УДК 32.019.51:323.28:323

ГОРДІЄНКО С.Г., *доктор юридичних наук, доцент*, професор кафедри безпеки та правоохоронної діяльності юридичного факультету Західноукраїнського національного університету.
ORCID: https://orcid.org/0000-0003-0392-2601.
ДОРОНІН І.М., *доктор юридичних наук, доцент*, завідувач наукової лабораторії права національної та міжнародної безпеки ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-5991-6713.

ІНФОРМАЦІЙНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

DOI…

Анотація. *Стаття присвячена проблематиці правової регламентації захисту критичної інфраструктури. Проаналізовано розвиток термінологічної основи критичної інфраструктури. Визначено, що правове забезпечення захисту критичної інфраструктури має позитивні моменти, водночас зазнає впливу від проблем у державному управлінні. Реалізація приписів законодавчого акту на рівні підзаконних актів відбувається доволі повільно. Інформаційно-правові аспекти захисту критичної інфраструктури визначають наявність проблемного поля. Проблеми правового регулювання зумовлені складним характером інформаційної інфраструктури, що зумовлює складнощі у правовому регулюванні. Іншим важливим аспектом є пошук балансу між захистом інформації про критичну інфраструктуру та державною політикою "відкритих даних". Це ж саме зумовлює і складнощі для політики прозорості і підзвітності у державному управлінні. Зазначені проблеми обумовлюють негативний вплив на правову регламентацію. Пошук шляхів їх вирішення є важливим завданням для правотворчості та правової науки.*

Ключові слова: *правове регулювання, критична інфраструктура, захист критичної інфраструктури, інформаційна інфраструктура, інформація, інформаційне право, доступ до інформації, відкриті дані.*

Summary. *This paper is committed to the problems of legal regulation of critical infrastructure protection. It has been determined that the legal provision of protection of critical infrastructure has positive aspects, but at the same time it is affected by problems in public administration. The implementation of the provisions of the legislative act at the level of by-laws is rather slow. Informational and legal aspects of critical infrastructure protection determine the presence of a problem fields. The problems of legal regulation are caused by the complex nature of the information infrastructure, which causes difficulties in legal regulation. Another important aspect is finding a balance between the protection of critical infrastructure information and the government's "open data" policy. This also causes difficulties for the policy of transparency and accountability in public administration. The specified problems cause a negative impact on legal regulation. Finding ways to solve this problem is an important task for law-making and legal science.*

Keywords: *legal regulation, critical infrastructure, critical infrastructure protection, information infrastructure, information law, open data, access to the information.*

Постановка проблеми. Агресія проти нашої держави, ескалація бойових дій та ураження об'єктів економіки і промислового потенціалу України безумовно свідчить про важливість вжиття усіх необхідних заходів щодо захисту відповідних об'єктів. Визначення на рівні термінології поняття "критичної інфраструктури" та нормативно-правове регулювання її статусу, а також відповідного кола суспільних відносин,

пов’язаних із захистом та забезпеченням належного функціонування, що відбулось при ухваленні актів законодавства, вирішивши з одного боку вирішило нагальні проблеми концептуалізації поняття, з іншого – окреслило коло відповідних викликів, що з’явились у ході правозастосування. Розгляд правових аспектів захисту та функціонування критичної інфраструктури у сучасних умовах потребує комплексного підходу, а не лише відповідного огляду та технічного регулювання адміністрування у цій сфері. Тобто проблема не обмежується суто адміністративно-правовим її характером.

Зазначене викликає необхідність у розгляді інших правових аспектів функціонування та захисту критичної інфраструктури у першу чергу з точки зору інформаційного права, що особливо актуально у період розвитку інформаційного суспільства.

