УДК 342.9:004.056:351.86
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364481

Ярослав Сергійович Мануілов
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0001-8149-2745

ПРОТИДІЯ ФІЗИЧНИМ КІБЕРЗАГРОЗАМ ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: МІЖНАРОДНИЙ ДОСВІД ТА СТРАТЕГІЧНІ ПРІОРИТЕТИ

Анотація. *У статті здійснено теоретико-правове дослідження трансформації безпекової парадигми в умовах конвергенції цифрового та фізичного просторів. Автор обґрунтовує перехід від класичної концепції "кібербезпеки" до ширшої парадигми "кіберфізичної стійкості", де об'єктом правового захисту виступає не лише інформація, а безперебійність технологічних процесів критичної інфраструктури. Особливу увагу приділено новому класу загроз — фізичним кіберзагрозам, які є латентними для традиційних програмних засобів моніторингу. На основі аналізу знакових кібератак (Stuxnet, Triton, NotPetya) доведено, що кіберінструментарій сьогодні виконує роль "детонатора" для фізичного руйнування матеріальних об'єктів. Міститься аналіз зарубіжного досвіду, зокрема інтегрованої моделі ЄС, що базується на синергії Директив ЄС NIS2 (цифрова безпека) та CER (фізична стійкість). Проаналізовано досвід США щодо впровадження концепції "Secure by Design", яка зміщує фокус відповідальності за вразливості з оператора критичної інфраструктури на виробника обладнання. Зроблено висновок, що ефективний захист критичної інфраструктури можливий лише за умови правової конвергенції фізичних та цифрових заходів безпеки, зкоординованих з діями спецслужб, правоохоронних органів та Збройних Сил України.*

Ключові слова*: критична інфраструктура, кіберфізична стійкість, фізичні кіберзагрози, Директива NIS2, активна кібероборона, кібердиверсія, воєнний стан.*

Yaroslav S. Manuilov
Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
Kyiv Ukraine
ORCID: https://orcid.org/0000-0001-8149-2745

COUNTERING PHYSICAL CYBER THREATS AND CRITICAL INFRASTRUCTURE PROTECTION: INTERNATIONAL EXPERIENCE AND STRATEGIC PRIORITIES

Summary*. The article provides a theoretical and legal study of the transformation of the security paradigm in the context of the convergence of digital and physical spaces. The author substantiates the transition from the classical concept of "cybersecurity" to a broader paradigm of "cyber-physical resilience", where the object of legal protection is not only information but the continuity of technological processes of critical infrastructure (CI). Particular attention is paid to a new class of threats — physical cyber threats, which remain latent to traditional software-based monitoring tools.*

Based on an analysis of landmark attacks (Stuxnet, Triton, NotPetya), it is demonstrated that cyber tools currently serve as a "detonator" for the physical destruction of material objects.

The study includes an analysis of international experience, specifically the EU's integrated model based on the synergy of the NIS2 (digital security) and CER (physical resilience) Directives. The US experience in implementing the "Secure by Design" concept, which shifts the focus of responsibility for vulnerabilities from the CI operator to the equipment manufacturer, is analyzed. It is concluded that effective CI protection is possible only through the legal convergence of physical and digital security measures, coordinated by the actions of intelligence services, law enforcement agencies, and the Armed Forces of Ukraine.

Keywords: *critical infrastructure, cyber-physical resilience, physical cyber threats, NIS2 Directive, active cyber defense, cyber sabotage, martial law.*

Постановка проблеми. Сучасна еволюція глобальних безпекових викликів характеризується остаточним стиранням меж між цифровим та фізичним просторами. Сьогодні концепція “кібербезпеки” трансформувалася в ширшу парадигму “кіберфізичної стійкості”, де атака на програмне забезпечення має на меті руйнування матеріальних об’єктів — від енергомереж до систем водопостачання. Для України, яка перебуває в епіцентрі повномасштабної кібервійни, захист критичної інфраструктури (КІ) став питанням виживання держави як суверенного суб’єкта[1].

