.2025).
4. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. *Офіційний вісник Європейського Союзу*. 2016. L 194. С. 1–30.
5. Директива (ЄС) 2022/2557 Європейського Парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів та скасування Директиви Ради 2008/114/ЄС. *Офіційний вісник Європейського Союзу*. 2022. L 333. С. 164–206.
6. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності вдосконалення їх охорони та захисту. *Офіційний вісник Європейського Союзу*. 2008. L 345. С. 75–82. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj (дата звернення: 03.03.2025).
7. Коломієць В.І. Зарубіжний досвід взаємодії між органами досудового розслідування та можливості його використання в Україні. *Вісник Кримінологічної асоціації України*. 2023. № 1 (28). С. 226–233. DOI: https://doi.org/10.32631/vca.2023.1.20.
8. Маринів І.І. Боротьба з тероризмом в світлі актів Європейського Союзу та Ради Європи (співвідношення права Європейського Союзу з міжнародним правом). *Вісник Національного юридичного університету імені Ярослава Мудрого.* Серія: Міжнародне право. 2019. № 8. С. 19–27. URL: https://dspace.nlu.edu.ua/bitstream/123456789/16197/1/Maryniv_19-27.pdf (дата звернення: 04.03.2025).
9. Національний інститут стратегічних досліджень: офіційний сайт. URL: https://niss.gov.ua/ (дата звернення: 04.03.2025).
10. Саковський А.А., Єфіменко І.М., Хоруженко О.С. та інші. Розслідування посягань на об'єкти критичної інфраструктури: методичні рекомендації. Київ: НАВС, 2023. 73 с.
11. Теленик С.С. Досвід правового регулювання системи захисту критичної інфраструктури в США. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 2 (107). С. 358–370.
12. Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities. Hungarian Official Journal. 2012. URL: https://nki.gov.hu/wp-content/uploads/2020/11/CIP-Act_2012_166.pdf (дата звернення: 03.03.2025).
13. Agence nationale de la sécurité des systèmes d'information. Site officiel. URL: https://www.ssi.gouv.fr/ (дата звернення: 04.03.2025).

14. America's Water Infrastructure Act of 2018, Pub. L. No. 115–270, 132 Stat. 3765 (2018).
15. Barnsby R. A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership. *The Cyber Defense Review*. 2020. Vol. 5, No. 3. P. 29–44.
16. Carrera S., Stefan M., Mitsilegas V. Cross-border data access in criminal proceedings and the future of digital justice : Report of a CEPS and QMUL Task Force. Brussels : CEPS, 2020. 85 p. URL: https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf (дата звернення: 04.03.2025).
17. Centre for European Policy Studies : вебсайт. URL: https://www.ceps.eu/about-ceps/ (дата звернення: 03.03.2025).
18. Chemical Facility Anti-Terrorism Standards Program Extension Act: Public Law 116-2. URL: https://www.congress.gov/bill/116th-congress/house-bill/251 (дата звернення: 04.03.2025).
19. Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213-1225 (2018).
20. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. 2008. L 345. P. 75–82. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj (accessed: 03.03.2025).
21. Cybersecurity Act of 2015. Public Law 114-113, Division N. URL: https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf (дата звернення: 04.03.2025).
22. Cybersecurity and Infrastructure Security Agency : вебсайт. URL: https://www.cisa.gov/about (дата звернення: 03.03.2025).
23. Cybersecurity and Infrastructure Security Agency. Official website. URL: https://www.cisa.gov/ (date of access: 03.03.2025).
24. Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». Journal officiel de la République française. 2009. URL: https://www.legifrance.gouv.fr/loda/id/ JORFTEXT000020828212/ (дата звернення: 03.03.2025).
25. Department of Homeland Security. URL: https://www.dhs.gov/ (дата звернення: 04.03.2025).
26. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016. L 194. P. 1–30.
27. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. Official Journal of the European Union. 2017. L 88. P. 6□21.
28. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union. 2022. L 333. P. 164–202. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed: 03.03.2025).
29. Energy Act of 2020, Pub. L. No. 116-260, div. Z, 134 Stat. 1182 (2020).
30. Executive Order No. 13636. Improving Critical Infrastructure Cybersecurity. Federal Register. 2013. Vol. 78, No. 33. P. 11739-11744. URL: https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf (дата звернення: 04.03.2025).
31. Executive Order No. 14028. Improving the Nation's Cybersecurity. Federal Register. 2021. URL: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity (дата звернення: 04.03.2025).
32. Federal Bureau of Investigation. Cyber Crime. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 03.03.2025).
33. Federal Criminal Police Office. Official website. URL: https://www.bka.de/EN/Home/home_node.html (дата звернення: 04.03.2025).
34. Federal Office for Information Security. Official website. URL: https://www.bsi.bund.de/EN/Home/home_node.html (дата звернення: 03.03.2025).
35. Homeland Security Act of 2002. Public Law 107-296. URL: https://www.dhs.gov/ sites/default/files/2023-11/23_0930_HSA-2002-updated.pdf (дата звернення: 04.03.2025).
36. It's all about the data – regulatory barriers to cross-border investigations. Forensic Risk Alliance: вебсайт. URL: https://www.forensicrisk.com/news-and-insights/its-all-about-the-data–-regulatory-barriers-to-cross-border-investigations (дата звернення: 04.03.2025).
37. Kaiafa-Gbandi M. Jurisdictional Conflicts in Criminal Matters and their Settlement within EU's Supranational Settings. *EuCLR*. 2017. Vol. 7, No. 1. P. 30–41. DOI: 10.5771/2193-5505-2017-1-30.
38. Kondratov S.I., Sukhodolia O.M. The State Critical Infrastructure Protection System in the National Security System: the analytical report / general editor: O.M. Sukhodolia. Kyiv : NISS, 2020. 28 p.

