УДК 341:351.861(477)
DOI https://doi.org/10.24144/2307-3322.2025.90.5.21

СИСТЕМА ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА НАПРЯМИ УДОСКОНАЛЕННЯ

Ковальчук А.Т.,
начальник Військової академії, м. Одеса
ORCID:0009-0000-0907-6712

Ковальчук А.Т. Система правового регулювання захисту об'єктів критичної інфраструктури в Україні: сучасний стан та напрями удосконалення.

Стаття присвячена правовому регулюванню забезпечення захисту критичної інфраструктури. Автором у статті поставлено за мету дослідити теоретико-правове регулювання процесів забезпечення функціонування національної системи захисту критичної інфраструктури, визначити окремі проблемні питання, пов'язані з недосконалістю правових засад у цій сфері, та запропонувати шляхи їх вирішення.

Досліджено розвиток і впровадження законодавчих та нормативно-правових актів, які регламентують діяльність у зазначеній сфері. На підставі аналізу ретроспективи розвитку правового регулювання захисту об'єктів критичної інфраструктури та критичної інфраструктури загалом зроблено певні висновки щодо наявного масиву нормативно-правових документів, які регламентують зазначену діяльність, та відповідності їх положень нормам міжнародного права. Також визначено, які з положень потребують подальшого вдосконалення, доопрацювання або доповнення.

Зокрема, зазначається, що у сфері захисту національної системи критичної інфраструктури державою проведено значну роботу з розробки та імплементації законодавчих і нормативно-правових актів, які регламентують відповідну діяльність. У результаті сформовано правовий базис, основу якого складають Конституція України, Закон України «Про критичну інфраструктуру» та галузеві (секторальні) нормативно-правові акти. Розвиток правового регулювання національної системи захисту критичної інфраструктури був обумовлений різними факторами, починаючи з проблем природного й техногенного характеру і завершуючи викликами, спричиненими збройною агресією РФ, воєнними діями як на території України, так і на територіях окремих об'єктів критичної інфраструктури, а також кібератаками на них або на окремі галузі критичної інфраструктури. У своїй більшості нормативно-правові акти приймалися «точково» та стосувалися окремих об'єктів критичної інфраструктури. Вони були характерними для тієї чи іншої складової критичної інфраструктури й характеризувалися відсутністю єдиного підходу щодо їх застосування в інших сферах життєдіяльності або секторах критичної інфраструктури. Перевірка відповідності положень Закону «Про критичну інфраструктуру» вказує на те, що його положення потребують коригування з урахуванням досвіду застосування норм і положень уже чинних у правовому полі нормативно-правових актів, а також доопрацювання й уточнення, внесення змін і доповнень до вже чинних нормативно-правових актів з метою приведення їх у відповідність до Закону.

Ключові слова: критична інфраструктура, національна система захисту критичної інфраструктури, об'єкти критичної інфраструктури, правове регулювання захисту критичної інфраструктури України.

Kovalchuk A.T. System of legal regulation of the protection of critical infrastructure facilities in Ukraine: current state and directions for improvement.

The article is devoted to the legal regulation of critical infrastructure protection. The author aims to examine the theoretical and legal framework for ensuring the functioning of the national critical infrastructure protection system, identify specific issues related to deficiencies in the legal foundations of this area, and propose solutions to address them.

The development and implementation of legislative and regulatory acts governing activities in this area are examined. Based on an analysis of the retrospective development of legal regulation of the protection of critical infrastructure facilities and critical infrastructure in general, certain conclusions have been drawn regarding the existing body of regulatory and legal documents governing these activities and the compliance of their provisions with international law. It also identifies which provisions need further improvement, revision, or supplementation.

Specifically, it is noted that the state has undertaken significant efforts in developing and implementing legislative and regulatory acts to govern the protection of the national critical infrastructure system. As a result, a legal basis has been formed, based on the Constitution of Ukraine, the Law of Ukraine "On Critical Infrastructure" and sectoral regulatory acts. The development of legal regulation of the national critical infrastructure protection system was driven by various factors, ranging from natural and man-made problems to challenges arising from the armed aggression of the Russian Federation, military actions both within Ukraine and at individual critical infrastructure facilities, as well as cyberattacks targeting them or entire sectors of critical infrastructure. Most of the regulatory acts were adopted on a "case-by-case" basis addressing specific critical infrastructure facilities. They were tailored to a particular component of critical infrastructure and lacked a unified approach applicable across other sectors of critical infrastructure or areas of public life. A review of the provisions of the Law "On Critical Infrastructure" indicates that its provisions need to be adjusted taking into account the experience of applying the norms and provisions of regulatory legal acts already in force, as well as the need to refine and clarify, amend and supplement existing regulatory acts in order to align them with the Law.

Key words: critical infrastructure, national critical infrastructure protection system, critical infrastructure facilities, legal regulation of critical infrastructure protection in Ukraine.

Вже понад десять років Україна протистоїть збройній агресії Російської Федерації, яка проявляється в незаконній тимчасовій окупації частини її території та захопленні підприємств і установ критичної інфраструктури, розташованих на цих територіях; понад три роки вона відбиває її широкомасштабний наступ. Під час воєнних дій країна-агресор вдається до численних ракетних та ракетно-дронових ударів по КІУ, при цьому завдаючи уражень об'єктам КІУ (далі – ОКІ) не лише на лінії зіткнення, а й на всю глибину території України. Зазначене призводить до порушення функціонування КІУ та несе загрозу національній безпеці держави в цілому і, як наслідок, спонукає до більш ґрунтовного дослідження правового забезпечення у сфері захисту системи КІУ, в тому числі і його відповідності нормам міжнародного права у сучасних умовах – умовах воєнного стану.

Метою статті є дослідження теоретично-правового регулювання процесів забезпечення функціонування національної системи захисту критичної інфраструктури, визначення окремих проблемних питань, що пов'язані з недосконалістю правових засад у цій сфері, та визначення шляхів їх вирішення.