Результати аналізу наукових публікацій. У правовій науці проблематика критичної інфраструктури розглядається лише останнім часом і в основному через призму адміністративного права. Саме під таким кутом ця проблематика розглядалась у працях низки науковців, аналіз праць яких проведено в основній частині статті, також слід окремо згадати докторську дисертацію С.С. Теленика, захищену у 2021 році щодо адміністративно-правових аспектів захисту критичної інфраструктури, яка є найбільш ґрунтовним дослідженням з цієї проблематики.

В інформаційному праві увага науковців в основному зосереджувалась навколо окремих дотичних проблем, насамперед щодо функціонування інформаційних ресурсів та правових аспектів функціонування інформаційної системи та її складових у сучасних умовах.

Мета статті полягає у визначенні інформаційно-правового аспекту захисту критичної інфраструктури України врахування викликів та загроз сьогодення, що зумовлене пошуком шляхів вдосконалення чинного законодавства.

Виклад основного матеріалу. На рівні визначення відповідної термінології ужиття терміну “критична інфраструктура” є запозиченням з англомовної термінології, що має міжнародний характер. При цьому саме ужиття терміну з 1990-х років зумовлено необхідністю виокремлення конкретного кола об’єктів для організації системи заходів із забезпечення їхнього функціонування та різного роду захисту в екстраординарних умовах. Потреба у захисті обумовлювалась терористичними загрозами після 2021 року та необхідністю вирішення супутніх проблем. Тому, наприклад, у Директиві Європейського Союзу 2008/114/ЄС від 8 грудня 2008 року зазначено, що “критичну інфраструктуру” слід розуміти як актив (економічний), систему або їхню частину, що розташовані у державах-членах ЄС, які важливі для підтримки життєво необхідних функцій, здоров’я, захисту, безпеки, економічного чи соціального благополуччя людей, порушення чи знищення яких могло б здійснити суттєвий вплив на державу-члена ЄС внаслідок нездатності підтримувати такі функції [1]. У даному випадку термін “актив” трактується в економічному значенні, тобто як будь-який предмет (річ, будівля, комплекс і т. п.), що обліковується в бухгалтерському обліку та має визначену вартість, тобто присутнє широке термінологічне трактування. Слід зазначити, що за час доволі тривалого застосування зазначеної директиви в ЄС було вибудовано відповідну систему захисту в межах Європейської програми захисту критичної інфраструктури (European Programme For Critical Infrastructure Protection (EPCIP). Її виконання підкреслило низку нових проблем, у т.ч. і термінологічного характеру, внаслідок чого Єврокомісією проводились заходи удосконалення чинного законодавства у сфері захисту критичної інфраструктури відповідно до потреб часу. Відповідно до цілей та завдань законодавчого регулювання мова йшла насамперед про уточнення переліку об’єктів, у

першу чергу стосовно інформаційної інфраструктури, мереж, транспортної системи та об'єктів у відкритому космосі (зокрема супутникового зв'язку). Водночас широке трактування об'єктів захисту як економічного активу цілком надає змогу розповсюдити дефініцію і на перелічені об'єкти.

В Україні до проблеми захисту критичної інфраструктури як з точки зору організації, так і правового її забезпечення звернулись дещо пізніше, до того ж із самого початку не було згоди стосовно термінології внаслідок іншого сприйняття, у т. ч. щодо відмови від вжиття терміну "критична інфраструктура" взагалі, оскільки воно є калькуванням англомовної термінології. При цьому термінологія нормативно-правових актів від самого початку відповідала правничій термінології інших держав, хоча вживались одночасно і терміни "критично важлива інфраструктура" та подібні. Але після 2014 року можливо стверджувати про сприйняття терміну "критична інфраструктура" у вітчизняному законодавстві, що зумовлено потребами в уніфікації законодавства і, відповідно, термінологічного узгодження. Прагматична потреба у визначенні заходів із забезпечення функціонування та захисту критичної інфраструктури може бути проілюстрована вимогами Закону України "Про національну безпеку України" від 21.06.18 р. № 2469-VIII, оскільки законодавчий акт у сфері національної безпеки, що діяв раніше, у всіх редакціях такої термінології не містив. Так, частина 4 статті 3 Закону України "Про національну безпеку України", яка визначає принципи державної політики у сферах національної безпеки і оборони, серед цілей цієї державної політики вказує і "забезпечення безпеки критичної інфраструктури" [2]. Крім цього, термін згадується у цьому законодавчому акті і при визначенні відповідного кола завдань для суб'єктів сектору безпеки і оборони (п. 3 ч. 1 ст. 19; ч. 1 ст. 22, ч. 1 і 3 ст. 27). На рівні підзаконних актів термінологія вживалась у першу чергу у технологічному значенні, наприклад щодо організації кібербезпеки та кіберзахисту відповідних об'єктів [3].