URL: https://niss.gov.ua/sites/default/files/2020-12/english-version-cip-dopovid_0.pdf (дата звернення: 04.03.2025).
39. Littlewood J. US Critical Infrastructure Protection under Obama. RUSI : вебсайт. URL: https://rusi.org/publication/us-critical-infrastructure-protection-under-obama (дата звернення: 04.03.2025).
40. Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. Journal officiel de la République française. 2023. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000047914986/ (дата звернення: 03.03.2025).
41. Metropolitan Police. Official website. URL: https://www.met.police.uk/ (date of access: 03.03.2025).
42. Mulyk K.T. Historical and theoretical issues of implementation of pre-trial investigation provisions. Visegrad Journal on Human Rights. 2023. № 5. P. 164–202. DOI: https://doi.org/10.61345/1339-7915.2023.5.6. URL: https://journals.uran.ua/journal-vjhr/article/ view/295276 (дата звернення: 03.03.2025).
43. National Cyber Security Centre (United Kingdom). Wikipedia : website. URL:https://en.wikipedia.org/wiki/National_Cyber_Security_Centre_(United_Kingdom) (дата звернення: 03.03.2025).
44. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018. URL: https://nvlpubs.nist.gov/ nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата звернення: 04.03.2025).
45. Operational cooperation. European Commission: вебсайт. URL: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/operational-cooperation_en (дата звернення: 04.03.2025).
46. Pipeline Security Act: H.R. 3243, 117th Congress. 2021.
47. Presidential Decision Directive/NSC-63: Critical Infrastructure Protection. Washington: The White House, 1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (дата звернення: 03.03.2025).
48. Presidential Policy Directive – Critical Infrastructure Security and Resilience. The White House. 2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата звернення: 04.03.2025).
49. Pretrial services programs. Wikipedia: вебсайт. URL: https://en.wikipedia.org/ wiki/Pretrial_services_programs (дата звернення: 03.03.2025).
50. Pretrial Services. United States Courts: веб-сайт. URL: https://www.uscourts.gov/about-federal-courts/probation-and-pretrial-services/pretrial-services (дата звернення: 04.03.2025).
51. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. COM/2020/823 final. European Commission: вебсайт. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (дата звернення: 03.03.2025).
52. Protected Critical Infrastructure Information (PCII) Program. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program (дата звернення: 04.03.2025).
53. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88.
54. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union*. 2019. L 151. P. 15–69. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (date of access: 03.03.2025).
55. Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure. Cyberspace Solarium Commission 2.0: вебсайт. URL: https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/ (дата звернення: 04.03.2025).
56. S. 1456 – Critical Infrastructure Information Security Act of 2001. 107th Congress (2001-2002). URL: https://avalon.law.yale.edu/sept11/s1456_is.asp (дата звернення: 04.03.2025).
57. The European Public Prosecutor's Office (EPPO) is off to an active and promising start. Navacelle Law. URL: https://navacelle.law/the-european-public-prosecutors-office-eppo-is-off-to-an-active-and-promising-start/ (дата звернення: 04.03.2025).
58. U.S. Department of Homeland Security. Cyber Safety Review Board (CSRB). URL: https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb (дата звернення: 04.03.2025).
59. United States Secret Service. Official website. URL: https://www.secretservice.gov/ (дата звернення: 03.03.2025).

60. Urgent Reports. Justice Manual. URL: https://www.justice.gov/jm/jm-1-13000-urgent-reports (дата звернення: 04.03.2025).
61. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dziennik Ustaw. 2007. Nr 89. poz. 590. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/ U/D20070590Lj.pdf (дата звернення: 03.03.2025).