Постановка проблеми. У сфері захисту національної системи КІУ державою проведено значну роботу щодо розробки та імплементації законодавчих і нормативно-правових актів, які регламентують зазначену діяльність. Розвиток правового регулювання системи захисту КІУ обумовлений різними факторами, починаючи з проблем природного і техногенного характеру, непередбачуваних наслідків розповсюдження програм штучного інтелекту, завершуючи викликами, які спровоковані збройною агресією рф, воєнними діями, як на території України, так і на територіях окремо взятих ОКІ, кібератаками на них та або на окремі галузі КІУ.

Однак, враховуючи беззаперечну актуальність побудови в Україні національної системи захисту КІУ, зміну форм і способів впливу противника на об'єкти КІУ, появу нових загроз, цей процес виявився складним і тривалим, а напрацьовані заходи правового врегулювання потребують подальшого аналізу, визначення необхідності подальшого вдосконалення, доопрацювання системи захисту об'єктів КІУ та систематизації нормативно-правової бази.

Аналіз досліджень та публікацій. Дослідженню проблематики врегулювання та впровадження захисту критичної інфраструктури, її складових присвятили свої праці Бірюков Д.С. [1-3, 5], Бобро Д.Г. [6, 38], Горбулін В.П. [38], Єрменчук О.П. [11, 40], Кондратов С.І. [2, 3, 38], Насвіт О.І. [3], Суходоля О.М. [6, 3, 36-38]. Правові аспекти розбудови захисту національної системи критичної інфраструктури у фінансовій сфері та банківській сфері КІ розглядали Богдан Б.В. [4], Іванов Ю.А. [12], Пядишев В.Г. [34], Солопова І.В. [35], аспекти забезпечення інформаційної безпеки об'єктів критичної інфраструктури досліджували Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. [7].

Правове регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури досліджувались Єрменчуком О.П., Пальчиком М.Л. [11]. Майбутні перспективи застосування штучного інтелекту (ШІ) концептуально оглянуті Богом'я В.І., Гудзь А.С. [39].

Разом з цим, при достатньо широкому, у сенсі напрямків досліджень, глибокому обґрунтуванні різних теоретично-правових і прикладних аспектів розбудови національної системи захисту КІУ, комплексний аналіз національного правового регулювання у сфері захисту КІУ не проводився.

Виклад основного матеріалу. Понад тридцять років Україна розбудовує незалежну державу. За цей час суб'єктами законодавчої ініціативи та парламентом проведено велику роботу з формування національного законодавства та правового регулювання усіх сфер функціонування держави та життєзабезпечення суспільства (населення). На цей період розвитку нашої держави припадає й стрімкий розвиток у сфері інформаційно-комунікаційних технологій та засобів зв'язку, що суттєвим чином вплинуло на функціонування органів державної влади, місцевого самоврядування та управління у всіх сферах життя, а також на організацію діяльності більшості установ і організацій незалежно від форми їх власності. Разом з безумовними перевагами, застосування сучасних технологій призвело до появи нових факторів впливу на стійкість системи державного управління, на безпеку діяльності тих чи інших критично важливих об'єктів господарювання та спонукало державу вживати заходів щодо зменшення або до бажаного унеможливлення стороннього впливу на діяльність, особливо ОКІ та покращення захисту національної КІУ в цілому.

Ретроспектива правового регулювання процесів захисту КІУ вказує на певну повільність у прийнятті та впровадженні законодавчих і нормативно-правових актів, які регламентують діяльність у цій сфері. Законодавчі акти та нормативно-правові акти приймалися по мірі виникнення певних загроз або потреб у тому. Зазначене обумовлене різними факторами, починаючи з проблем природного і техногенного характеру, завершуючи викликами, що пов'язані зі збройною агресією рф, воєнними діями, як на території України, так і на територіях окремо взятих ОКІ, кібератаками на них та/або на окремі галузі КІУ. У своїй більшості нормативно-правові акти приймалися "точково" та стосувалися окремо взятих ОКІ, були притаманними тій чи іншій складовій КІУ і характеризувалися відсутністю єдиного підходу у застосуванні в інших сферах життєдіяльності або секторах КІУ.

Рішучим поштовхом до вдосконалення правового регулювання у сфері захисту національної КІУ стали події, що пов'язані з окупацією рф АР Крим, частини Донецької та Луганської областей, що супроводжувалося інформаційними вкидами та кібератаками; захопленням при цьому ОКІ, здійсненням на них хакерських і озброєних нападів та навіть нанесенням по деяким з них ракетно-бомбових ударів.

Незважаючи на те, що термін "критична інфраструктура" увійшов у науковий обіг ще з середини 1990-х років і спочатку був пов'язаний з інформаційною інфраструктурою, у нормативно-правових актах України поняття "критичної інфраструктури", хоча й вживалося, але не мало законних підстав. Відсутність чіткого визначення цього терміна і, як наслідок, відсутність переліку об'єктів, які мають бути віднесеними до цієї категорії, створювали перешкоду для ефективного виконання заходів щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України.

Наприклад, вперше про небезпеку знищення або порушення функціонування ОКІ було акцентовано увагу в рішенні РНБО України від 01.03.2014 року "Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України" [35], але відсутність переліку об'єктів такої категорії створювала певні перешкоди для ефективного виконання п. 6 вищезазначеного Рішення РНБО, згідно з яким Міністерству внутрішніх справ України наказувалося забезпечити "посилену охорону об'єктів енергетики та критичної інфраструктури"[35]. Справа полягає в тому, що у відповідності до статті 2 Закону України "Про Національну гвардію України" [14], охороні підрозділами МВС підлягають ядерні установки, ядерні матеріали, радіоактивні відходи, інші джерела іонізуючого випромінювання державної власності, важливі державні об'єкти. А отже, не зрозуміло: які саме об'єкти енергетики та критичної інфраструктури мають бути ще підсиленими охороною МВС.

