DOI: 10.34015/2523-4552.2022.4.05
УДК: 351.81

Кулешов М. В.,
здобувач аспірантури Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ОБ'ЄКТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Статтю присвячено дослідженню нормативно-правового регулювання об'єктів критичної інфраструктури та їх кібербезпеки в умовах триваючої військової агресії рф проти України. На підставі порівняльного аналізу та аналізу чинних нормативно-правових актів визначено особливості формування переліку об'єктів критичної інфраструктури як об'єктів забезпечення кібербезпеки. Встановлено, що з урахуванням характеру та розміру шкоди, яка завдається ракетними ударами по цивільній та воєнній інфраструктурі, запропоновано переглянути наведені у додатках 1 і 2 Методики категоризації об'єктів критичної інфраструктури критерії оцінки критичності об'єкта критичної інфраструктури.

Ключові слова: *об'єкти критичної інфраструктури, кібербезпека, нормативно-правове регулюванн*.

Постановка проблеми. Майже десятиліття тому автори Стратегії кібербезпеки Німеччини наголосили, що забезпечення доступності кіберпростору, а також цілісності, достовірності та конфіденційності інформації в кіберпросторі є однією з найважливіших проблем XXI-го сторіччя. Саме тому захист кіберпростору стає головним завданням держави, економіки і суспільства як на державному, так і на міжнародному рівні [1]. Разом з цим, і це є принциповою точкою зору, інформація дедалі частіше стає предметом, і, навіть більше – засобом вчинення кримінальних правопорушень. І в більшості випадків проблема у кіберпросторі, створена зловмисними діями, може бути вирішена не окремим застосуванням апаратних, програмних чи організаційно-правових засобів, а саме їх збалансованим поєднанням, що характеризує особливість кібербезпеки як інституту інформаційного права.

На думку аналітиків, які досліджують окремі питання стратегічної конкуренції у кіберпросторі, військова агресія рф проти України демонструє ставки у стратегічних змаганнях в кіберпросторі, де росія намагається пошкодити і розірвати українські військові, урядові і цивільні мережі і все, що від них залежить. Те, що росії досі не вдалося досягти стратегічного результату в

Україні за допомогою кіберзасобів не означає, що потенційно вона не може цього зробити, і не повинно відволікати увагу від проблем, створюваних для воєнних зусиль України і потенціалу суспільства загалом це робити, через кібероперації російської військової розвідки. Російські спроби завдати шкоди військовій обороні України і ускладнити цивільне життя показали обмежену корисність кібероперацій для стратегічного примусу, але не варто забувати про ресурси і рішучість, які необхідні для відбиття російських кібероперацій протягом тривалого часу [2]. З урахуванням реалій воєнного часу вбачається за доцільне проаналізувати сучасний стан нормативно-правового регулювання кібербезпеки об'єктів критичної інфраструктури та визначити подальші напрями удосконалення чинного законодавства в цій сфері.

Аналіз останніх досліджень і публікацій. Проблеми правового забезпечення кібербезпеки критичної інфраструктури України неодноразово досліджувались О. Барановим, П. Гарасимою, К. Бєляковим, С. Божком, І. Діордіцею, В. Ліпканом, Н. Коваленком, Б. Кормичем, І. Кушніром, О. Малашком, Ю. Максименком, М. Микитюком, Л. Сопільником, М. Стрельбіцьким, А. Тарасюком, О. Тихомировим, О. Юдіним та ін.

Постановка завдання. Проаналізувати сучасний стан нормативно-правового регулювання забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах триваючої збройної агресії та визначити перспективні напрямки його удосконалення.

Виклад основного матеріалу. Указом Президента України від 24 лютого 2022 року № 64/2022 «Про введення воєнного стану в Україні». Зазначений Указ як підставу введення воєнного стану в Україні зазначає військову агресію рф проти України [3].

У своїй резолюції «Агресія проти України» A/RES/ES-11/1 від 2 березня 2022 року Генеральна Асамблея Організації Об'єднаних Націй визнала, що росія вчинила агресію проти України, порушивши базові норми ООН, і висунула російській федерації вимогу припинити збройну агресію проти України, включаючи також деокупацію Криму та Донбасу, негайно, повністю та безумовно вивести всі свої збройні сили з території України в межах її міжнародно визнаних кордонів. Також Генеральна Асамблея ООН висловила жаль з приводу участі білорусі у цьому незаконному застосуванні сили проти України, закликавши її дотримуватися своїх міжнародних зобов'язань.