Актуальність теми захисту об’єктів критичної інфраструктури зумовлена появою нового класу загроз — фізичних кіберзагроз, що передбачають кібердиверсії проти апаратного забезпечення, сенсорів, кабельних ліній та космічного сегмента передачі даних. Традиційні юридичні механізми, що розділяли “фізичну охорону” та “ІТ-безпеку”, виявилися неефективними проти скоординованих кібератак, де кіберінструменти використовуються як детонатор для фізичного знищення інфраструктури. Це вимагає від юридичної науки розробки цілісної концепції правового захисту кіберфізичного простору, інтегрованої в міжнародну систему колективної безпеки[2].

Сучасна парадигма безпеки критичної інфраструктури базується на усвідомленні нерозривності цифрового та фізичного просторів. Об’єкти енергетики, водопостачання, транспорту, оборонно-промислового комплексу та інші об’єкти критичної інфраструктури стають цілями гібридних атак, де фізичне проникнення або пошкодження апаратної частини є прелюдією до масштабного кіберінциденту[3].

Актуальність тематики цієї статті також зумовлена необхідністю адаптації національного законодавства України до стандартів ЄС (зокрема Директиви NIS2) в умовах правового режиму воєнного стану, що вимагає переосмислення методів захисту об’єктів КІ.

Аналіз останніх досліджень. Питання захисту критичної інфраструктури від гібридних загроз перебуває у центрі уваги провідних українських та іноземних вчених. Різні аспекти цього питання досліджували М. Боровик[4], Я. Дорогий[5], С. Гнатюк, А. Ковальчук [6], О. Манжай[4], Р. Мурасов[7], О. Потій, О. Скіцько [8], В. Цуркан[5], Р. Ширшов [8] та ін.

Значний внесок у дослідження цієї проблеми зробили зарубіжні дослідники – Р. Лангнер (R. Langner), І. Стергіопулос (E. Stergiopoulos) [9] та Д. Катехакіс (D. Katehakis), Дж. Крістоу (G. Christou), М. Шміт (M. Schmitt), Н.Цагуріас (Ni. Tsagourias) та М. Фаррелл (M. Farrell). Методологію управління ризиками в умовах конвергенції фізичної та цифрової безпеки висвітлювали у своїх працях зарубіжні експерти ЄС та НАТО з питань кібербезпеки - Е. Каспарін (E. Casparine) та Т. Мінарді (T. Minardi) [10]. Дослідження цих експертів спрямовані на створення єдиних

протоколів взаємодії між операторами КІ та державними органами у разі виникнення транскордонних кіберінцидентів [10].

По-новому розкрив природу кіберфізичних систем (CPS) Р. Лангнер (R.Langner). Аналіз цього вченого атаки Stuxnet став базовим елементом для розробки стратегій ізоляції промислових мереж[11].

Водночас, незважаючи на значну кількість напрацювань зарубіжних та вітчизняних вчених, залишається недостатньо вивченим питання правового та організаційного регулювання використання систем активної кіберпротидії (зокрема систем спуфінгу та джамінгу) цивільними операторами КІ, що зумовлює актуальність цієї статті.

Метою цієї статті є теоретико-правове обґрунтування концепції захисту критичної інфраструктури від фізичних кіберзагроз, виявлення на базі аналізу зарубіжного досвіду прогалин у національному законодавстві, а також розробка пропозицій щодо вдосконалення правового режиму функціонування об’єктів критичної інфраструктури в умовах воєнного стану.

Виклад основного матеріалу. Фізичні кіберзагрози слід розглядати як деструктивний вплив на об’єкти критичної інфраструктури, що здійснюється шляхом фізичного доступу до компонентів автоматизованих систем керування (АСК ТП) або шляхом маніпуляції з фізичним середовищем функціонування сенсорів. На відміну від суто логічних (програмних) деструктивних впливів, сучасні кіберфізичні загрози характеризуються конвергентною природою. Вони охоплюють спектр дій від фізичного заволодіння матеріальними носіями інформації та інсталяції несанкціонованих апаратних модулів (hardware implants) до застосування засобів радіоелектронного подавлення (РЕБ) з метою блокування каналів управління об’єктами критичної інфраструктури. Окрему небезпеку становлять атаки на сенсорні рівні промислових систем (IoT), що призводять до викривлення первинних даних технологічного процесу. Такий комплексний характер втручання нівелює ефективність традиційних засобів мережевого екранування (фаєрволів) та актуалізує потребу в розробці правових механізмів цілісного кіберфізичного захисту, що охоплював би як цифровий, так і матеріальний сегменти інфраструктури [12].

