МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет
ім. М. Є. Жуковського
«Харківський авіаційний інститут»

БЕЗПЕКА ТА СТАЛИЙ РОЗВИТОК КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Тези доповідей
науково-практичної конференції
8 листопада 2023 р.

SECURITY AND SUSTAINABLE DEVELOPMENT OF CRITICAL INFRASTRUCTURE IN THE CONDITIONS OF MARTIAL LAW

Abstracts of the Scientific and Practical Conference
November 8, 2023

Харків – 2023

УДК 351.86 (063) doi: https://doi.org/10.32620/SSDCICML.23
Б40

Затверджено рішенням засідання кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (протокол № 3 від 18 жовтня 2023 р.)

Затверджено Вченою радою гуманітарно-провового факультету Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (протокол № 2 від 23 жовтня 2023 р.)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ:

Голова Оргкомітету:
- Олексій ЛИТВИНОВ – доктор юридичних наук, професор, Заслужений працівник освіти України, в. о. ректора Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут».

Заступники голови Оргкомітету:
- Микола НЕЧИПОРУК – доктор технічних наук, професор, Заслужений працівник освіти України, перший проректор Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»,
- Володимир ПАВЛІКОВ – доктор технічних наук, професор, проректор з наукової роботи Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»,
- Сергій ТЮЛЄНЄВ – кандидат економічних наук, директор Національного наукового центру «Інститут судових експертиз ім. заслуженого професора М. С. Бокаріуса».

Члени Оргкомітету:
- Наталія ФІЛІПЕНКО – докторка юридичних наук, професорка, в.о. завідувачки кафедри права Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»,
- Ганна СПІЦИНА – докторка юридичних наук, професорка, заступниця директора Національного наукового центру «Інститут судових експертиз ім. заслуженого професора М. С. Бокаріуса»,
- Михайло МОЖАЄВ – доктор технічних наук, професор, директор Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України,
- Василь СТРАТОНОВ – доктор юридичних наук, професор, заслужений юрист України, професор кафедри національного, міжнародного права та правоохоронної діяльності Херсонського державного університету,
- Алла БЛАГА – докторка юридичних наук, доцентка, професорка кафедри цивільного та кримінального права і процесу юридичного факультету Чорноморського національного університету імені Петра Могили,
- Ігор ШИНКАРЕНКО – кандидат юридичних наук, професор, професоркафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»,
- Світлана ГУЦУ – кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», заступниця декана гуманітарно-правового факультету,
- Алла ГОРДЕЮК – кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»,
- Олена САВЧУК – кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»,
- Сергій ЛУКАШЕВИЧ – кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут».

Секретар Оргкомітету: Наталія ФЕДОСЕНКО – кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут».

Технічний секретар: Тетяна ЛАЗАРЕВА – старша лаборантка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут».

Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану [Електронний ресурс] : тези доповідей науково-практичної конференції, 8 листопада 2023 р., Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут». – Харків : ХАІ, 2023. – 184 с.

До збірника увійшли тези доповідей учасників Науково-практичної конференції, присвяченої відзначенню Всесвітнього дня науки в ім'я миру та розвитку.
Видання призначене для науковців, науково-педагогічних працівників, здобувачів вищої освіти, практиків, які займаються вивченням питань сучасної науки.

Адреса редакційної колегії:

61070, м. Харків, вул.Чкалова, 17
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський авіаційний інститут».

Тези розповсюджуються в електронному вигляді.

Тези доповідей відтворені з авторських оригіналів.

Матеріали викладено в авторській редакції з незначними коректорськими правками.
Відповідальність за точність поданих фактів, цитат,
цифр і прізвищ несуть автори та їх наукові керівники.

Деякі доповіді та повідомлення мають дискусійний характер, оскільки в них висловлюється особиста думка автора, яка не завжди збігається з поглядами членів редколегії.

ЗМІСТ

ВІТАЛЬНЕ СЛОВО

Олексій ЛИТВИНОВ
доктор юридичних наук, професор,
в.о. ректора Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна

ШАНОВНІ КОЛЕГИ!

*Від себе особисто та за дорученням колективу Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» щиро вітаю учасників та гостей науково-практичної конференції «Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану»*із початком роботи цього представницького форуму!