Стратегія воєнної безпеки України, затверджена Указом Президента України від 25 березня 2021 року № 121/2021, наголошує на тому, що стійкість у ході всеохоплюючої оборони України досягається здатністю системи управління державою, сил оборони, національної економіки, інфраструктури та суспільства швидко відновлюватися та адаптуватися до змін у безпековому середовищі й до тривалого протистояння в наданні відсічі і стримування збройної агресії проти України, підтриманням спроможностей до здійснення стратегічного розгортання, територіальної оборони України, руху опору, ведення операцій (бойових, спеціальних, стабілізаційних дій), налагодженням надійних каналів комунікації з населенням та

підтриманням його життєдіяльності [4]. Як бачимо, Стратегія вказує на інфраструктуру та на здатність управління нею, як на елемент стійкості у ході всеохоплюючої оборони України.

Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р, визначає, що, з урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури (сукупності об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України) є одним із пріоритетів у реформуванні сектору оборони і безпеки України [5].

Перелік об'єктів кібербезпеки визначено у ч. 1 ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України». Серед них окремо виділено об'єкти критичної інфраструктури. Більшість підприємств, віднесених за відповідними ознаками до об'єктів критичної інфраструктури, мають певні потужності, які при руйнуванні здатні завдати значної шкоди екологічній безпеці регіону, спричинити загибель людей чи завдати шкоди їхньому здоров'ю. І ця їх особливість інколи і є вирішальною у випадку, коли, наприклад, особа, яка планує вчинити терористичний акт чи диверсію, обирає для цього найбільш уразливий об'єкт. Аналогічна шкода може бути завдана у ході ведення бойових дій або у разі спричинення державою-агресором ракетних ударів.

Зазначену позицію підтримує О. П. Єрменчук, вказуючи, що «критична інфраструктура завжди була і залишається першочерговим об'єктом захисту та джерелом інтересу агресора чи важливим об'єктом, що може бути уражений різного роду факторами, в т.ч. не лише соціального, а і природного характеру» [6, с. 14]. Аналогічної точки зору дотримується С. Кавин, зазначаючи, що «деякі держави розглядають забезпечення кібербезпеки як цивільну або економічну задачу, хоча багато держав залучають до вирішення цього завдання спецслужби, зокрема, для здійснення політики забезпечення кібербезпеки. Водночас міжнародна співпраця стосовно уніфікованих підходів до боротьби з кіберзагрозами в інформаційному просторі має дещо обмежений характер, оскільки спецслужби насамперед захищають національну критичну інфраструктуру від кіберзагроз і діють у рамках національних інтересів» [7, с. 315].

Деталізоване згадування поняття «критична інфраструктура» в нормативно-правових актах здійснено в Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року № 287/2015 [8], у якій серед актуальних загроз національній безпеці України визначено: 1) загрози кібербезпеці і безпеці інформаційних ресурсів, а саме: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також 2) загрози безпеці критичної інфраструктури, а саме: критична зношеність основних фондів об'єктів інфраструктури України

та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури та систем життєзабезпечення.

В подальшому, вже в тексті Стратегії забезпечення державної безпеки об'єкти критичної інфраструктури поруч із державним суверенітетом, конституційним ладом, територіальною цілісністю України, оборонним, економічним і науково-технічним потенціалом, кібербезпекою, інформаційною безпекою, державною таємницею та службовою інформацією віднесено до об'єктів забезпечення державної безпеки. Одночасно констатовано посилення загроз для критичної інфраструктури, пов'язаних з тимчасовою окупацією частини території України, триваючими гібридними впливами з боку суб'єктів розвідувально-підривної діяльності, погіршенням технічного стану такої інфраструктури та намаганнями несанкціонованого втручання в її функціонування, зокрема фізичного і кіберхарактеру [9].

Аналізуючи руйнівний вплив кібернетичних атак на критичну інфраструктуру, К. Б. Ганкевич, В. Д. Левчук та С. С. Корольов підсумовують, що «збитки можуть вимірюватися не лише фінансовими втратами, а й впливом на економіку держави, безпеку життєдіяльності громадян та загальну суспільно-політичну ситуацію в країні загалом. Кіберзлочинці прагнуть захопити максимальний контроль над інфраструктурою, атакуючи системи ІТ-управління шляхом зараження робочих станцій шкідливим програмним забезпеченням, яке використовується для знищення, копіювання, блокування, модифікації інформації в критичній інфраструктурі, або нейтралізації засобів захисту зазначеної інформації. Очевидно, що наша держава не зможе ефективно реагувати на загрози та виклики щодо захисту інформаційного простору без створення відповідної системи кібербезпеки критичної інфраструктури та необхідного набору правових засобів, що дозволять подолати прогалини правового регулювання у цій сфері» [10, с. 81].