В технічній площині специфіка кіберфізичних загроз полягає у зміщенні вектора атаки з програмно-логічного рівня на апаратну складову (hardware), що нівелює ефективність традиційних систем моніторингу трафіку. При цьому неможливість оперативної ідентифікації технічного джерела впливу та доведення спеціальної мети злочинного діяння суттєво ускладнює процесуальну атрибуцію та формування доказової бази для притягення винних осіб до відповідальності.

Найбільш відомим прикладом фізично-цифрового впливу на критичну інфраструктуру є виявлений у 2010 році шкідливий програмний черв’як Stuxnet. Його унікальність полягала в здатності долати “повітряний зазор” (air-gap) за допомогою заражених USB-накопичувачів, що підтверджує критичну роль фізичного доступу до об’єктів КІ навіть за умови їх повної мережевої ізоляції. Шкідлива програма була націлена на контролери Siemens Step7, які керували частотними перетворювачами центрифуг. Шляхом маніпуляції швидкістю обертання та викривлення показників датчиків у системі моніторингу, ця кібератака призвела до фізичного руйнування обладнання, залишаючись непомітною для операторів [11].

Логіка розвитку кіберфізичних систем (CPS) передбачає, що будь-який датчик температури на атомній станції або контролер тиску в газогоні є потенційною точкою входу для кібератаки. Фізичне пошкодження або заміна даних на рівні сенсорів може призвести до техногенної катастрофи, масштаб якої перевищує наслідки застосування

традиційних видів звичайної зброї. Таким чином, об’єктом правового захисту стає не просто “інформація”, а безперебійність технологічного процесу об’єктів критичної інфраструктури.

Продовженням еволюції таких загроз стала кібератака на нафтохімічний завод у Саудівській Аравії (2017 рік) із використанням шкідливого праграмного забезпечення Triton (Trisys), яка була спрямована безпосередньо на контролери систем протиаварійного захисту (Safety Instrumented Systems, SIS). На відміну від кібератак на ІТ-інфраструктуру, Triton мав на меті деактивувати механізми безпеки, що в разі успіху призвело б до фізичного вибуху або викиду токсичних речовин. Цей випадок продемонстрував, що кіберзагроза фізичній інфраструктурі може мати наслідком масштабну екологічну катастрофу та людські жертви, що переносить проблему з технічної площини в площину національної безпеки [13].

На жаль, Україна давно є об”єктом триваючих кібератак. Найбільш відомою є масштабна кібератака NotPetya у 2017 р., наслідком якої став перегляд підходів до мережевої ізоляції та усвідомлення необхідності захисту не лише даних, а й самих операційних систем управління обєктів критичної інфраструктури.

Аналіз наслідків кібератак для критичної інфраструктури (КІ) України в період 2017–2025 рр. дозволяє простежити еволюцію ворожої стратегії: від поодиноких деструктивних актів до системного кібертероризму, спрямованого на виснаження державного ресурсу та паралізацію системи життєзабезпечення населення.

Після повномасштабного вторгнення рф на територію України кіберпростір остаточно трансформувався у повноцінний театр воєнних дій із вираженою тенденцією до кількісної та якісної ескалації. Понад половину кібератак спрямовано на енергетику, транспорт та фінанси, що свідчить про намір ворога спричинити гуманітарну катастрофу через відключення КІ.

Експоненціальне зростання кількості кіберінцидентів в Україні (з 2194 у 2022 році до 5927 у 2025 році) [14] та якісна трансформація їхнього характеру — від шпигунства до тотальної деструкції кіберфізичних систем — свідчать про те, що цифрова агресія стала невід’ємним компонентом сучасної конвенційної війни. Такий масштабний і системний вплив на національні цифрові ресурси зумовлює об’єктивну необхідність ґрунтовної правової рефлексії та адаптації вітчизняного законодавства до реалій ведення бойових дій у кіберпросторі.

Еволюція кіберзагроз, описана вище, стала головним детермінантом (визначальним фактором) формування сучасної нормативної бази України з питань забезпечення кібербезпеки. Вона висвітлила критичну потребу у переході від фрагментарного регулювання окремих аспектів інформаційної безпеки до розбудови комплексної системи кіберзахисту, де правові норми виступають не лише обмежувальним фактором, а й фундаментом для забезпечення кіберстійкості (resilience) держави.