В подальшому, у відповідь на політичну ситуацію, що склалась наприкінці 2014 року – початку 2015 року Президентом України 27 січня 2016 року був підписаний указ про введення в дію рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" [32].

Слід зауважити, що захист інформації безпосередньо впливає на діяльність всіх економічних суб'єктів держави, як на макро-, так і на мікрорівні. Як показує практика, результатами кібератак є знищення та спотворення даних; отримання доступу до секретних і конфіденційних даних; пошкодження пристроїв інформаційної системи; отримання прав на виконання дій, що передбачені тільки для окремих керівних осіб; отримання доступу до здійснення фінансових операцій замість власників рахунків; отримання повного доступу до керування інформаційною системою. Таким чином, своєчасне вжиття заходів щодо організації кібербезпеки на всіх рівнях дозволило попередити кіберзагрози та мінімізувати негативні наслідки кібератак, що в кінцевому випадку має призвести до зменшення збитків та інших негативних соціально-економічних наслідків для всіх економічних суб'єктів.

Саме прийняття цього документу підкреслило важливість захисту КІУ в контексті забезпечення національної безпеки держави. Фактично цим документом було покладено початок формування правового регулювання захисту КІУ, хоча і мало вузько спрямований напрямок розвитку – на захист інформаційно-телекомунікаційних систем та кіберзахист.

Стратегією встановлено комплекс пріоритетів, заходів та напрямів із забезпечення кібербезпеки України, зокрема [32]:

вироблення та оперативна адаптація державної політики, спрямованої на розвиток кіберпростору та досягненні сумісності з відповідними стандартами ЄС та НАТО;

створення державної нормативно-правової та бази термінів у цій сфері;

формування конкурентного середовища у сфері електронних комунікацій.

Реалізація Стратегії кібербезпеки України потребувала внесення низки змін до національного законодавства, що мало забезпечити підґрунтя для впровадження її положень в життя, а також підвищення відповідальності за правопорушення у сфері кібербезпеки.

Постановою Кабінету Міністрів України № 563 від 23 серпня 2016 року затверджений та введений в дію Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [19], в якому вперше надано офіційне визначення поняття "критична інфраструктура", як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку й оборону, природне середовище, призвести до значних фінансових збитків та людських жертв.

З метою проведення відповідних заходів на загальнодержавному, галузевому й регіональному рівнях щодо правового й організаційно-методичного забезпечення, координації та консолідованого забезпечення ресурсами систем безпеки, спільного використання засобів безпеки, що знаходяться в підпорядкуванні окремих відомств, Кабінетом Міністрів України на виконання Рішення РНБО України від 29 грудня 2016 року "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" [31] розроблено Концепцію створення державної системи захисту критичної інфраструктури України, що введена в дію Розпорядженням Кабінету Міністрів України № 1009-р від 06.12.2017 року [21]. Концепція визначила основні напрямки, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління в цій сфері, а також План заходів з реалізації зазначеної вище Концепції [27].

Реалізація Концепції розрахована на десятирічний строк (до 2027 року) та передбачає короткострокові, середньострокові, довгострокові завдання. Зокрема, Концепцією окреслено основні проблеми у сфері побудови державної системи захисту КІУ:

недостатність та неузгодженість нормативно-правового регулювання в Україні захисту систем і об'єктів, які відносять до критичної інфраструктури, зокрема, відсутність у національному законодавстві профільного закону про критичну інфраструктуру та її захист;

відсутність на національному рівні державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури існуючих державних систем захисту та кризового реагування;

невизначеність функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;

відсутність єдиної методології проведення оцінки загроз та ризиків критичній інфраструктурі, запобігання їх реалізації та реагування на загрози;

відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;

нерозвиненість державно-приватного партнерства та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;

недостатній рівень міжнародного співробітництва у цій сфері.

Крім того, у цей період були прийняті важливі законодавчі та нормативно-правові акти, дія яких спрямована на вдосконалення системи національної безпеки та оборони, у більшому ступені, що стосується сфери захисту інформаційно-телекомунікаційних систем, зокрема:

Закон України "Про основні засади забезпечення кібербезпеки України" [16] та на його реалізацію цілу низку нормативно-правових актів галузевої спрямованості:

Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [28];

Постанова Кабінету Міністрів України № 519 від 19.06.2019 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [29];

Постанова Кабінету Міністрів України від 09.10.2020 № 943 "Деякі питання об'єктів критичної інформаційної інфраструктури";

Постанова Кабінету Міністрів України № 519 від 19.06.2019 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [8];

Постанова Кабінету Міністрів України від 9.10.2020 № 1109 "Деякі питання об'єктів критичної інформаційної інфраструктури" [9];

Постанова Кабінету Міністрів України № 1176 від 11.11.2020 "Про затвердження порядку проведення огляду стану кіберзахисту критичної інфраструктури, державних інформаційних ресурсів та інформації, вимоги щодо захисту якої встановлені законом" [21];

Постанова Правління НБУ від 30.11.2020 № 151 "Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України" [22];

Постанова Кабінету Міністрів України № 1295 від 23.12.2020 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" [10];

Постанова Кабінету Міністрів України № 1426 від 29.12.2021 "Про затвердження Положення про організаційно-технічну модель кіберзахисту" [23].