Сучасна наука не в змозі розвиватися без обміну досвідом між різними науковими школами та пошуку можливостей для апробації та впровадження результатів досліджень. Особливої популярності набувають компаративні дослідження, у зв'язку з чим вбачається за доцільне залучення представників наукової еліти інших вузів нашої країни. Особливо важливим та актуальним на сьогодні це завдання стає в умовах воєнного стану, коли захист об'єктів критичної інфраструктури та життєзабезпечення є складовою частиною забезпечення національної безпеки України.

Дана науково-практична конференція стане майданчиком обміну думками, звірки теоретичних позицій і наукової творчості. Такі заходи мають вагомий теоретичний ефект, значущій резонанс як у науковому середовищі, так і серед практиків, оскільки розглядаються актуальні питання *модернізації вітчизняної безпекової системи*, імплементації до неї найкращих зразків правової дійсності зарубіжжя. Ми впевнені, що розробка стратегії розвитку та модернізації вітчизняної науки – це складний і відповідальний шлях створення перспективи прогресу у науковій сфері.

Дана зустріч – унікальна можливість для фахівців з різних навчальних закладів та наукових установ України обговорити актуальні питання розвитку науки, обмінятися досвідом, новими напрацюваннями, досягненнями й відкриттями.

Мета конференції – надання науково-педагогічному складу НАУ «ХАІ» та різних вузів нашої держави можливості поспілкуватися на науковому рівні, обмінятися ідеями і обговорити наукові проблеми щодо питань безпеки та сталого розвитку критичної інфраструктури в умовах воєнного стану, оволодіти практичними навичками у сфері наукової діяльності, зрештою, зав'язати або зміцнити наші дружні стосунки.

Переконаний, що професіоналізм, знання, досвід і високі людські якості науковців нашого університету, потужний науковий та освітній потенціал усіх засновників цієї конференції дадуть можливість ефективно модернізувати *вітчизняну безпекову систему* й вивести її на найвищий європейський рівень.

У досягненні цієї мети велике значення має обмін досвідом. Сподіваюся, що професійна дискусія та обмін досвідом дадуть новий імпульс подальшому удосконаленню *вітчизняної безпекової системи* та ефективному використанню її можливостей.

Бажаю учасникам та *гостям науково-практичної конференції «Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану»*плідної роботи та нових творчих здобутків в ім'я процвітання нашої країни!

СЛАВА УКРАЇНІ!

УДК 378:356:355

Світлана АНДРЕНКО
помічник ректора Ректорату Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
кандидатка юридичних наук
e-mail: sweta-a@ukr.net, ORCID: 0000-0002-2900-3120
Юрій ПОПЕЛЬНЮК
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права) Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна;
начальник відділу поліції 1 Харківського районного управління поліції 3 Головного управління Національної поліції в Харківської області, полковник поліції
e-mail: popelnyk_yuriy@ukr.net, ORCID: 0000-00021-7621-9506
Наталія ФІЛІПЕНКО
докторка юридичних наук, професорка,
професорка закладу вищої освіти кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: n.filipenko@khai.edu, ORCID: 0000-0001-9469-3650

ВЗАЄМОДІЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ІЗ АДМІНІСТРАЦІЄЮ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ ЯК ЕЛЕМЕНТУ СЕКТОРУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ПОПЕРЕДЖЕННІ ПРАВОПОРУШЕНЬ

Анотація: у доповіді розглянуті питання створення належних умов безпеки для учасників освітнього процесу шляхом налагодження взаємодії підрозділів національної поліції України із адміністрацією закладів вищої освіти як елементу сектору критичної інфраструктури у попередженні правопорушень, створення безпекового освітнього середовища за допомогою не лише стандартних заходів, але й новітніх проєктів, наприклад, використання послугспеціаліста з безпеки.

Ключові слова: безпекове освітнє середовище, взаємодія, поліція, заклади вищої освіти, спеціаліст з безпеки.

Сучасна концепція демократичної правової держави виходить із положення про державу-гаранта, особливість якої полягає в тому, що вона не тільки декларує загальнолюдські цінності, права і свободи особистості, а й здійснює широкі заходи щодо їх реального втілення у життя. Поліція в цьому випадку виступає одним із найважливіших інструментів (засобів) держави в забезпеченні подібних гарантій. Унікальність діяльності поліції полягає в тому, що, будучи частиною державного механізму реалізації державних інтересів і державної політики, вона виступає найбільшим за обсягом виконуваних правоохоронних функцій інститутом забезпечення гарантій, прав і свобод громадян. І найголовнішим із прав осіб – жити у безпечному

суспільстві, коли попередження правопорушень дозволяє забезпечувати власну безпеку та правопорядок.