У цьому контексті особливої ваги набуває аналіз того, наскільки чинне законодавство України, зокрема профільний Закон України “Про критичну інфраструктуру” та Стратегія забезпечення кібербезпеки України, корелюють із динамікою виявлених кіберзагроз та чи здатні ці акти забезпечити належний правовий режим захисту об’єктів у ситуації безперервного кібернетичного тиску.

Закон України “Про критичну інфраструктуру” (2021 р.), будучи базовим елементом правового регулювання у досліджуваній сфері, визначив правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури [15], запровадивши системний підхід до класифікації та захисту стратегічно важливих об'єктів КІ. Проте динаміка кібератак 2022–2024 років

виявила певну статичність законодавчих норм: чинна система категоріювання об'єктів критичної інфраструктури (I–IV категорії критичності) переважно базується на оцінці наслідків фізичного руйнування, тоді як кібернетичний вплив, що призводить до "цифрової паралізації" без механічного пошкодження, потребує більш гнучких критеріїв оцінки кіберризиків. Це зумовлює необхідність переходу від статичного переліку об'єктів до динамічного управління безпековими процесами, що передбачає безперервний аудит вразливостей таких об'єктів.

Логічним доповненням до інституційних засад захисту КІ стала Стратегія кібербезпеки України, яка в умовах воєнного стану трансформувалася з концептуального документа в оперативний план дій із забезпечення кібербезпеки. У Стратегії проголошено, що Україна посилить кіберготовність, що полягатиме у здатності всіх заінтересованих сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури[16]. Ця Стратегія заклала правовий фундамент для розбудови національної екосистеми кібербезпеки, проте саме досвід відбиття атак на енергетику та телекомунікації у 2024 році підтвердив пріоритетність впровадження моделі "кіберстійкості" (resilience). На відміну від класичної "кібероборони", кіберстійкість передбачає здатність системи зберігати мінімально необхідний рівень функціонування навіть в умовах успішного проникнення ворога, що потребує нормативного закріплення обов'язкових стандартів резервування та протоколів швидкого відновлення.

Невід'ємною частиною цієї стійкості є розширення повноважень суб'єктів забезпечення кібербезпеки, зокрема Служби безпеки України у частині проведення активних заходів протидії кібератакам. Аналіз правозастосовної практики свідчить, що пасивний захист периметра об'єктів КІ є недостатнім проти високотехнологічних угруповань, підтримуваних державою-агресором. Відтак, на порядку денному стоїть питання законодавчої легалізації інструментів "активної кібероборони" (Active Cyber Defence), які дозволяють ідентифікувати та нейтралізувати загрози на етапі їх підготовки в інфраструктурі противника, що зумовлює потребу внесення відповідних змін до законів України "Про Службу безпеки України" та "Про критичну інфраструктуру".

Зауважимо, що описана трансформація національного права у сфері забезпечення кібербезпеки відбувається паралельно з процесом європейської інтеграції, що вимагає від України не просто ситуативного реагування на атаки, а повної гармонізації законодавства з acquis communautaire ЄС. Ключовим правовим орієнтиром тут виступає Директива (ЄС) 2022/2555 (NIS2), яка встановлює значно суворіші вимоги до безпеки ланцюгів постачання та персональної відповідальності керівництва за стан кіберзахисту. Впровадження стандартів NIS2 в національне законодавство дозволить створити єдиний безпековий контур із партнерами по ЄС, забезпечуючи автоматизований обмін даними про загрози через захищені канали зв'язку, що є критичним для протидії транскордонним кіберінцидентам [17].

Ключовим досягненням правової думки ЄС стало впровадження регуляторного пакета, що складається з Директиви ЄС 2022/2555 (NIS2) та Директиви ЄС 2022/2557 (CER). Юридична інновація полягає у їхній взаємодоповнюваності: якщо NIS2 фокусується на цифровій безпеці мереж та інформаційних систем, то CER — на фізичній стійкості суб'єктів критичної інфраструктури. Такий дуалістичний підхід

дозволяє державам-членам формувати цілісну оцінку кіберризиків, де кібератака на систему управління розглядається в одному контексті з фізичною диверсією або природною катастрофою [18].