Незважаючи на те, що прийнята у 2017 році Концепція [30] містила цілком зрозумілу й комплексну дорожню карту, її практична реалізація виявилася складною й довготривалою. Прийняті нормативно-правові акти мали вузьку спрямованість, яка визначалася своїм призначенням для окремих секторів КІУ. Так, зокрема, поняття "об'єкт критичної інфраструктури" вперше з'явилося у Законі України "Про основні засади забезпечення кібербезпеки України" [16], однак предмет його регулювання, у значній мірі, є вузькоспеціалізованим, призначеним для визначення базового для зазначеного Закону поняття – "об'єкт критичної інформаційної інфраструктури". Прийняті вище перелічені підзаконні нормативно-правові акти, щодо ідентифікації об'єктів критичної інфраструктури та у банківській сфері стосувалися виключно інформаційно-телекомунікаційних систем та кіберзахисту в окремих сферах життєдіяльності та/або галузях національної економіки України.

Отже, прийняття вищезазначених нормативно-правових документів, визначення в них поняття ОКІ та визначення їх переліку відбулося виключно для потреб національної системи кібербезпеки, а про формування загального правового регулювання системи захисту КІУ в той період не йшлося.

Загалом, у період з 2016 по 2022 рік, заходи щодо забезпечення національної безпеки України були спрямовані насамперед на протидію агресії рф, протидії дезінформації та кібератакам; на зміцнення обороноздатності та розвиток міжнародного співробітництва. Ключовими напрямами у цій сфері були:

реформування сектору безпеки і оборони (продовжена робота щодо реформування Збройних Сил України, зокрема, перехід на стандарти НАТО, впровадження нових процедур закупівель та управління ресурсами);

зміцнення обороноздатності (розвиток військово-промислового комплексу, збільшення фінансування оборонних потреб, модернізація військової техніки та озброєння);

протидія гібридним загрозам (захист інформаційного простору, протидія дезінформації, кібербезпека, захист критичної інфраструктури);

міжнародне співробітництво та посилення міжнародної підтримки (розширення співпраці з країнами-партнерами, зокрема, щодо отримання військової допомоги, обміну досвідом та навчання військовослужбовців);

розвиток громадського сектору (залучення громадських об'єднань та волонтерів до забезпечення національної безпеки, зокрема, у сфері гуманітарної допомоги та підтримки військовослужбовців);

інформаційна безпека (створення системи захисту інформаційного простору, протидія російській пропаганді та дезінформації).

З початком повномасштабного вторгнення рф на територію України процес розбудови національної системи захисту КІУ суттєво прискорився.

В цей період введено в дію головний законодавчий акт, що регламентує зазначену діяльність – Закон України № 1882-IX від 16.11.2021 "Про критичну інфраструктуру" [17]. Слід зауважити, що цей Закон був введений в дію лише 15 червня 2022 року. Він визначає базове правове підґрунтя, зокрема, частиною 1 Статті 2 Закону [17] визначено, що правовою базою у сфері захисту КІУ є Конституція України, цей Закон, інші закони України, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, інші нормативно-правові акти, прийняті на виконання цього Закону.

Закон визначає життєво важливі функції та/або послуги, зокрема до них належать [17, ст. 2]:

урядування та надання найважливіших публічних адміністративних послуг;

енергозабезпечення (у тому числі постачання теплової енергії);

водопостачання та водовідведення;

продовольче забезпечення;

охорона здоров'я;

фармацевтична промисловість;

виготовлення вакцин, стале функціонування біологічних лабораторій;

інформаційні послуги;

електронні комунікації;

фінансові послуги;

транспортне забезпечення;

оборона, держбезпека;

правопорядок, здійснення правосуддя, тримання під вартою;

цивільний захист населення та територій, служби порятунку;

космічна діяльність, космічні технології та послуги;

хімічна промисловість;

дослідницька діяльність.

Законом введено в дію певний понятійно-категорійний апарат у сфері захисту КІУ, який дає визначення ключовим поняттям, зокрема, об'єктам критичної інфраструктури – це підприємства та установи (незалежно від форми власності) таких галузей, як енергетична, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне підприємство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв; дає визначення критичній інфраструктурі – це сукупність об'єктів критичної інфраструктури [17].

Таким чином, з прийняттям зазначеного Закону на законодавчому рівні окреслено організаційну структуру системи захисту КІУ; нормативно визначено механізм формування складу КІУ, що створило правове підґрунтя для належної організації КІУ та її захисту.

Разом з цим, слід зауважити, на деякі неточності. Так, у відповідності до п. 1 Статті 3, Закон [17] регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час. Підкреслюю, у мирний час! В умовах введення правових режимів надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються Законами України "Про правовий режим воєнного стану" [34], "Про правовий режим надзвичайного стану" [19], "Про функціонування єдиної транспортної системи України в особливий період" [30], "Про оборону України" [15].

При цьому слід звернути увагу на певну логічну неузгодженість між різними частинами зазначеної статті [17, ст. 3]. За такого формулювання її першої частини можна зробити висновок, що у

воєнний час, який є антиподом мирного часу, відносини у сфері функціонування та захисту критичної інфраструктури Закон України "Про критичну інфраструктуру" не регулює взагалі. Однак, реалії сьогодення, вказують на те, що об'єктивно це не так. В умовах російсько-української війни, на ОКІ майже щоденно здійснюються ворожі атаки, на що відповідні органи влади належним чином реагують та виконують передбачені Законом [17] повноваження. Зазначене вказує на те, що положення цього Закону продовжують діяти й в умовах воєнного стану, але з деякими уточненнями та коригуваннями, які пов'язані з конкретними загрозами і викликами, рішення по яких приймаються на рівні операторів ОКІ із залученням відповідних суміжників у відповідності до Закону [17]. Комплексний аналіз застосування положень Закону "Про критичну інфраструктуру" в умовах воєнного часу свідчить, що більшість із них за своєю сутністю і змістом є правовим регулюванням функціонування системи захисту КІУ за будь-яких умов. Отже, згадана вище частина друга зазначеної статті [17, ст. 3] має зазначати відповідні законодавчі акти не як такі, що підмінюють собою у період дії того чи іншого правового режиму базовий Закон України "Про критичну інфраструктуру", а як такі, що доповнюють його регулятивний вплив окремими особливостями захисту ОКІ з урахуванням специфіки тих чи інших правових режимів.