Підрозділи Національної поліції України є однією із головних ланок системи попередження правопорушень. Вони здійснюють комплекс різноманітних заходів організаційного, соціально-економічного та виховного характеру. Невід'ємним обов'язком цих підрозділів є попереджувальна функція, що випливає з Положень Закону України «Про Національну поліцію» [1]. До їх головних завдань можна віднести: проведення заходів профілактичного характеру;виявлення умов і причин, що сприяють поширенню негативних явищ у молодіжному середовищі, що тягнуть за собою правові наслідки;контроль за підлітками, які перебувають у важкій життєвій ситуації та соціальнонебезпечному становищі;посилення взаємодії з органами, організаціями та установами, відповідальними за роботу з молоддю та захист їх прав тощо.

У системі попередження правопорушень одним із елементів є заклади вищої освіти (далі – ЗВО). До компетенції освітніх установ у цій сфері належить, наприклад, таке:розробка і застосування методик, спрямованих на формування правової поведінки; проведення комплексних обстежень для визначення необхідних форм навчання і правового виховання тощо.

Саме тому їхня взаємодія може розглядатися як найважливіше стратегічне доповнення традиційної поліцейської практики. Вважаючи своїм основним завданням встановлення партнерських відносин поліції і закладів вищої освіти, за яких усі поліцейськіструктури та всі співробітники ЗВО активно співпрацюють у вирішенні проблем, поліцейська робота з освітянами являє собою зміну практики, але не основнихцілей поліцейської діяльності. Ці цілі, як і раніше, передбачаютьзабезпечення громадського спокою і правопорядку; захистосновних прав і свобод особистості - особливо життя; запобігання та розкриття злочинів. Разом з тим, партнерство поліції та ЗВО дійсно забезпечує більш ефективну та дієву стратегію досягнення цих цілей.

Але з початку збройної агресії РФ проти України на підрозділи Національної поліції України покладено ще одне, найголовніше завдання – забезпечення безпеки в освітньому середовищі, у тому числі запобігання, раннє виявлення, припинення та усунення можливих негативних явищ, шляхом запровадження та організації діяльності спеціаліста із безпеки в освітньому середовищі [2].

Згідно із положеннями Порядку реалізації експериментального проекту «Спеціаліст із безпеки в освітньому середовищі»,спеціаліст із безпеки в освітньому середовищі (далі – спеціаліст) –працівник органу місцевого самоврядування, який працює у виконавчому органі сільської, селищної,

міської ради, на якого на період реалізації експериментального проекту покладено виконання функціональних обов'язків, спрямованих на створення та підтримання належного рівня безпеки в освітньому середовищі, забезпечення організації та участь у здійсненні узгоджених заходів із запобігання, раннього виявлення, припинення та усунення негативних явищ в освітньому середовищі.

Саме на спеціаліста з безпеки покладаються такі функціональні обов'язки:

1) здійснює безпосередню взаємодію із суб'єктами взаємодії відповідно до їх компетенції з питань забезпечення безпеки в освітньому середовищі;

2) розробляє і узгоджує із суб'єктами взаємодії відповідно до їх компетенції плани заходів (короткострокових, довгострокових) щодо покращення стану забезпечення безпеки в освітньому середовищі, а також питання щодо організації їх виконання, визначення ефективності відповідних заходів за результатами їх здійснення;

3) проводить інформаційно-просвітницькі заходи для педагогічних працівників з питань забезпечення безпеки в освітньому середовищі;

4) вносить керівництву закладів освіти, які закріплено за спеціалістом, пропозиції щодо покращення стану цивільного захисту, пожежної та техногенної безпеки в закладах освіти;

5) бере участь у проведенні фахівцями компетентного суб'єкта взаємодії превентивних заходів (лекцій, інтерактивних занять тощо) з основ безпеки та захищеності життя і діяльності дитини, суспільства і життєвого середовища від небезпечних та шкідливих факторів;