На особливу увагу заслуговує запроваджений у межах NIS2 механізм суворого нагляду за ланцюгами постачання (supply chain security). На відміну від попередніх підходів, де відповідальність за вразливості апаратного чи програмного забезпечення часто була розмитою, сучасне європейське право покладає на операторів КІ обов'язок проводити аудит безпеки кожного елемента системи КІ. Це включає перевірку походження комплектуючих та ідентифікацію потенційних "апаратних закладок", що є критично важливим для протидії фізичним кіберзагрозам у кіберпросторі [19].

З цього приводу цінним й таким, що може бути запозичений під час удосконалення вітчизняної кібербезпеки, є американський досвід щодо запобігання здійсненню фізичних кібератак. У США координацію захисту КІ здійснює Агентство з питань кібербезпеки та безпеки інфраструктури (CISA), діяльність якого базується на принципі добровільного партнерства між державою та приватним сектором. Стратегічний план CISA на 2024–2026 роки передбачає впровадження концепції вбудованої безпеки (Secure by Design), яка вимагає від виробників ІТ-продуктів для КІ брати на себе основний тягар відповідальності за вразливості. Це правове рішення зміщує акцент із "користувача, який помилився", на "виробника, який не забезпечив належний рівень захисту", що є революційним для кіберправа [20].

Крім того, американська модель превентивного реагування "Shields Up", яка розроблена після початку повномасштабної агресії проти України, передбачає безпрецедентний рівень обміну розвідувальними даними про кіберзагрози в реальному часі. Юридично це оформлено через спеціальні угоди про нерозголошення, які дозволяють спецслужбам ділитися секретними індикаторами компрометації з приватними енергетичними чи транспортними компаніями без ризику витоку інформації з обмеженим доступом. Такий механізм дозволяє нейтралізувати кіберзагрози на етапі розвідки противником вразливостей системи [21].

Висновки. Узагальнення світових тенденцій дозволяє стверджувати, що ефективний захист КІ неможливий без правової конвергенції фізичних та цифрових загроз. Традиційний поділ на "кіберзахист" та "фізичну охорону" об'єктів КІ є недостатньо ефективним. Фізичні кіберзагрози (hardware backdoors, маніпуляції з сенсорами) є найбільш небезпечними через свою невидимість для стандартних засобів моніторингу трафіку. Сучасне правове регулювання має базуватися на концепції кіберстійкості (Cyber-Physical Resilience), де об'єктом захисту є не інформація, а безперебійність технологічного циклу таких об'єктів. Це потребує перегляду стандартів належного врядування для ланцюгів постачання обладнання для об'єктів КІ І та ІІ категорій критичності. Офіційна статистика кібератак у період 2022-2025 років показує, що виключно захисні заходи не здатні зупинити таргетовані кібератаки, підтримувані державами. Законодавство України у сфері захисту критичної інфраструктури наразі перебуває на етапі активної трансформації, намагаючись відійти від застарілих моделей кіберзахисту. Правовий режим безпеки КІ має включати легітимні інструменти активної кібероборони для нейтралізації загроз на початкових етапах розвитку у інфраструктурі агресора. Світова практика демонструє, що успіх забезпечується трьома факторами: автоматизацією обміну даними, покладанням персональної відповідальності на керівництво об'єктів КІ за стан кіберзахисту та легалізацією активних заходів кіберзахисту. Для України критично важливим є не просто запозичення правових норм NIS2, а їх адаптація до умов реальної кібервійни, де правовий режим "надзвичайного

стану в кіберпросторі" має бути чітко регламентованим та скоординованим із діями Збройних Сил України, правоохоронних органів та спецслужб.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Список використаних джерел

1. Куліков Є. Сім трендів кібербезпеки на 2026 рік. URL:https://ko.com.ua/sim_trendiv_kiberbezpeki_na_2026_rik_152188.

2. Толкачов М.Ю. Механізми захисту трафіку в кіберпросторі. *Сучасний захист інформації.* 2024. № 4(60). С. 85-99. DOI: 10.31673/2409-7292.2024.040009. URL:file:///C:/Users/user/Desktop/3063-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9477-1-10-20241221.pdf.