В аналітичних оглядах та науковій літературі можливо визначити наступні основні підходи до оперування терміном "критична інфраструктура" та відповідних його варіантів. Так, в одній з перших аналітичних доповідей з цієї проблематики, підготовленій фахівцями Національного інституту стратегічних досліджень у 2012 році, констатується очевидна відсутність усталеної та ухваленої дефініції терміну і визначається, що під критичною інфраструктурою можливо розглядати "енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства і підприємства військово-промислового комплексу, а також центральні органи влади" [4, с. 4].

У той же час науковцями запропоновано розглядати термін і на іншому рівні наукового абстрагування, наприклад як "множинність розташованих в межах території країни функціонально пов'язаних елементів національної інфраструктури чи їх частини у вигляді фізичних, організаційних інформаційно-комунікаційних структур (незалежно від форми власності), технологій, активів, засобів, систем, мереж, поставок, процесів та фахівців які ними управляють, які є вирішальними для забезпечення державою життєво важливих для суспільства функцій (здоров'я, захищеності, соціально-економічного благополуччя громадян, забезпечення суверенітету та сталого розвитку країни) порушення функціонування, знищення, збій або дисфункція у роботі яких матиме критичний вплив на здатність влади забезпечувати вказані функції та може спричинити виникнення людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків та призведе до суттєвого порушення національної безпеки й

оборони" [5, с. 79]. В інших випадках підтримується розуміння критичної інфраструктури як сукупності "активів" чи об'єктів, відповідних систем та їх зв'язків [6; 7].

Слід порівняти зазначені підходи і з поглядами вчених у галузі інформаційного права стосовно інформаційних систем та відповідної інфраструктури. Так, О.А. Баранов під "інформаційною інфраструктурою" запропонував розуміти "сукупність систем: виробництва інформації та інформаційних послуг; поширення інформації та інформаційних продуктів; виробництва засобів виробництва інформації та інформаційних технологій; накопичення та зберігання інформації; сервісного обслуговування інформаційних засобів і технологій; підготовки кадрів; забезпечення інформаційної безпеки" [8, с. 47]. У такому разі ця сукупність систем зумовлює і розгляд всіх її складових як певної сукупності об'єктів. Тобто "поняття інформаційної інфраструктури охоплює "значну кількість суб'єктів із самих різних сегментів інформаційної діяльності, спрямованої як на формування власне обороту інформації, так і на забезпечення цього обороту" [8, с. 54].

Дещо інше визначення для інформаційної інфраструктури запропонував О.Д. Довгань, зокрема "поняття інформаційної інфраструктури визначається як сукупність програмно-технічних засобів, інформаційних комунікацій, інших механізмів управління інформаційними ресурсами, напрацьованих суспільною практикою, організаційних систем збереження і використання наявних обсягів інформації, а також інститутів продукування нової інформації в інтересах суспільного розвитку, засобів нормативно-правового забезпечення інформаційної діяльності, захисту вітчизняних інформаційних ресурсів від усіх видів загроз та негативних впливів" [9, с. 18]. Тобто у даному випадку мова йде про доволі широке коло об'єктів, що цілком можуть бути визначені як "активи" відповідно до Директиви 2008/114/ЄС.

