УДК 342.
DOI https://doi.org/10.32782/2524-0374/2024-5/168

ВСТАНОВЛЕННЯ ТА ПОСИЛЕННЯ ОХОРОНИ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ЗАХІД ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

ESTABLISHMENT AND STRENGTHENING OF CRITICAL INFRASTRUCTURE PROTECTION AS A MEASURE OF THE LEGAL REGIME OF MARTYR STATE

Стефанчишен Р.В.,
доктор філософії в галузі права

Стаття присвячена дослідженню встановленню та поселенню охорони об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення як заходу правового режиму воєнного стану. Встановлено, що нормативно встановлено ряд механізмів, які підтверджують спеціальний режим захисту об'єктів критичної інфраструктури; 2) здійснення секторизації об'єктів критичної інфраструктури та закріплення за ними секторальних органів, які уповноважені забезпечувати захист відповідного сектору критичної інфраструктури шляхом виділення; 3) наявність нормативно встановленого порядку та методики категоризації об'єктів критичної інфраструктури; 4) ведення Реєстру об'єктів критичної інфраструктури; 5) вироблення плану національного захисту та забезпечення безпеки та стійкості критичної інфраструктури, що передбачає виконання чітко поставлених завдань.

Акцентовано увагу на тому, що захист об'єктів критичної інфраструктури в період дії воєнного стану постійно удосконалюється. Важливим кроком у цьому напрямку є затвердження вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Стверджено, що поступовість втілення заходів забезпечення кіберзахисту паливно-енергетичного комплексу, яких передбачено для його об'єктів як об'єктів критичної інфраструктури не вказує на хронології застосування окремих заходів, а є алгоритмом дій, що мають застосовуватись в кожному конкретному випадку залежно від трансформації інформаційних загроз. Зроблено висновок, що в умовах дії воєнного стану обмін інформацією між суб'єктами національної системи захисту критичної енергетичної інфраструктури відбувається переважно в режимі реагування на виникнення кризової ситуації.

Встановлено, що застосування посиленої охорони об'єктів критичної інфраструктури передбачає спеціальний порядок правового регулювання суспільних відносин в сфері критичної інфраструктури, встановлює можливість впливу на конкретних об'єктів та порядок їх діяльності, що має прояв у встановленні додаткових гарантії, пільг, форм державної підтримки, обмежень, заборон і додаткових підстав юридичної відповідальності.

Ключові слова: захід правового режиму воєнного стану, охорона, спеціальний режим захисту, об'єкти критичної інфраструктури, об'єкти критичної енергетичної інфраструктури.

The article is devoted to the study of the establishment and settlement of protection of critical infrastructure facilities and facilities that ensure the vital activity of the population as a measure of the legal regime of martial law. It is established that a number of mechanisms have been established by law that confirm the special regime of protection of critical infrastructure facilities; 2) implementation of sectorization of critical infrastructure facilities and assignment of sectoral bodies to them, which are authorized to ensure the protection of the relevant sector of critical infrastructure by allocation; 3) the presence of a normatively established procedure and methodology for categorization of critical infrastructure facilities; 4) maintenance of the Register of Critical Infrastructure Facilities; 5) development of a national plan for protection and ensuring the security and stability of critical infrastructure, which provides for the implementation of clearly set tasks.

Attention is focused on the fact that the protection of critical infrastructure facilities during the period of martial law is constantly being improved. An important step in this direction is the approval of the requirement for cybersecurity of the fuel and energy sector of critical infrastructure. It is argued that the gradual implementation of measures to ensure cyber protection of the fuel and energy complex, which are provided for its facilities as critical infrastructure facilities, does not indicate the chronology of the application of individual measures, but is an algorithm of actions that should be applied in each specific case depending on the transformation of information threats. It is concluded that under martial law, the exchange of information between the subjects of the national system of protection of critical energy infrastructure occurs mainly in the mode of response to the emergence of a crisis situation.