Таким чином, враховуючи наведене вище, доходимо до висновку, що у разі віднесення об'єкту до критичної інфраструктури, необхідно опиратись на низку взаємопов'язаних факторів, які мають визначений характер та можуть бути обраховані чи охарактеризовані в конкретному вимірі. В подальшому такі фактори будуть чітко визначені та закріплені у Переліку секторів критичної інфраструктури та Методиці категоризації об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384) «Деякі питання об'єктів критичної інфраструктури» [11].

Наведена інформація дає всі підстави погодитись із окремими висновками О.А. Баранова, який відносить до об'єктів критичної інфраструктури в загальному випадку ті інфраструктурні об'єкти, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави. Також, як вказує названий вчений, «для випадку кібер-

безпеки: об’єкти критичної інфраструктури – це інфраструктурні об’єкти, що мають у своєму складі комп’ютерні системи та/або телекомунікаційні мережі, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави» [12, с. 60]. Дійсно, об’єкти критичної інфраструктури, які не мають комунікації з кіберпростором, певним чином убезпечені від кіберзагроз, що дозволяє не розглядати їх як об’єкти кіберзахисту.

В подальшому, з прийняттям Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX визначення «критична інфраструктура» та «об’єкти критичної інфраструктури» було закріплено на законодавчому рівні.

Відповідно до п. 13 ч. 1 ст. 1 Закону України «Про критичну інфраструктуру», до об’єктів критичної інфраструктури відносяться 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. Сама ж критична інфраструктура у п. 9 вказаної вище норми визначається як сукупність об’єктів критичної інфраструктури. В даному випадку можна констатувати, що у Законі України «Про критичну інфраструктуру» фактично відсутнє визначення критичної інфраструктури, сформульоване через її особливості та зміст. Натомість вона визначається через сукупність своїх складових. Означена особливість визначення критичної інфраструктури є, на наш погляд, вадою та має бути вирішена в подальшому.

Що ж саме заклав законодавець у законодавче визначення та зміст об’єктів критичної інфраструктури? Доцільно виділити наступні їх особливості:

1. Об’єкти інфраструктури, системи, їх частини та їх сукупність є важливими для економіки, національної безпеки та оборони.

2. Порушення їх функціонування може завдати шкоди життєво важливим національним інтересам.

Згідно п. 3 Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури, затверджених Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 15 січня 2021 року № 23, визнання того, що наслідки порушення сталого функціонування одного або низки об'єктів критичної інфраструктури можуть спричинити надзвичайні ситуації та/або мати негативний вплив на стан екологічної, енергетичної, економічної, фінансової безпеки, на стан обороноздатності держави, порушити систему управління нею, є головним критерієм віднесення об'єктів до об'єктів критичної інфраструктури. Тому передусім необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій.

Відповідно до ч. 1-2 ст. 8 Закону України «Про критичну інфраструктуру», віднесення об’єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України, за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологіч-

ну 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.

До критеріїв, які враховуються при вирішенні питання про віднесення об'єкта до об'єктів критичної інфраструктури 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.

Пункт 10 ч. 1 ст. 1 Закону України «Про національну безпеку України» визначає національні інтереси як життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [13]. Конкретних критеріїв, за якими національні інтереси можуть бути визначені важливими, ні наведений вище Закон, ні інші нормативно-правові акти не містять, що залишає це питання оціночним та відкритим.

Життєво важливі функції, про які йшла мова вище, в цілому можуть бути взяті як критерій для поділу об'єктів критичної інфраструктури на види. Так, з урахуванням наведених вище життєво важливих функцій Кабінетом Міністрів України у Постанові від 9 жовтня 2020 р. № 1109 сформовано перелік секторів крити-

чної інфраструктури, до яких наразі віднесені наступні: паливно-енергетичний сектор; цифрові технології; захист інформації; системи життєзабезпечення; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт і пошта; промисловість (хімічна промисловість, металургійна промисловість, оборонна промисловість, космічна промисловість, авіаційна промисловість, суднобудівна промисловість); сектор громадської безпеки; цивільний захист населення і територій; міграція (імміграція та еміграція); охорона навколишнього природного середовища; сектор оборони (зберігання боєприпасів, виробництво боєприпасів); національна безпека; правосуддя; тримання під вартою; наукові дослідження та розробки; фінансовий сектор; вибори та референдуми; соціальний захист; інформаційні послуги; державна влада та місцеве самоврядування.