3. А. Муравський. Понад 3000 об'єктів критичної інфраструктури в Україні потребують захисту – Кулеба. URL: https://epravda.com.ua/biznes/ponad-3000-ob-yektiv-kritichnoji-infrastrukturi-v-ukrajini-potrebuyut-zahistu-kuleba-819540/.

4. Фізичний та кібернетичний захист об'єктів критичної інфраструктури України органами та підрозділами поліції: навч. посіб. / М.О. Боровик, О.В.Манжай, І.Т. Ларіонова та ін.; МВС України, Харків. нац. унів. Вінниця: ХНУВС. 2025. 317 с.

5. Дорогий Я.Ю., Цуркан В.В. Кібербезпека критичної інфраструктури під час військової загрози. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні*: матеріали XII міжн. наук.-практ. конф., [Київ], (Київ, 21-22 листопада 2024 р.), 2024. С. 3. URL: https://ela.kpi.ua/items/761f174e-462a-4146-a7aa-e3d60b5b5201

6. Ковальчук А.Т. Система правового регулювання захисту об'єктів критичної інфраструктури в україні: сучасний стан та напрями удосконалення. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія ПРАВО. Випуск 90: частина 5. С. 172-184. DOI https://doi.org/10.24144/2307-3322.2025.90.5.21. URL:https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/23-4.pdf

7. Мурасов Р.К., Фараон С.І., Гук О.М. Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2025. №3. Том 54. С. 75–83. DOI: https://doi.org/10.33099/2311-7249/2025-54-3-75-83. URL: https://sit.nuou.org.ua/article/view/338906

8. Скіцько О.І., Ширшов Р.А. Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури. *Юридичний науковий електронний журнал*. 2024. № 10/2024. С. 312-314. URL: https://lsej.org.ua/10_2024/73.pdf.

9. Stergiopoulos E.S. Critical Infrastructure Security and Resilience: A Cyber-Physical Approach. *Journal of Cybersecurity and Information Management*. 2023. Vol. 12. Iss. 4. P. 210–225.

10. Minardi T., Valeriano B. The Hybrid Threat Landscape: Cyber-Physical Attacks on Energy Grids. NATO CCDCOE Research Paper. 2025. 118 p.

11. Langner R. To Kill a Centrifuge: A Technical Analysis of What Stuxnet Did to Iran's Enrichment Plant. The 11. Langner Group. 2013. 36 p. URL: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

12. NIST Special Publication 800-82 Revision 3. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology. 2023. 154 p. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final.

13. Di Pinto A., Dragoni Y., Carcano A. TRITON: The First Malware That Targets Industrial Safety Systems. Nozomi Networks Research. 2017. 22 p. URL: https://www.nozominetworks.com/blog/technical-analysis-triton-industrial-malware/.

14. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37.

15. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/

17. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). OJ L 333. 2022. P. 80–152.

18. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). OJ L 333. 2022. P. 164–198.

19. Regulation (EU) 2019/881 on ENISA (European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). OJ L 151. 2019. P. 15–69.

20. CISA Strategic Plan 2024-2026: Leading the National Effort to Understand, Manage, and Reduce Risk. Washington: CISA, 2024. 68 p. URL: https://www.cisa.gov/strategic-plan.

21. Executive Order 14028 on Improving the Nation's Cybersecurity. The White House, 2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Ярослав Сергійович Мануілов
старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенко, 3, Київ, Україна
email: jpochander@gmail.com

Yaroslav S. Manuilov
Senior Reseacher of the Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
03113, Kyiv Ukraine, M. Vasylenka Str. 3
email: arpserg@ukr.net

Рекомендоване цитування: Мануілов Я.С. Протидія фізичним кіберзагрозам та захист критичної інфраструктури: міжнародний досвід та стратегічні пріоритети. *Інформація і право.* № 2(57)/2026. 2026. С. 210-217. https://doi.org/10.37750/2616-6798.2026.2(57).364481

Suggested Citation: Manuilov Ya. (2026) Countering Physical Cyber Threats and Critical Infrastructure Protection: International Experience and Strategic Priorities. *Information and Law*. 2(57)/2026. 210-217. https://doi.org/10.37750/2616-6798.2026.2(57).364481

Дата надходження статті до редакції: 01.05.2026 р.
Дата прийняття статті до друку після рецензування: 05.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~
~~~~~~~~~~~~