6) бере участь в організації та проведенні практичних заходів із цивільного захисту, надає за результатами їх проведення органу місцевого самоврядування (керівнику відповідної військової адміністрації) пропозиції щодо готовності закладу освіти, який закріплено за спеціалістом, до дій у разі виникнення надзвичайних ситуацій;

7) бере участь у розробленні рекомендацій (їх проектів) для учнів та педагогічних працівників з питань щодо дотримання прав та інтересів учнів, забезпечення їх безпеки;

8) бере участь в організації забезпечення безпеки під час проведення масових заходів у закладах освіти, які закріплено за спеціалістом;

9) готує та надає суб'єктам взаємодії відповідно до їх компетенції пропозиції щодо вжиття заходів до забезпечення безпеки, запобігання виникненню, раннього виявлення, припинення та усунення негативних явищ в освітньому середовищі щодо безпеки, а також вживає у співпраці з компетентними суб'єктами взаємодії відповідних заходів;

10) веде паспорт безпеки закладу освіти відповідно до визначеної форми, збирає та вносить до нього інформацію про стан пожежної та техногенної безпеки в закладі освіти, який закріплено за спеціалістом;

11) виявляє та невідкладно інформує про виявлені негативні явища в освітньому середовищі та/або причини і умови виникнення таких явищ відповідного суб'єкта взаємодії з метою вжиття ним заходів реагування відповідно до законодавства, вносить відомості про це до паспорта безпеки закладу освіти;

12) здійснює обстеження прилеглої до закладу освіти території щодо діяльності гральних закладів, закладів торгівлі, які порушують вимоги законодавства щодо заборони продажу дітям алкогольних напоїв і тютюнових виробів, взаємодіє із цього питання з Національною поліцією та виконавчим органом відповідної ради з метою вжиття заходів реагування відповідно до законодавства;

13) у разі виявлення ознак правопорушення негайно повідомляє відповідним суб'єктам взаємодії та/або службам, органам державної влади про такий факт, обов'язково реєструє таке повідомлення в паспорті безпеки закладу освіти;

14) невідкладно інформує підрозділи ДСНС про виявлення пожеж та інших надзвичайних ситуацій в закладі освіти та/або на прилеглій до закладу освіти території;

15) проводить моніторинг стану забезпечення безпеки у приміщенні закладу освіти, на території обслуговування, закріпленій за закладом освіти, на прилеглих територіях та дорогою до (із) закладу освіти (у тому числі щодо наявності (відсутності) негативних явищ в освітньому середовищі; ефективності заходів, що здійснюються з метою виявлення, припинення, усунення негативних явищ в освітньому середовищі; повноти виконання плану профілактичних та інших заходів, пов'язаних із забезпеченням безпеки освітнього середовища);

16) невідкладно інформує орган місцевого самоврядування (керівника відповідної військової адміністрації) про надзвичайні ситуації, нещасні випадки, що виникають в закладі освіти, який закріплено за спеціалістом, та/або на прилеглій до закладу освіти території;

17) бере участь в евакуації учасників освітнього процесу в разі загрози їх життю та здоров'ю [2].

Підсумовуючи питання взаємодії підрозділів національної поліції України із адміністрацією закладів вищої освіти як елементу сектору критичної інфраструктури у попередженні правопорушень хочемо зазначити наступне: основною передумовою партнерства між поліцією та закладами

вищої освіти є нагальна необхідність підвищення рівня їх залученості до забезпечення безпеки як здобувачів вищої освіти, так і всіх співробітників ЗВО, а також розв'язання проблеми підвищення ефективності протидії злочинності в освітянському середовищі, оскільки це завдання не може бути вирішене силами однієї лише поліції.Для досягнення подібних партнерських відносин, поліція повиннаглибше інтегруватися в діяльність закладів вищої освіти і зміцнити свою легітимність на основі узгоджених дій і поліпшення якості послуг, що надаються.