У спеціально присвяченому адміністративно-правовій регламентації захисту критичної інфраструктури дослідженні С.С. Теленика запропоновано розглядати критичну інфраструктуру як "системний комплекс стратегічно важливих матеріальних та нематеріальних об'єктів виробничої, невиробничої, соціальної сфери, а також окремі складники цього комплексу (в тому числі ресурси), метою яких є забезпечення його повноцінного життєвого циклу, безпека, охорона здоров'я, добробут людини, сталий розвиток суспільства й економіки держави, підтримання її суверенітету з огляду на те, що зловмисне втручання у функціонування, а також пошкодження, руйнація або виведення з ладу таких об'єктів внаслідок диверсій, техногенних чи природних катастроф може призвести до тяжких наслідків" [10, с. 29-30]. Така дефініція зумовлена розширеним розглядом визначення терміну відповідно до Директиви 2008/114/ЄС і видається доволі широкою, що містить деякі загальні поняття, які навряд чи можуть бути однозначно визначені тим більше у нормативно-правових актах.

Як вже зазначалось вище, реалізація EPCIP зумовила для регуляторів ЄС пошук нових шляхів як щодо організації захисту, так і щодо правової регламентації захисту об'єктів. Зокрема, ґрунтуючись на широкому розуміння терміну "критична інфраструктура" та погоджуючись із закладеним у Директиві 2008/114/ЄС загальним підходом до властивостей, що характеризують об'єкт критичної інфраструктури, запропоновано розглядати діяльність із захисту критичної інфраструктури як діяльність, що складається із ідентифікації та визначення об'єкту, його реєстрації та організації захисту на плановій основі [11].

Саме така схема закладена і у чинне вітчизняне законодавство. Зокрема, Закон України "Про критичну інфраструктуру" від 16.11.21 р. № 1882-IX передбачає відповідний процес віднесення об'єктів до критичної інфраструктури із визначенням

відповідності певним критеріям, категоризацію об’єктів та внесення до відповідних реєстрів [12]. Оскільки у визначеннях термінів “критичну інфраструктуру” можливо розглядати через термін “об’єкти критичної інфраструктури”, варто визначити, що до них віднесено “об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам” [12].

При розгляді інформаційно-правових проблем, що виникають при захисті критичної інфраструктури, можливо відразу розподілити їх на наступні групи. По-перше, мова йде про складнощі із належністю окремих складових інфраструктури саме до об’єктів критичної інфраструктури. Так, до інформаційної інфраструктури можливо віднесення так званих “віртуальних” об’єктів, а також комплексних об’єктів, що існують лише як система [13; 14, с. 10; 15, с. 97-99]. Існуючий порядок віднесення об’єктів до критичної інфраструктури навряд чи дозволяє зробити висновок про належне правове регулювання цього процесу в існуючій правовій реальності. Водночас, саме атака на віртуальні об’єкти інформаційної інфраструктури завдає значної шкоди [16].

Другим проблемним колом варто вважати співвідношення заходів інформаційної, кібернетичної безпеки із заходами фізичного захисту щодо певних об’єктів критичної інфраструктури. Оскільки проблема кібератак на такі об’єкти технічно цілком зрозуміла і потребує у першу чергу застосування відповідних технічних заходів з протидії більш складним є питання захисту від інформаційних атак, оскільки маніпулювання інформацією, розголошення та розповсюдження чутливої для об’єктів інформації також може завдавати шкоди. Оскільки ця проблема пов’язана із законодавчими прогалинами щодо визначення категорій захисту інформації відповідно до вимог Закону України “Про інформацію”, шляхи її вирішення також мають полягати у царині законодавчого регулювання. Мова у такому разі насамперед йде про обмеження доступу та уникнення недоцільного та невиправданого розповсюдження інформації. Стаття 21 чинного Закону України “Про інформацію” визначає, що інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [17]. Але враховуючи численні виключення стосовно можливості віднесення інформації до числа інформації з обмеженим доступом, що визначено у ч. 4 ст. 21 цього ж Закону, особливо з урахуванням наступних змін і доповнень, а також відсутність законодавчого регулювання використання службової інформації, як інформації з обмеженим доступом, наразі можливо стверджувати лише про належну регламентацію захисту інформації, що становить державну таємницю. І оскільки “державною таємницею” є “вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України” [18] інформація щодо об’єктів критичної інфраструктури цілком може бути визнана державною таємницею у встановленому цим Законом порядку. Водночас, існує певна неузгодженість та дисбаланс між приписами законодавчих актів стосовно охорони інформації з обмеженим доступом із політикою “відкритих даних”, що проводиться в державі останнім часом.