В умовах триваючої збройної агресії особливої уваги необхідно приділити захисту кібербезпеки об'єктів критичної інфраструктури оборонного значення, а також тих, що надають критично важливі послуги із забезпечення найважливіших потреб населенню. Законодавець зобов'язаний проводити політику передбачення і негайного реагування на динамічні зміни, що відбуваються в кіберпросторі, розробляти і впроваджувати ефективні засоби та інструментарій можливого реагування на агресію в кіберпросторі, які можуть бути використані як засіб стримування військових конфліктів і загроз у кіберпросторі. В умовах глобалізації кіберзагроз доцільно уніфікувати підходи до адміністративно-правового регулювання у сфері кібербезпеки та стандартизувати заходи безпеки для ефективної співпраці, координації зусиль на національному та міжнародному рівнях [14, с. 270].

Висновки. З моменту початку нового етапу збройної агресії рф проти України 24 лютого 2022 року, жодних концептуальних змін до чинного законодавства чи законодавчих новацій в частині забезпечення кібербезпеки, у тому числі на об'єктах критичної інфраструктури, не приймалось, незважаючи на те, що кількість загроз кібербезпеці об'єктів критичної інфраструктури суттєво зросла. Зокрема, з урахуванням характеру та розміру шкоди, яка завдається ракетними ударами по цивільній та воєнній інфраструктурі, пропонується переглянути наведені у додатках 1 і 2 Методики категоризації об'єктів критичної інфраструктури критерії оцінки критичності об'єкта критичної інфраструктури, яка проводиться секторальним органом у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури.

Список використаних джерел

1. German Cyber Security Strategy 2011. URL: http://www.enisa.europa.eu/ media/news-items/german-cyber-security-strategy-2011-1.

2. НАТО і стратегічна конкуренція в кіберпросторі. [Електронний ресурс]. URL: https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html.

3. Про введення воєнного стану в Україні / Указ Президента України від 24 лютого 2022 року № 64/2022. URL: https://www.president.gov.ua/documents/1212021-37661.

4. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» / Указ Президента України від 25 березня 2021 року № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661.

5. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р., [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р#Text.

6. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

7. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в країнах Балтії [Текст]/ Підприємництво, госп-во і право : наук.-практ. госп.-прав. журн. 2020. № 12. С. 315-320.

8. Про рішення Ради національної безпеки та оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс] : Указ Президента України від 26 трав. 2015 р. № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015.

9. Про рішення Ради національної безпеки та оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» [Електронний ресурс] : Указ Президента України від 16 лютого 2022 р. № 56/2022. URL: https://president.gov.ua/documents/562022-41377.

10. Ганкевич К. Б., Левчук В. Д., Корольов С. С. Особливості становлення правових засад існування об'єктів критичної інфраструктури України в системі Міністерства оборони України. Юридичний науковий електронний журнал. 2021. № 11. С 79-82.

11. Деякі питання об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384) [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

12. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2 (42). С. 54-62.

M. Kuleshov, *graduate student of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"*

Critical infrastructure objects as an object of ensuring cyber security in conditions of armed aggression

The article is devoted to the study of regulatory and legal regulation of critical infrastructure objects and their cyber security in the conditions of the ongoing mili-

tary aggression of the russian federation against Ukraine. In particular, on the basis of a comparative analysis and an analysis of current legal acts, the specifics of forming a list of critical infrastructure objects as objects of cyber security were determined. It was established that since the beginning of the new stage of armed aggression of the russian federation against Ukraine on February 24, 2022, no conceptual changes to the current legislation or legislative innovations in terms of ensuring cyber security, including at critical infrastructure facilities, have been adopted, despite a significant increase in the number threats to their cyber security. Taking into account the nature and extent of damage caused by missile strikes on civilian and military infrastructure, it is proposed to revise the criteria for assessing the criticality of a critical infrastructure object given in Appendices 1 and 2 of the Methodology for Categorizing Critical Infrastructure Objects.

Keywords: *critical infrastructure facilities, cyber security, legal regulation*.