Список використаних джерел:

1. Про Національну поліцію (Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379). URL:https://zakon.rada.gov.ua/laws/show/580-19#Text
2. Порядок реалізації експериментального проекту "Спеціаліст із безпеки в освітньому середовищі". Затверджено постановою Кабінету Міністрів України від 15 серпня 2023 р. № 867. URL:https://zakon.rada.gov.ua/laws/show/867-2023-п#Text

УДК 343.98

Дар'я БАРБАШ
здобувачка вищої освіти третього освітньо-наукового рівня
(доктор філософії з Права) Національного аерокосмічного університету
імені М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: d.barbash@khai.edu, ORCID: 0000-0001-7814-9620

АТАКИ НА ЕНЕРГОСИСТЕМУ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ: УКРАЇНА ТА СВІТ

Анотація:Тези присвячені явищу атак на енергосистему в призмі відкритої збройної агресії зі сторони Російської Федерації проти України. Одночасно автор звертається до прикладів застосування вказаних атак під час інших збройних конфліктів у світі. Попри не винятковість у сучасній історії тотожних вчинених Російською Федерацією дій, характер атак на українську енергосистему відносить їх до категорії чистого терору.

Ключові слова: критична інфраструктура, енергосистема, терор, геноцид

ATTACKS ON THE ENERGY SYSTEM DURING ARMED CONFLICTS: UKRAINE AND THE WORLD

Abstract: The thesis is devoted to the phenomenon of attacks on the energy system in the context of the Russian Federation's open armed aggression against Ukraine. At the same time, the author refers to examples of the use of these attacks during other armed conflicts in the world. Despite the fact that similar actions committed by the Russian Federation are not exceptional in modern history, the nature of the attacks on the Ukrainian energy system places them in the category of pure terror.

Keywords: critical infrastructure, energy system, terror, genocide.

Всупереч тому, що поняття «критичної інфраструктури» є досить новим для сучасного українського законодавства, воно регулюється цілим переліком нормативно-правових актів, до яких входить, зокрема, Закони України «Про критичну інфраструктуру», «Про національну безпеку України», Рішення Ради національної безпеки і оборони України «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури», «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» та інш. Порядок-же віднесення об'єктів до критичної інфраструктури закріплений у Постанові Кабінету Міністрів України від 9 жовтня 2020 р. №1109 «Деякі питання об'єктів критичної інфраструктури».

Відповідно до вказаного порядку, до секторів критичної інфраструктури входить Паливно-енергетичний сектор, до якого своєю чергою відноситься підсектор «електро-енергетика». Типом основних послуг для означеного підсектору є: виробництво електричної енергії, забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку, управління системами передачі та енергопостачання та розподіл електричної енергії [1]. Таким чином об'єкти національної енергосистеми віднесені Постановою Кабінету Міністрів України від 9 жовтня 2020 р. №1109 до об'єктів критичної інфраструктури.

Протягом періоду відкритої збройної агресії зі сторони Російської Федерації, Україна зазнала значних пошкоджень саме енергосистеми внаслідок масованих ракетних обстрілів. Так, згідно з інформацією Офісу Генерального прокурора України «Збільшилася кількість атак ворога по об'єктах критичної інфраструктури. З жовтня по грудень 2022 року 70% ударів було саме по енергосистемі. Це підтверджує той факт, що ворог завдавав ударів та чинив ці злочини свідомо. Плюс вони збільшили не лише кількість, а й масштаби територій» [2].

Розглядаючи явище атак енергосистеми під час збройних конфліктів, слід зазначити, що такі прецеденти відомі всесвітній історії повсякчас. Так, під час Першої світової війни радянська енергосистема була об'єктом нападів Німеччини після втрати оперативної ініціативи під Сталінградом. Також на початковому етапі Корейської війни Сполучені Штати здійснювали атаки проти енергосистеми Північної Кореї з метою змусити її сісти за стіл переговорів. Під час війни у В'єтнамі електроенергія була ключовою ціллю операцій «Роллінг Тандер» і «Лайнбекер I і II» [3, с. 5-6].