Сутність концепції політики “відкритих даних” полягає у наступному. Розпорядники інформації (як правило, державні органи та юридичні особи, що їм підпорядковані) мають своїм обов’язком оприлюднювати публічно практично усю інформацію про свою діяльність у тому числі у вигляді, що дозволяє отримувати її у будь-якому обсязі вільно, безоплатно та без ідентифікації отримувача з можливістю її будь-якої автоматичної обробки. Оскільки така політика передбачає повний доступ до всіх державних реєстрів за виключенням інформації, що містить персональні дані,

службову інформацію або становить державну таємницю, виник ринок послуг щодо збору та аналітичної обробки з наданням за запитом практично будь-якої інформації щодо об'єкту критичної інфраструктури. При цьому сама по собі аналітична обробка великих масивів інформації у різних сферах є потенційно небезпечною для певних сфер з точки зору національної безпеки, діяльність агрегаторів інформації з державних реєстрів має передумови для виникнення загроз, але спроби державного регулювання їхньої діяльності через низку перепон політичного характеру та критики окремих громадських інституцій успіху не мали.

Після ескалації російської агресії проти України у лютому 2022 році питання захисту інформації щодо об'єктів критичної інфраструктури набуло особливої ваги. Звісно, що традиційні заходи з обмеження інформації шляхом її віднесення до різних видів інформації з обмеженим доступом, вирішило проблему далеко не повністю, особливо у питаннях забезпечення прозорості державних закупівель та аналітики за даними державних реєстрів. Окремі пропозиції щодо введення поняття "чутливості" як характеристики інформації і уведення нової категорії "чутливої інформації" (або "критичної інформації" чи подібних видів) [19] не вирішить проблему з огляду на наступне. Сам по собі термін "чутлива інформація" є буквальним перекладом терміну *Sensitive Information*, що вживався в політичній дискусії та засобах масової інформації США у випадках, коли державні органі чи політичні діячі не розголошували, приховували або ж навпаки розголошували з політичною метою інформацію, що не мала обмежень доступу, не становила державної таємниці, але могла бути використана з метою завдання шкоди чиїмось інтересам, насамперед мова йшла про репутаційну та політичну шкоду. У тих випадках, що стосувались саме терміну "чутливості", мова йшла про, як правило, про зовнішньополітичні контакти, що не мали публічного характеру, дипломатичні домовленості, які не оприлюднювались, при цьому чіткого критерію такої чутливості ніколи не було. Іноді як "чутлива інформація" розглядались кулуарні політичні домовленості, особисті повідомлення політиків тощо. Більш того – критерій можливого завдання шкоди цілком доречний до будь-якого виду інформації з обмеженим доступом і тому немає потреби визначати новий її вид.