It is established that the application of enhanced protection of critical infrastructure facilities provides for a special procedure for legal regulation of public relations in the field of critical infrastructure, establishes the possibility of influencing specific facilities and the procedure for their activities, which is manifested in the establishment of additional guarantees, benefits, forms of state support, restrictions, prohibitions and additional grounds for legal liability.

Key words: martial law legal regime measure, protection, special protection regime, critical infrastructure facilities, critical energy infrastructure facilities.

Актуальність дослідження. Серед заходів правового режиму воєнного стану, що спрямовані на охорону значущих об'єктів та цінностей під час дії воєнного стану, чільне місце відведено встановленню та поселенню охорони об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення. Виокремлення об'єктів критичної інфраструктури здійснюється в порядку та на підставі Закону України «Про критичну інфраструктуру». Відповідно до п. 13 ст. 1 цього нормативно-правового акту, «об'єктами критичної інфраструктури» визнаються «… 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» [1]. При цьому, дослідження цього заходу правового режиму воєнного стану практично не проводились. Тому, ***метою статті*** є здійснення характеристики такого заходу правового режиму воєнного стану як встановлення та поселення охорони об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення.

Виклад основного змісту. нормативно встановлено ряд механізмів, які підтверджують спеціальний режим захисту об'єктів критичної інфраструктури:

1) визначення відповідності сукупності критеріям, що вказують на: а) соціальну, політичну, економічну, екологічну значущість об'єктів для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, в тому числі для реалізації життєво важливих функцій та надання життєво важливих послуг; б) існування загроз для таких об'єктів, 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 [1];

2) здійснення секторизації об'єктів критичної інфраструктури та закріплення за ними секторальних органів, які уповноважені забезпечувати захист відповідного

сектору критичної інфраструктури шляхом виділення: а) паливно-енергетичного сектору та надання відповідних повноважень Міністерству енергетики України, б) сектору цифрових технологій та надання відповідних повноважень Міністерству цифрової трансформації України, в) сектору захисту інформації та надання відповідних повноважень Держспецзв'язку, г) сектору харчової промисловості та агропромислового комплексу та надання відповідних повноважень Мінагрополітики, д) сектору державного матеріального резерву та надання відповідних повноважень Мінекономіки тощо [2];

3) наявність нормативно встановленого порядку [3] та методики категоризації об'єктів критичної інфраструктури [4], що передбачає виокремлення: I категорії критичності, до якої відноситимуться особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив, а порушення їх функціонування може призвести до виникнення кризової ситуації державного значення; II категорії критичності, до якої відноситимуться життєво важливі об'єкти, а порушення їх функціонування призведе до виникнення кризової ситуації регіонального значення; III категорія критичності, до якої відноситимуться важливі об'єкти, а порушення їх функціонування призведе до виникнення кризової ситуації місцевого значення; IV категорія критичності, до якої відноситимуться необхідні об'єкти, а порушення їх функціонування призведе до виникнення кризової ситуації локального значення [1];

4) ведення Реєстру об'єктів критичної інфраструктури. Примітно, що у період дії правового режиму воєнного стану, а також протягом дванадцяти місяців після його припинення чи скасування діють спеціальні правила доступу до цього Реєстру та його адміністрування. Зокрема, обмежується безпосередній доступ до інформації (включно з тією, яка розміщується на офіційному вебсайті уповноваженого органу у сфері захисту критичної інфраструктури України), а надання інформації з Реєстру посадовим/службовим особам надається виключно за письмовим запитом до Адміністрації Державної служби спеціального зв'язку та захисту інформації [5];

5) вироблення плану національного захисту та забезпечення безпеки та стійкості критичної інфраструктури, що передбачає виконання чітко поставлених завдань, а саме: правова регламентація діяльності суб'єктів національної системи захисту критичної інфраструктури; створення системи координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури; запровадження управління ризиками критичної інфраструктури; посилення стійкості національної системи захисту критичної інфраструктури; налагодження міжнародної співпраці [6].