Окремим законом також регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки ОКІ [17, ст.3], яка має бути складовою правового регулювання захисту системи КІУ.

Вищезазначене вказує, що з введенням в дію основного закону в сфері захисту КІУ виникли певні розбіжності між раніше напрацьованим правовим масивом нормативно-правових актів у складових КІУ та знов прийнятим Законом. Першопричина, на нашу думку, полягає у тому, що протягом тривалого часу розробка та накопичення нормативно-правових актів відбувалися з порушенням принципу "від загального до особливого", тобто в процесі нескоординованої, іноді не послідовної роботи, у правовому регулюванні виникли певні розбіжності та недосконалості, які потребують виправлення та введення та/або залучення їх до єдиного понятійно-категорійного апарату з метою подальшого єдиного розуміння тотожних понять, як то "об'єкт критичної інфраструктури", "система критичної інфраструктури", "захист критичної інфраструктури" тощо. Свідчення цього містяться у Розділі VI Прикінцеві та перехідні положення. Зокрема, законодавець вимагає внести зміни до певних законодавчих актів, які регламентують діяльність у суміжних сферах.

Наприклад, стосовно одного з найголовніших поняття у цій сфері "об'єкти критичної інфраструктури". Закон дає конкретне визначення – це підприємства та установи (незалежно від форми власності) таких галузей, як енергетична, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне підприємство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Разом з цим, законодавець до різних Законів вносить різні не зовсім тотожні поняття, які за змістом і значенням можливо підпадають під визначення ОКІ. Так, зокрема, законом передбачено:

частину другу статті 17 Кодексу цивільного захисту України (Відомості Верховної Ради України, 2013 р., № 34-35, ст. 458) після пункту 53 доповнити п'ятьма новими пунктами такого змісту, крім іншого:

55) реалізує заходи державної політики у сфері захисту критичної інфраструктури щодо впровадження інженерно-технічних заходів цивільного захисту ***на об'єктах критичної інфраструктури;***

56) бере участь у межах компетенції в оцінці захищеності ***об'єктів критичної інфраструктури;***

57) здійснює заходи щодо постійного та обов'язкового на договірній основі аварійно-рятувального обслуговування суб'єктів господарювання та окремих територій, на яких існує небезпека виникнення надзвичайних ситуацій, віднесених до ***об'єктів критичної інфраструктури,*** аварійно-рятувальними службами, що пройшли атестацію в установленому порядку;

58) у взаємодії з Міністерством внутрішніх справ України, Службою безпеки України забезпечує організацію захисту від терористичних посягань об'єктів аварійно-рятувальних служб, які залучаються і виконують свої функції на ***об'єктах критичної інфраструктури*** в разі виникнення надзвичайних ситуацій;

пункт “б” частини першої статті 38 Закону України “Про місцеве самоврядування в Україні” (Відомості Верховної Ради України, 1997 р., № 24, ст. 170 із наступними змінами) доповнити підпунктом 2^{-1} такого змісту:

2^{-1}) вжиття необхідних заходів щодо захисту критичної інфраструктури, відновлення функціонування ***важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення***, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи припиненням здійснення життєво важливих функцій, взаємодія між суб’єктами національної системи захисту критичної інфраструктури з урахуванням вимог Закону України “Про критичну інфраструктуру;

статтю 25 Закону України “Про місцеві державні адміністрації” (Відомості Верховної Ради України, 1999 р., № 20-21, ст. 190 із наступними змінами) доповнити пунктом 24 такого змісту:

“24) забезпечує захист критичної інфраструктури, ***відновлення функціонування важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення,*** підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій, взаємодію між суб’єктами національної системи захисту критичної інфраструктури”;

у пункті 3 статті 16 Закону України “Про правовий режим надзвичайного стану” (Відомості Верховної Ради України, 2000 р., № 23, ст. 176; 2013 р., № 15, ст. 99; 2014 р., № 12, ст. 178) слова “*об’єктів, що забезпечують життєдіяльність населення та народного господарства*” замінити словами “***важливих об’єктів національної економіки та об’єктів критичної інфраструктури”***;

у Законі України “Про Збройні Сили України” (Відомості Верховної Ради України, 2000 р., № 48, ст. 410 із наступними змінами):

у статті 1:

частину четверту після слів “до здійснення заходів правового режиму воєнного і надзвичайного стану” доповнити словами “безпеки та захисту критичної інфраструктури”, а після слів “ліквідації надзвичайних ситуацій природного і техногенного характеру” – словами “кризових ситуацій”;

після частини четвертої доповнити новою частиною такого змісту:

“Збройні Сили України у сфері захисту критичної інфраструктури забезпечують організацію захисту ***військових об’єктів критичної інфраструктури*** Збройних Сил України від терористичних загроз, підготовку до застосування військ (сил) Збройних Сил України у разі вчинення терористичного акту в повітряному просторі або територіальному морі України, проведення заходів з підвищення рівня захищеності, усунення ризиків і загроз вибухопожежобезпеки арсеналів, баз та складів Збройних Сил України, виконання завдань з протиповітряного прикриття ***важливих об’єктів держави*** (критичної інфраструктури), перелік яких визначається Кабінетом Міністрів України”.

у Законі України “Про оборону України” (Відомості Верховної Ради України, 2000 р., № 49, ст. 420 із наступними змінами):

у статті 3:

абзац десятий після слів “єдиної державної системи цивільного захисту” доповнити словами “***об’єктів критичної інфраструктури***”;

абзац тринадцятий після слів “підготовку національної економіки” доповнити словами “***об’єктів критичної інфраструктури***”;

в абзаці сьомому статті 9 слова “живучості об’єктів національної економіки та державного управління” замінити словами “живучості ***важливих об’єктів національної економіки, об’єктів критичної інфраструктури та державного управління***”;

в абзаці третьому частини першої статті 13 слова “інших об’єктів інфраструктури” замінити словами “***інших об’єктів критичної інфраструктури***”.