Іншим можливим шляхом вирішення проблем є намагання впровадження різних відступів від політики "відкритих даних" щодо обмежень надання окремих відомостей з державних реєстрів як запитувачам, так і агрегаторам. Саме у цьому контексті варто згадати проект закону "Про внесення змін до деяких законів України щодо запобігання розголошенню окремих відомостей у текстах судових рішень" (реєстр. 7033-д від 13.01.23 р.), що ухвалено у першому читанні. Водночас характер зауважень юридичного характеру, висловлених при його обговоренні як Головним науково-експертним управлінням Апарату Верховної Ради України так і окремими фахівцями свідчить про неузгодженість між приписами Закону України "Про критичну інфраструктуру", відповідних підзаконних актів, приписів законодавства в інформаційній сфері та відповідними пропозиціями ініціаторів проекту. Окрім цього, сама концепція обмеження надання інформації з Єдиного реєстру судових рішень явно не сприймається у суспільстві.

Отже, саме ці два кола проблем інформаційно-правового характеру зумовлюють пошук ефективних шляхом удосконалення чинного законодавства в інформаційній сфері та його узгодження з приписами спеціального законодавчого акту. Що стосується загального стану правового регулювання у сфері захисту критичної інфраструктури, то визначені у п. 5 Прикінцевих та перехідних положень Закону України "Про критичну інфраструктуру" підзаконні акти і відповідні заходи Кабінетом Міністрів України вживаються доволі повільно, що зумовлено об'єктивними та, можливо, суб'єктивними

причинами. Зокрема, це стосується наступного. Кабінетом Міністрів України лише 12 липня 2022 р. затверджено Постанову № 787 “Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України”, що не набрала чинності. У той же час заходи щодо її фактичного утворення необхідно було прискорити від самого початку, оскільки доволі тривалий час зберігається ситуація невизначеності та розподілу компетенції цієї служби між різними державними органами. 28 квітня 2023 року Кабінетом Міністрів України затверджено Постанову № 415 “Про порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього”. Водночас зазначені заходи поки що не реалізовані. Це ж саме стосується і Розпорядження Кабінету Міністрів України від 19 вересня 2023 р. № 825-р, яким затверджено “Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури” в умовах відсутності Реєстру і багатьох неврегульованих питань щодо особливостей його ведення та наповнення.

Загалом Законом України “Про критичну інфраструктуру” визначено, що віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю певних критеріїв. Ці критерії об’єктів визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму [12].

Законодавчо визначено сім критеріїв, до яких належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об’єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість таких об’єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури [12].

На сьогодні варто утриматись від критики, хоча саме формулювання, що обрано законодавцем до дефініцій критеріїв, видається занадто складним. Слід також зазначити,

що з часу ухвалення Закону України “Про критичну інфраструктуру” до нього вже вносились зміни трьома Законами. При цьому законодавчі зміни були спрямовані на уточнення завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури та статусу уповноваженого органу у сфері захисту критичної інфраструктури України, діяльність якого спрямовує, координує та контролює Кабінет Міністрів України.

Отже, слід визнати, що заходи щодо створення інституційної системи захисту критичної інфраструктури, передбаченої Законом України “Про критичну інфраструктуру”, дещо затягнулись.

Висновки.

1. Загалом реалізація на законодавчому рівні концепту “критичної інфраструктури”, що не був актуальним для вітчизняного законодавства протягом тривалого часу, відбувалась із урахуванням підходів, дефініцій та норм законодавства ЄС стосовно захисту критичної інфраструктури. Таким чином ухвалення спеціального законодавчого акту – Закону України “Про критичну інфраструктуру” є позитивним моментом для вітчизняного правового регулювання.

2. Реалізація норм законодавчого акту відбувається у складних умовах збройної агресії проти нашої держави під впливом негативних факторів, пов’язаних із недостатньою ефективністю загальної системи державного управління. Зазначена реалізація шляхом ухвалення необхідних підзаконних актів та формування необхідної інституційної системи, що спроможна належним чином виконувати визначені законодавчим актом завдання, на жаль, відбувається доволі повільно.