Захист об'єктів критичної інфраструктури в період дії воєнного стану постійно удосконалюється. Наприклад, щодо паливно-енергетичного комплексу, то Законом України «Про функціонування паливно-енергетичного комплексу в особливий період» встановлено, що: до паливно-енергетичного комплексу входять підприємства, установи та організації електроенергетичного, ядерно-промислового, вугільно-промислового та нафтогазового комплексів незалежно від форми власності; виокремлено спеціальні завдання підприємств, установ та організацій паливно-енергетичного комплексу; за організацію роботи підприємств, установ та організацій паливно-енергетичного комплексу відповідає Кабінет Міністрів України; щодо вирішення питань забезпечення функціонування паливно-енергетичного комплексу, його технічне прикриття та відбудова його об'єктів – покладено на центральний орган виконавчої влади, що реалізує державну політику у паливно-енергетичному комплексові; відповідальність за невиконання підприємствами, установами та організаціями комплексу мобілізаційних завдань несуть їх керівники тощо [7].

Пріоритетні напрями формування державної політики щодо безпеки паливно-енергетичного комплексу зосереджено й в положеннях Енергетичної стратегії України на період до 2050 року [8], що базується на таких положеннях: 1) досягнення максимального рівня кліматичної нейтральності; 2) максимальне зменшення використання вугілля в енергетичному секторі; 3) оновлення та модернізація енергетичної інфраструктури; 4) підвищення ефективності використання ресурсів у енергетичному секторі; 5) широка інтеграція з ринками Європейського Союзу та ефективне функціонування внутрішніх ринків; 6) забезпечення енергетичного сектору власними ресурсами з урахуванням економічної доцільності; 7) розвиток альтернативних джерел енергії, нових продуктів та інноваційних рішень в енергетичному секторі тощо.

Тобто, загальна місія Енергетичної стратегії України до 2050 року полягає у створенні умов для сталого розвитку національної економіки шляхом забезпечення доступу до надійних, стійких та сучасних джерел енергії (альтернативних джерел енергії), що матиме наслідком забезпечення безпеки паливно-енергетичного комплексу.

Слід зазначити, що в разі недоступності або пошкодження об'єктів паливно-енергетичного комплексу, можуть виникнути серйозні наслідки для функціонування економіки та соціальної сфери країни. Як наслідок, мають бути застосовані усі можливі засоби захисту цього об'єкту критичної інфраструктури в період дії воєнного стану. До них віднесемо й інформаційний захист. Заходи з кіберзахисту передбачаються та реалізуються на всіх етапах життєвого циклу об'єкта критичної інфраструктури та покладаються на органами, які здійснюють керівництво даними об'єктними паливно-енергетичного комплексу [9].

Важливим кроком у цьому напрямку є затвердження вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Згідно вказаного документа, виокремлюють декілька етапів розробки та впровадження кіберзахисту: 1) визначення пріоритетів та області застосування вимог (ставлення цілей та пріоритетів організації; вибір заходів кіберзахисту та обсягу інформаційних систем та активів); 2) аналіз оточення для надання життєво важливих послуг та функцій (виявлення систем та активів, які забезпечують послуги та функції; оцінка нормативних вимог та управління ризиками; проведення консультацій з фахівцями з кібербезпеки); 3) створення поточного профілю кіберзахисту (розробка опису поточних заходів кіберзахисту); 4) оцінка ризику (аналіз ймовірності кіберінцидентів та їх наслідків; урахування нових загроз та вразливостей) тощо [10].

Можна стверджувати, що поступовість втілення заходів забезпечення кіберзахисту паливно-енергетичного комплексу, яких передбачено для його об'єктів як об'єктів критичної інфраструктури не вказує на хронології застосування окремих заходів, а є алгоритмом дій, що мають застосовуватись в кожному конкретному випадку залежно від трансформації інформаційних загроз.