У Законі України “Про правовий режим воєнного стану” (Відомості Верховної Ради України, 2015 р., № 28, ст. 250; 2021 р., № 41, ст. 339):

частину першу, абзаци перший і другий частини сьомої, друге речення частини восьмої статті 4 після слів “громадської безпеки і порядку” доповнити словами “захисту критичної інфраструктури”;

у частині першій статті 8:

у пункті 1 слова “об’єктів державного значення, об’єктів державного значення національної транспортної системи України” замінити словами ***“об’єктів критичної інфраструктури”;***

у пункті 2 слова “та сфері забезпечення життєдіяльності населення” і “та системи забезпечення життєдіяльності населення” замінити словами ***“та захисту критичної інфраструктури”;***

пункт 9 після слів “посягання на” доповнити словами ***“стійкість критичної інфраструктури”;***

у статті 15:

частину першу після слів “Про мобілізаційну підготовку та мобілізацію” доповнити словами “Про критичну інфраструктуру”;

у пункті 25 частини другої слова “важливих об’єктів національної економіки” замінити словами “об’єктів критичної інфраструктури”;

у пункті 7 частини третьої слова “важливих об’єктів національної економіки” замінити словами “об’єктів критичної інфраструктури”;

у частині першій статті 23 Закону України “Про Національну поліцію” (Відомості Верховної Ради України, 2015 р., № 40-41, ст. 379 із наступними змінами):

пункт 20 доповнити словами “а також ***об’єктів критичної інфраструктури,*** перелік яких визначається Кабінетом Міністрів України”.

Таким чином, у нормативно-правових актах продовжують мати місце використання різних термінів, щодо ОКІ, а саме: “***важливі державні об’єкти національної економіки, об’єкт критичної інфраструктури та об’єкти, які забезпечують життєдіяльність населення”,*** “***військові об’єкти критичної інфраструктури”,*** “***важливі об’єкти національної економіки та об’єкти критичної інфраструктури”***; “***об’єкти критичної інфраструктур”.*** Отже, якщо ті чи інші об’єкти галузей національної економіки та/або секторів системи захисту критичної інфраструктури відповідають критеріям, яке встановлено відповідним визначенням “об’єкт критичної інфраструктури” у Законі України “Про критичну інфраструктуру” [17], то це об’єкт критичної інфраструктури (ОКІ). Про це конкретно має бути зазначено у текстових частинах інших нормативно-правових актів, в частинах, які стосуються виконання заходів із захисту системи КІУ.

Такі неточності, скоріш за все вказують, на те що зміни до вищезазначених нормативно-правових актів готувалися представниками різних відповідних відомств, які є суб’єктами системи захисту КІУ без належної координації дій. Що є ознакою необхідності створення окремого уповноваженого органу влади з відповідними функціями.

До речі, це важливе у організаційному сенсі, питання стосовно уповноваженого органу у сфері захисту КІУ вирішено законодавцем лише на тимчасовій основі, а остаточне його унормування відтерміновано на повоєнний період.

Також з припиненням дії воєнного стану пов’язується й перехід до повноцінного функціонування у штатному режимі реєстру ОКІ. На мою думку, зволікання з визначенням уповноваженого органу, на який покладається здійснення функціонального управління системою захисту КІУ створює певні проблеми у координації дій усіх суб’єктів цієї системи. Так, у статті 16 Закону України “Про критичну інфраструктуру” [17, ст. 16] не конкретизовано статус цього органу, а лише в загальних рисах окреслено його компетенцію (частина друга передбачає, що безпосередньо визначити уповноважений орган у сфері захисту критичної інфраструктури та затвердити положення про нього належало Кабінету Міністрів України), що він і зробив своєю постановою від 12 липня 2022 року № 787. Згідно зазначеного урядового нормативно-правового документу мала б бути утворена Державна служба захисту КІ та забезпечення національної системи стійкості України (далі – ДЗКІ) як центральний орган виконавчої влади зі спеціальним статусом. Однак, набрання чинності зазначеного документу було відкладено до прийняття законодавчих змін, щодо бюджетного фінансування. Як видно із назви ДЗКІ, вона мала б стати державною інституцією, котра поєднувала б компетенцію одночасно в двох національних системах: системі забезпечення національної стійкості та системі захисту КІУ. Зрештою вищезазначена урядова постанова не набрала чинності й фактичного утворення нової державної інституції не відбулося.

У жовтні 2022 року було внесені чергові зміни до Закону України “Про критичну інфраструктуру”, згідно з п. 5-1 його прикінцевих і перехідних положень під час дії воєнного стану, а також протягом дванадцяти місяців після його припинення чи скасування, повноваження уповноваженого органу у сфері захисту критичної інфраструктури України мають здійснюватися Державною службою спеціального зв’язку та захисту інформації України (Держспецзв’язку). Безумовно

важко переоцінити результати діяльності Держспецзв'язку щодо розбудови нормативно-правової бази та вжитих заходів для забезпечення захисту інформаційних об'єктів від кібератак тощо. Однак, нами вбачається, уповноважений орган має консолідувати діяльність усіх суб'єктів системи захисту КІУ та координувати їх діяльність не лише на захисті інформаційно-телекомунікаційних систем, а і не менш важливих потенційних загрозах (техногенного, природного характеру та/або звичайного фізичного вторгнення).

З точки зору економії коштів в умовах воєнного часу, створення окремого уповноваженого державного органу начебто не на часі. Але можливо саме через нові загрози для ОКІ, що виникли внаслідок воєнних дій, саме зараз це актуально. Скоріш за все не лише матеріальний аспект став визначальним у прийнятті такого рішення. Щоб новий орган влади розпочав свою діяльність необхідні не лише кошти для обладнання приміщень, робочих місць та утримання персоналу. Насамперед, потрібен навчений персонал, на підготовку якого теж потрібен час, якого за цих умов не має.