НАТО ж здійснювало атаки на електроенергетичні трансформаторні підстанції Союзної Республіки Югославії під час компанії «Союзні сили» у 1999 році. У Остаточному звіті Прокурора Комітету, створеного для розгляду

кампанії НАТО з бомбардування Союзної Республіки Югославії виправдано вказані дії наступним чином: «З намічених електроенергетичних трансформаторних підстанцій одна трансформаторна підстанція подавала електроенергію в координаційну мережу протиповітряної оборони, а інша постачала електроенергію в оперативний центр північного сектора. Обидва ці об'єкти були ключовими елементами управління інтегрованою системою ППО Союзної Республіки Югославії» [4]

Відтак, дії Російської Федерації з атак української енергосистеми не є винятковими та новими для історії військових конфліктів. Разом з тим, масовий характер таких атак та невибірковість у їх здійсненні ще з 2022 року засуджуються світовою спільнотою, зокрема, Президентка Єврокомісії Урсула фон дер Ляйен у своєму зверненні до ЗМІ з приводу української кризи в Брюсселі (Бельгія, 28 вересня 2022 р.) назвала цілеспрямовані атаки Російської Федерації на цивільну інфраструктуру з чіткою метою відрізати чоловіків, жінок, дітей від води, електрики та опалення з наближенням зими - актами чистого терору. Одночасно в Офісі Генерального прокурора України розглядають вказані атаки як складову злочину геноциду [2], відтак вони будуть покладені в доказову базу для доведення вчинення Російською Федерацією геноциду українського народу задля притягнення до відповідальності Президента РФ та вищого керівництва країни-агресора.

Список використаних джерел:

1. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. №1109 «Деякі питання об’єктів критичної інфраструктури». Редакція від 11.05.2023. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 07.11.23)
2. Юрій Бєлоусов: Атаки ворога на критичну інфраструктуру ми розглядаємо як складову злочину геноциду. Офіс Генерального прокурора України. URL:https://www.gp.gov.ua/ua/posts/yurii-bjelousov-ataki-voroga-na-kriticnu-infrastrukturu-mi-rozglyadajemo-yak-skladovu-zlocinu-genocidu (дата звернення: 07.11.23)
3. Crawford, J.W. “The law of noncombatant immunity and the targeting of national electrical power systems.” *The Fletcher Forum of World Affairs* 21, no. 2 (1997): 101–119. URL: https://apps.dtic.mil/sti/pdfs/ADA312110.pdf (дата звернення: 07.11.23)
4. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. International Criminal Tribunal for the former Yugoslavia. URL: https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal (дата звернення: 07.11.23)

УДК 351.862.4:351.743(477)
Олег БАТЮК
доктор юридичних наук, доцент, професор кафедри державної безпеки
Волинського національного університету імені Лесі Українки, м. Луцьк, Україна
e-mail: olegbatiukibrlpnt@gmail.com, ORCID: 0000-0002-2291-4247

СЛУЖБОВО-БОЙОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Анотація: У положеннях тез наукової доповіді автор розкриває механізм організації службово-бойового забезпечення з охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об'єктів, об'єктів критичної інфраструктури та спеціальних вантажів підрозділами Національної гвардією України.
Ключові слова: безпека,критична інфраструктура, об'єкт, національна гвардія України, службово-бойові завдання.

SERVICE AND COMBAT SUPPORT OF SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES BY UNITS OF NATIONAL GUARD OF UKRAINE

Abstract: The author reveals the mechanism of organization of service and combat support of security of nuclear facilities, nuclear materials, radioactive waste, and other sources of state-owned ionizing radiation, important state facilities, critical infrastructure facilities and special cargo by units of National Guard of Ukraine in the provisions of theses of the scientific report.
Keywords: security, critical infrastructure, facility, National Guard of Ukraine, service and combat missions.

Актуальність теми обумовлена екологічною трагедією яка трапилась 6 червня 2023 року на території України в результаті злочинних дій російських військ які підірвали дамбу на Каховській Гідро електро станції, на далі (ГЕС). За офіційними даними Greenpeace станом на 14 червня 2023 року оприлюднили наступні відомості про наслідки підриву дамби на Каховській ГЕС (рис. 1.) [4].

На наше переконання, службово-бойове забезпечення безпеки об'єктів критичної інфраструктури підрозділами Національної гвардії України, на далі (НГУ), це комплекс заходів які реалізовуються особовим складом щодо вирішення бойових, спеціальних, ізоляційних, рейдових, пошуково-рятувальних завдань, спрямованих на забезпечення оборони та охорони від неправомірних посягань на об'єкти критичної інфраструктури та окремі їх елементи [3].