Наразі здійснюється побудова системи кіберзахисту паливно-енергетичного комплексу на узгоджені зусилля двох ключових галузевих кіберцентрів під керівництвом Національної енергетичної компанії «Укренерго» та Національної акціонерної компанії «Нафтогаз України». Планується, що ці кіберцентри перетворяться на головні центри кібербезпеки для електроенергетичного та газового секторів відповідно. Більш того, на базі цих центрів передбачається розвиток додаткових напрямків, щоб охопити й інші важливі галузі, такі як ядерна енергетика, вугільна та торфодобувна промисловість [11].

Окремо зазначимо, що особливого захисту об'єктів паливно-енергетичного сектору потребують об'єкти енергетики. В цілому, критична енергетична інфраструктура – це об'єкти енергетики, що є необхідними для забезпечення життєво важливих для суспільства функцій, безпеки

та добробуту населення, виведення з ладу або руйнування яких матиме істотний вплив на національну безпеку та оборону, навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв [12; 13]. Таке визначення надано в профільному енергетичному законодавстві, зокрема Законах України «Про ринок природного газу» (п. 14^4 ч. 1 ст. 1) [12] та «Про ринок електричної енергії» (п. 40^1 ч. 1 ст. 1) [13].

У період дії воєнного стану впроваджується спеціальний порядок забезпечення обміну інформацією та взаємодії суб'єктів національної системи захисту критичної енергетичної інфраструктури [1]. Цей порядок передбачає послідовний обмін інформацією між суб'єктами національної системи захисту критичної енергетичної інфраструктури, що здійснюється відповідальними особами за допомогою використання засобів електронних комунікацій, національної системи конфіденційного зв'язку, спеціального зв'язку, шифрувального зв'язку та інформаційно-комунікаційних систем [14].

Отже, в умовах дії воєнного стану обмін інформацією між суб'єктами національної системи захисту критичної енергетичної інфраструктури відбувається переважно в режимі реагування на виникнення кризової ситуації. Паралельно відбувається розширення компетенції Адміністрації Державної служби спеціального зв'язку та захисту інформації України як центрального органу виконавчої влади із спеціальним статусом, що уповноважений забезпечувати формування та реалізації державної політики у сфері організації спеціального зв'язку, захисту інформації, кіберзахисту, активної протидії агресії у кіберпросторі [15]. Так, до Постановою Кабінету Міністрів України «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 24.02.2024 р. було передбачено, що вказаний суб'єкт забезпечує здійснення повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування [16].

Виходячи з положень Національного Плану захисту та забезпечення безпеки та стійкості критичної інфраструктури за Державною службою спеціального зв'язку та захисту інформації встановлено ряд завдань, серед яких: удосконалення порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури; удосконалення порядку віднесення об'єктів до критичної інфраструктури та методики категоризації об'єктів критичної інфраструктури; підготовка пропозицій до проектів документів стратегічного планування щодо забезпечення безпеки та стійкості критичної інфраструктури, здійснення її захисту; формування та ведення Реєстру об'єктів критичної інфраструктури; подання рекомендацій щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно до категорій об'єктів критичної інфраструктури тощо [6].

Як наслідок, Державною службою спеціального зв'язку та захисту інформації України визначено заходи з реагування на кіберінцидент/кібератаку для забезпечення: швидкого виявлення кіберінциденту/кібератаки; належного інформування про їх виникнення уповноважених органів та залучених сторін; запобігання, мінімізацію та усунення негативних наслідків; виявлення вразливостей; відновлення надання суб'єктами забезпечення кібербезпеки послуг; сталості і надійності систем та інших об'єктів кіберзахисту, що належать суб'єктам забезпечення кібербезпеки; унеможливлення повторної реалізації виявленого кіберінциденту, а щодо кібератак – збереження можливих електронних доказів тощо [17]. Система управління подіями інформаційної безпеки (SIEM – Security Information and Event Management) використовується і в сфері енергетики. Крім того, з метою врегулювання питань забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлено вимоги до аудиторів інформаційної безпеки та порядок їх атестації (переатестації) [18].