Крім того, разом із тимчасовим покладанням додаткових функцій на службу Держспецзв'язку, Закон України "Про критичну інфраструктуру" передбачає, що протягом дванадцяти місяців після припинення чи скасування в нашій державі воєнного стану Кабінету Міністрів України належить визначити уповноважений орган у сфері захисту критичної інфраструктури [17, ст. 5-2]. При буквальному розумінні змісту тексту на думку приходить декілька висновків щодо створення нового державного органу у сфері захисту системи КІУ:

по-перше, питання його створення з порядку денного знімається взагалі;

по-друге, припинення дії воєнного стану передбачається визначення уповноваженого органу, тобто з числа вже існуючих державних органів;

по-третє, уповноваженим органом необов'язково має залишиться тимчасово визначена у цьому статусі служба Держспецзв'язку, хоч така можливість і не виключається.

Вбачається, що вирішальним чинником майбутнього вибору має стати об'єктивне співставлення компетенції кожного із суб'єктів національної системи захисту КІУ з передбаченими Законом України "Про критичну інфраструктуру" функціями уповноваженого органу. Враховуючи, що право вибору майбутнього уповноваженого органу влади у цій сфері законодавець покладає саме на Кабінет Міністрів України, чим обмежує цей вибір лише підпорядкованими йому державними інституціями. Як наслідок – апріорі не розглядаються інші суб'єкти державного механізму. Отже, у повоєнний період до питання щодо уповноваженого органу з питань захисту КІУ слід повернутися на законодавчому рівні.

Також важливою складовою правового регулювання системи захисту КІУ, крім визначення її організаційно-функціональної структури, суб'єктів цієї системи та їх повноважень, є нормативно-правове забезпечення відповідальності за правопорушення чинного законодавства в сфері, що досліджується. Загалом, умовно правову регламентацію захисту КІУ складають три основні взаємопов'язані компоненти:

перший – нормативне визначення критичної інфраструктури як такої, формування її складових (секторів та під секторів) і створення реєстру (переліку) об'єктів, які підлягають захисту;

другий – впорядкування організаційного механізму системи захисту КІУ та встановлення повноважень суб'єктів системи захисту КІУ;

третій – правова відповідальність за порушення норм чинного законодавства у цій сфері.

У [17] питання відповідальності за порушення законодавства у сфері захисту КІУ відображено лише у форматі максимально абстрактної відсильної норми [17, ст. 29]. Зважаючи на це, законодавець зобов'язав уповноважений орган у сфері захисту КІУ протягом року з моменту початку його діяльності, а отже знов на повоєнний період, підготувати відповідні зміни (пункт 11 прикінцевих та перехідних положень Закону).

Разом з цим, слід зауважити, що окремі важливі аспекти залишилися поза увагою законодавця та/або відкладені на післявоєний період. Так, зокрема, у частині другій ст. 259 Кримінального кодексу України вживається термін "критично важливі об'єкти інфраструктури", задля тлумачення змісту якого примітка зазначеної статті відсилає до Закону України "Про основні засади забезпечення кібербезпеки України", з якого цей термін наразі вже вилучено. Таким чином, при практичному застосуванні згаданої вище норми частини другої ст. 259 Кримінального кодексу України доведеться спочатку обґрунтовувати ідентичність термінів "критично важливий об'єкт інфраструктури" й "об'єкт критичної інфраструктури", що потребуватиме застосування юридич-

но небездоганного прийому – посилання на вже виключену норму п. 16 частини першої статті 1 Закону України "Про основні засади забезпечення кібербезпеки України".

Стосовно імплементації положень Закону "Про критичну інфраструктуру" [17] до секторальних нормативно-правових актів системи захисту КІУ, зазначена робота триває та потребує всеосяжного контролю з боку уповноваженого органу. Наприклад, у Положенні про визначення об'єктів критичної інфраструктури в банківській системі України, затвердженому згаданою постановою Правління Національного Банку України, й досі зазначено, що його розроблено відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" з метою врегулювання питань кіберзахисту в банківській системі України, хоч на тепер сфера його застосування є насправді значно ширшою.

Окремо слід розглянути перспективи застосування штучного інтелекту, продуктом використання якого можуть бути як засоби захисту КІУ так і загрози її сталого функціонування. Основними концептуальними загрозами, що викликані впровадженням елементів ШІ, для функціонування КІУ, можуть бути [39]:

порушення конфіденційності, що викликане здатністю мовних моделей ШІ виділяти та узагальнювати інформацію, якою володіють посадові особи, в тому числі через соціальні мережі та дистанційне управління мобільними пристроями;

розповсюдження фейкової інформації, спрямованої на визначені групи, з метою дезінформації та саботування виконання критичних задач;

посилення кіберзагроз через створення удосконалених вірусів, автоматизація цих процесів з метою "зламу" систем захисту ОКІ;

заміщення фізичних процесів, що потребують управлінських рішень кваліфікованого спеціаліста машинами під управлінням ШІ, може призвести до порушення через можливу упередженість внаслідок вибіркового навчання програм ШІ;

можлива втрата контролю над дистанційно керованими комплексами захисту ОКІ.

Крім іншого, слід зауважити, що діяльність суб'єктів системи захисту КІУ в останній час значно пожвавилася. Спостерігається поступове розширення реєстру (переліку) секторів і ОКІ. Як відомо, ідея впровадження самого поняття "критична інфраструктура" концептуально полягає у тому, щоб виокремити найбільш життєво важливі для нормального функціонування держави та суспільства об'єкти й сфокусувати на їх захисті основні зусилля, а також ресурсне забезпечення. При цьому за основу береться той незаперечний факт, що навіть у найбільш економічно розвинених країнах світу, ресурси, що можуть бути спрямовані на убезпечення ОКІ від впливу загроз їх стабільній діяльності, є завжди тією чи іншою мірою обмеженими.