Рис. 1. Офіційні дані Greenpeace про наслідків підриву дамби на Каховській ГЕС

Варто зауважити що відповідно до положення пункту 5-1 частини 1 статті 2 статті Закон України «Про Національну гвардію України» до основних функцій Національної гвардії України відносять охорону об’єктів критичної інфраструктури, перелік яких визначається Кабінетом Міністрів України; участь у ліквідації наслідків кризових ситуацій на об’єктах критичної інфраструктури, що нею охороняються [1].

15 червня 2023 року Наказом № 497 Міністра внутрішніх справ України було затверджено Положення про організацію і порядок несення служби з охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об’єктів, об’єктів критичної інфраструктури та спеціальних вантажів Національною гвардією України [2].

Охорона об’єкта критичної інфраструктури підрозділами НГУ здійснюється по його периметру, у контрольно-пропускних пунктах (далі - КПП), режимних приміщеннях, будівлях, спорудах (далі - режимні приміщення).

Охорона об’єкта критичної інфраструктури підрозділами НГУ здійснюється такими способами або їх поєднанням: несенням служби чатовими на КПП, визначених ділянках периметра об’єкта та/або його режимних приміщень, реагування вартою на протиправні посягання стосовно

об’єкта, а також на порушення пропускного чи внутрішньо-об’єктового режимів; оперативним чергуванням варти, тобто забезпеченням виявлення особовим складом варти людей або предметів по периметру об’єкта та/або в його режимних приміщеннях за допомогою засобів виявлення та відеоспостереження.

Доцільно наголосити, що зовнішня огорожа, установлена по периметру об’єкта, позначається покажчиками з написом «Заборонена зона», «Прохід (проїзд, польоти) заборонено (закрито)», «Стороннім особам прохід заборонено».

В’їзд, виїзд транспортних засобів, вхід і вихід працівників та інших осіб, унесення (увезення) на територію чи винесення (вивезення) ними з території об’єкта майна здійснюється за перепустками або іншими документами, передбаченими пропускним чи внутрішньо-об’єктовим режимами (далі - перепустки).

Для організації та здійснення охорони об’єкта критичної інфраструктури підрозділами НГУ визначаються пости.

Межі постів на території об’єкта критичної інфраструктури позначаються розмежувальними знаками, які нумеруються і послідовно встановлюються в забороненій зоні таким чином, щоб були добре видні чатовим і не проглядалися із зовнішнього боку забороненої зони. Охорона об’єкта критичної інфраструктури вартою військовослужбовців НГУ здійснюється відповідно до плану охорони, форма якого встановлюється командувачем НГУ.

Зауважимо, що план охорони об’єкта критичної інфраструктури розробляється штабом військової частини НГУ, від якої споряджено варту, підписується начальником штабу та затверджується її командиром.

У частині, що стосується організації охорони режимних приміщень об’єкта критичної інфраструктури, план охорони об’єкта погоджується керівником такого об’єкта або його заступником з режиму. Тривалість несення служби вартою військовослужбовцями НГУ з охорони об’єкта критичної інфраструктури становить 12 або 24 години.

У варті, яка несе службу протягом 12 годин, призначається по одній зміні чатових на кожен пост, а також необхідна кількість вартових для проведення їх тимчасової підміни, а у варті, яка несе службу протягом 24 годин,- по три зміни.

До складу варти військовослужбовців НГУ з охорони об’єкта критичної інфраструктури призначаються: начальник варти, помічники начальника варти, помічник начальника варти - кінолог, розвідні, чатовий-оператор технічних засобів охорони (далі - ТЗО), водій транспортного засобу, чатові

КПП та чатові варти за кількістю постів і змін, а також вартові варти для тимчасової підміни чатових.

Зауважимо, що за потреби до складу варти можуть входити: механік інженерно-технічних засобів охорони (далі - ІТЗО), кухар, а в опалювальний період – опалювач (кочегар).

Особливістю є те, що до складу варти з охорони ядерної установки розвідний і помічник начальника варти - кінолог можуть не призначатися.