3. Певна “еклектика” нормативно-правових актів та категорійно-понятійного апарату, який не є однозначно зрозумілими через наявність протиріч для окремих державних органів, не дозволяє досягнути головного завдання – створення реєстру об’єктів критичної інфраструктури, як автоматизованої системи, що містить перелік найбільш важливих для життєдіяльності суспільства та держави об’єктів критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання, а й більш широкого переліку державних важливих інформаційних ресурсів, які також підлягають захисту.

4. Інформаційно-правові аспекти захисту критичної інфраструктури підкреслюють наявність проблемного поля, що полягає у наявності двох груп проблем. До першої належать складнощі із належністю окремих складових інфраструктури саме до об’єктів критичної інфраструктури, оскільки сенс законодавчого акту полягає у визначенні організаційних підходів щодо фізичних об’єктів, які не враховують особливостей інформаційної інфраструктури, інформаційних ресурсів та систем обробки інформації. Друга група проблем полягає у визначенні організаційних заходів, що полягають в інформаційному захисті об’єктів та обмеженні інформації щодо них, оскільки баланс між державної політикою “відкритих даних” та прозорості державного управління і потребами захисту критичної інфраструктури доволі складним, як і пошук шляхів побудови такого балансу. Саме на це мають бути спрямовані подальші комплексні наукові дослідження у галузі права.

Використана література

1. Council Directive 2008/114/ЄС 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.* 23.12.2008. L 345/75.

2. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. URL: http://zakon2.rada.gov.ua/laws/show/563-2016-п.

4. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. Київ: НІСД, 2012. 96 с.

5. Яременко О.І., Страхніцький Я.І. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. *Публічне управління та митне адміністрування.* 2022. № 1. С. 76-82.

6. Чумаченко С.М., Троцько В.В. Оцінювання загроз об'єктам критичної інфраструктури. *Цивільний захист та пожежна безпека.* 2017. № 1. С. 41-47.

7. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Наукові записки ІПіЕНД ім. І.Ф. Кураса НАН України.* 2013. Вип. 6 (68). С. 106-115.

8. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. Київ: Едельвейс, 2014. 497 с.

9. Довгань О.Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореф. дис. …д-ра юрид. наук: 12.00.07. Київ, 2016. 46 с.

10. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України: дис. …д-ра юрид. наук: 12.00.07. Запоріжжя, 2021. 467 с.

11. Anglmayer I. European critical infrastructure. Revision of Directive 2008/114/EC: Briefing for the European Parliamentary Research Service (EPRS). February, 2021. 12 p.

12. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

13. Краус К.М., Краус Н.М., Поченчук Г.М. Цифрова інфраструктура в умовах віртуалізації та нової якості управління економічними відносинами. *Ефективна економіка.* 2021. № 9. URL: http://www.economy.nayka.com.ua/?op=1&z=9279

14. Єфремова К.В. Роль цифрових інфраструктур у забезпеченні цифрового суверенітету // Базові аспекти цифровізації та їх правове забезпечення: монографія; НДІ прав. забезп. інновац. розвитку НАПрН України. Харків, 2021. С. 7-36.

15. Гладківська О.В. Вплив Хмарних технологій на стан інформаційної безпеки: правовий аспект. *Інформація і право.* 2014. № 3(12). С. 92-101.

16. Мельник Т. Телеком-Чорнобиль. *Forbes-UA*. Березень, 2024. URL: https://forbes.ua/company/telekom-chornobil-15032024-19815

17. Про інформацію: Закон України від 02.10.92 р. № 2657-XII, в ред. від 13.01.11 р. № 2938-VI. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

18. Про державну таємницю: Закон України від 21.01.94 р. № 3855-XII, в ред. від 21.09.99 р. № 1079-XIV. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

19. Задувайло О.К. Проблема визначення поняття "чутлива інформація" в контексті забезпечення інформаційної безпеки держави. *Гілея.* 2017. Вип. 116. С. 280-284.

20. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України: Постанова Кабінету Міністрів України від 12.07.22 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text

21. Про порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.23 р. № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

22. Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.23 р. № 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

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