Викладене дає підстави для низки **висновків**.

Захист системи КІУ ґрунтується на положеннях Конституції України, Закону України "Про критичну інфраструктуру", міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, інших нормативно-правових актах, що прийняті на виконання вищезазначеного Закону.

Ретроспективний аналіз процесу становлення системи захисту КІУ засвідчує його певну специфічність, яка полягає насамперед, у непослідовному формуванні правової регламентації у різних секторах КІУ. Через порушення послідовності дій суб'єктів та основний принцип "від загального до окремого (до складових)" під час формування в Україні національного законодавства про критичну інфраструктуру основний Закону, що регулює діяльність у сфері захисту критичної інфраструктури має певні розбіжності між положеннями, які містяться в ньому; неточностями у визначеннях і поняттях, які були сформовані раніше у певних нормативно-правових документах в галузях і секторах, які є відповідними складовими КІУ та мають бути частиною правового регулювання, зокрема, у сфері кібербезпеки та не нести в собі протиріч і непорозумінь.

Процес формування виваженого правового регулювання системи захисту КІУ триває. Закон "Про критичну інфраструктуру" є, але деякі його положення потребують коригування з урахуванням досвіду застосування норм і положень вже діючих у правовому полі нормативно-правових актів; доопрацювання і уточнень, внесення змін і доповнень в діючі нормативно-правові акти з метою приведення їх у відповідність до цього Закону.

Перспективи. Загалом проблематика, що пов'язана із системою КІУ та її захистом, потребує відповідного переосмислення з урахуванням досвіду та уроків воєнного часу, з урахуванням реальних загроз і потреб ОКІ та/або галузей і секторів КІУ.

Подальші наукові розробки можуть бути спрямовані на визначення ступеню відповідності правового регулювання системи захисту КІУ міжнародному праву, а також оптимізації національної системи захисту КІУ у контексті досягнення її максимальної сумісності та придатності до ефективної взаємодії з відповідними європейськими організаційно-правовими механізмами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бірюков Д.С. Державно-приватне партнерство у сфері попередження та реагування на надзвичайні ситуації. Стратегічні пріоритети. 2014. № 1 (30). С. 164–168.
2. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ: НІСД, 2012. 57 с.
3. Зелена книга з питань захисту критичної інфраструктури в Україні / Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. К.: Національний інститут стратегічних досліджень, 2015. 35 с.
4. Богдан Б.В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/4_2023/2.pdf (дата звернення 06.07.2025)
5. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: Аналітична доповідь. К.: "Фенікс", 2012. 92 с.
6. Бобро Д.Г. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Бобро Д.Г. та ін.; за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 223 с.
7. Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі,* 2014. № 806. С. 34–39: веб-сайт. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8 (дата звернення 12.06.2025).
8. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 943.
9. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. Офіційний Вісник України. 2020. № 93 від 27.11.2020.
10. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (дата звернення: 27.06.2025).
11. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. *Інформаційна безпека людини, суспільства, держави*. 2019. № 2 (26). С. 40–49.
12. Іванов Ю.А. Правова основа розбудови в Україні національної системи захисту критичної інфраструктури *International Scientific Journal Internauka. Series: Juridical Sciences*. URL: https://doi.org/10.25313/2520-2308-2024-1 (дата звернення: 14.06.2025).
13. Конституція України. Верховна Рада України від 28.06.1996 № 254к/96-ВР. Редакція від 01.01.2020 р.
14. Про Національну гвардію України: Закон України від 27.06.2024.
15. Про оборону України: Закон України від 06.12.1991р. № 1932-XII.
16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII.
17. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX.
18. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII.
19. Про правовий режим надзвичайного стану Закон України від 16.03.2000 р. № 1550-III.
20. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.2022 р. № 2684-IX.
21. Про затвердження порядку проведення огляду стану кіберзахисту критичної інфраструктури, державних інформаційних ресурсів та інформації, вимоги щодо захисту якої встановлені законом: Постанова Кабінету Міністрів України від 11.11.2020 р. № 1176.

22. Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України: Постанова Правління НБУ від 30.11.2020 р. № 151.
23. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426.
24. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.2022 р. № 821.
25. Про затвердження порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.2023 р. № 415.
26. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10.2022 р. № 1174.
27. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 612.2017 р. № 1009-р.
28. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 23.08.2016 р. № 563.
29. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 519.
30. Про функціонування єдиної транспортної системи України в особливий період: Закон України від 20.10.1998 р. № 194-XIV (зі змінами).
31. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури: Указ Президента України від 13.02.2017 р. № 32/2017 "Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації".
32. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27.01.2016 р.
33. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішенні РНБО України від 01.03.2014 р.
34. Пядишев В.Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Теоретичні та практичні аспекти забезпечення національної безпеки,* № 4 2022, с. 229–234.
35. Солопова І.В. Правові умови захисту об'єктів критичної інфраструктури в Україні: проблеми та перспективи. *Південно-український правничий часопис / Правове забезпечення адміністративної реформи,* № 2. 2021, с. 119–125. УДК 351.81. DOI: https://doi.org/10.32850/sulj.2021.2.20.
36. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62–76.
37. Суходоля О.М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. *Науковий часопис*, 2017. Вип. 1-2 (13-14). С. 50–80.
38. Developing The Critical Infrastructure Protection System in Ukraine: monograph / S. Kondratov, D. Bobro, V. Horbulin et al.; general editor O. Sukhodolia. Kyiv: NISS, 2017. 184 p.
39. Богом'я В.І., Гудзь А.С., Штучний інтелект: сучасний стан і перспективи застосування. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, Україна, 46 (1), с. 13–17. https://doi.org/10.33099/2311-7249/2023-46-1-13-17.