До суб'єктів, які своїми рішеннями забезпечують інформаційно-правове забезпечення захисту енергосистеми віднесено й Міністерство енергетики України. Як приклад, може слугувати розроблення цим уповноваженим органом центральної виконавчої влади методики оцінювання стану кібербезпеки електричних мереж, що має на меті визначення алгоритму оцінки та вдосконалення програм з кібербезпеки електричних мереж. Вказаний захід спрямовано на визначення чітких критеріїв, що свідчать про належний стан кібербезпеки при функціонуванні електричних мереж. Розрахунок здійснюється на основі індексу кібербезпеки електричних мереж, що формується на основі періодичних інформаційних матеріалів, складовими яких є експертні, аналітичні, статистичні відомості про стан кібербезпеки електричних мереж, а також про окремі показники шкідливого впливу реалізованих кіберзагроз, складені з метою оцінки стану кібербезпеки електричних мереж [19].

Висновки. Підсумовуючи приходимо до висновків, що застосування посиленої охорони об'єктів критичної інфраструктури передбачає спеціальний порядок правового регулювання суспільних відносин в сфері критичної інфраструктури, встановлює можливість впливу на конкретних об'єктів та порядок їх діяльності, що має прояв у встановленні додаткових гарантії, пільг, форм державної підтримки, обмежень, заборон і додаткових підстав юридичної відповідальності. Виявлено вплив дії режиму воєнного стану на порядок обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури та значення кіберзахисту об'єктів критичної інфраструктури в цілому.

ЛІТЕРАТУРА:

1. Про критичну інфраструктуру: Закон України від 16.11.2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#top

2. Перелік секторів критичної інфраструктури: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови Кабінету Міністрів України від 16 січня 2024 р. № 48). URL: https://zakon.rada.gov.ua/laws/show/48-2024-%D0%BF#Text

3. Порядок віднесення об'єктів до критичної інфраструктури: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n11

4. Методика категоризації об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n11

5. 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. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

6. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: розпорядження Кабінету Міністрів України від 19.09.2023 р.№ 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

7. Про функціонування паливно-енергетичного комплексу в особливий період: Закон України від 02.11.2006 р. № 307-V. URL: https://zakon.rada.gov.ua/laws/show/307-16#Text

8. Енергетична стратегія України на період до 2050 року. URL: https://www.mev.gov.ua/reforma/enerhetychna-stratehiya

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 року № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

10. Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури: Наказ Міненерго від 15.12.2022 року № 417. URL: https://zakon.rada.gov.ua/laws/show/z0249-23#Text

11. Кібербезпека енергетичної галузі. Офіційний веб-сайт Міністерства енергетики України. URL: https://mev.gov.ua/storinka/kiberbezpeka-enerhetychnoyi-haluzi

12. Про ринок природного газу: Закон України від 09.04.2015 р. № 329-VIII. URL: https://zakon.rada.gov.ua/laws/show/329-19#Text

13. Про ринок електричної енергії: Закон України від 13.04.2017 р. № 2019-VIII. URL: https://zakon.rada.gov.ua/laws/show/2019-19#n1784

14. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10.2022 р. № 1174. URL: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#n8

15. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 3.09.2014 р. № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#n8

16. Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 24.02.2023 р. № 167. URL: https://zakon.rada.gov.ua/laws/show/167-2023-%D0%BF#Text

17. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 р. № 570. URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text

18. Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації): наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.04.2024 р. № 228. URL: https://zakon.rada.gov.ua/laws/show/z0880-24#Text

19. Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж: Наказ Міністерства електроенергетики України від 05.08.2024 р. № 285. URL: https://zakon.rada.gov.ua/laws/show/z1278-24#Text