Як **висновок** заначимо, що особливістю службово-бойового забезпечення безпеки об'єктів критичної інфраструктури підрозділами НГУ є вирішення невідкладних (бойових) завдань з оборони та охорони об'єкта критичної інфраструктури із числа військовослужбовців НГУ, що несуть службу у варті і не знаходяться на постах, створюються групи реагування: тривожна, посилення та блокування. Військовослужбовці варти, які не увійшли до жодної з груп реагування, становлять резерв варти. Тривожна група призначається для негайного реагування на спрацювання ТЗО шляхом виявлення причин їх спрацювання та/або припинення протиправних посягань чи порушень пропускного або внутрішньо-об'єктового режиму і затримання осіб, що їх вчинили. Тривожна група може діяти на об'єкті і на прилеглій до нього території на віддаленні до трьох кілометрів, а в разі візуального спостереження порушника - на відстані, необхідній для його затримання. Місце розташування тривожної групи варти обладнується у вартовому приміщенні поряд з кімнатою зберігання зброї. Група посилення призначається для посилення охорони периметра об'єкта, КПП, його режимних приміщень у разі протиправного проникнення особи (осіб) на такий об'єкт, іншого порушення пропускного або внутрішньо-об'єктового режиму чи виникнення надзвичайних ситуацій. Група блокування призначається для перекриття окремих ділянок території об'єкта в разі проникнення порушника на такий об'єкт. Групи реагування варти, яка несе службу протягом 12 годин, можуть формуватися із числа особового складу взводів реагування. Під час несення служби варта з охорони об'єкта критичної інфраструктури підпорядковується командирові військової частини НГУ, начальникові штабу військової частини НГУ, від якої її споряджено, а також черговому військової частини НГУ. Особливістю є те, що у разі якщо начальник варти за своїм військовим званням вищий за чергового військової частини, така варта черговому військової частини не підпорядковується. З питань здійснення пропускного та забезпечення внутрішньо-об'єктового режимів на об'єкті варта підпорядковується комендантові комендатури цього об'єкта та його черговому помічнику. Повноваження щодо підпорядкування варти під час несення служби зазначеним посадовим особам реалізуються через начальника

такої варти. Варта з охорони об'єкта підпорядковується черговому військової частини НГУ, комендантові комендатури цього об'єкта та його черговому помічнику з моменту прийняття такою вартою об'єкта під охорону. Варта виходить з підпорядкування зазначених осіб з моменту здавання об'єкта з-під охорони.

Список використаних джерел:

1. Закон України «Про Національну гвардію України» від 13 березня 2014 року № 876-VII в редакції від 02.08.2023, підстава - 3232-IX.URL: https://zakon.rada.gov.ua/laws/show/876-18#Text *(дата звернення 05.10.2023 р.)*
2. Наказ № 497 від 15.06.2023 р. Міністра внутрішніх справ України про затвердження «Положення про організацію і порядок несення служби з охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об'єктів, об'єктів критичної інфраструктури та спеціальних вантажів Національною гвардією України». URL: https://zakon.rada.gov.ua/laws/show/z1085-23#Text *(дата звернення 05.10.2023 р.)*
3. Батюк О. В. Криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури: монографія. Луцьк: Волиньполіграф, 2021. 450 с.
4. Коломієць В. Через підрив Каховської ГЕС затоплені 32 об'єкти з хімікатами, нафтою та бензином – Greenpeace. URL: http://surl.li/ibepu *(дата звернення 02.10.2023 р.)*

УДК 342

Євген БЕРЕЖНИЙ
Аспірант, 1-го курсу спец. 081
Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авівційний інститут», м. Харків, Україна
e-mail: bereg_evg@ukr.net

ПУБЛІЧНО-ПРАВОВІ ЗАСАДИ БЕЗПЕКИ ТА СТАЛОГО РОЗВИТКУ ТРАНСПОРТУ

Анотація: розглянуто транспорт, як один із ключових об'єктів критичної інфраструктури, який впливає на економічний, суспільний, соціальний, політичний, культурний та інші напрямки розвитку держави. Виділено публічно-правові засади для забезпечення, регулювання та контролю за дотриманням правил та норм безпеки на транспорті. Визначено концепцію сталого розвитку в транспортному секторі.

Ключові слова: публічно-правові засади, сталий розвиток, транспорт, норми, покарання.

PUBLIC-LEGAL PRINCIPLES OF SAFETY AND SUSTAINABLE DEVELOPMENT OF TRANSPORT

Abstract: The article examines transport as one of the key critical infrastructure facilities that affects the economic, social, political, cultural and other spheres of state development. The

author highlights the public law principles of ensuring, regulating and monitoring compliance with transport safety standards and rules. The concept of sustainable development in the transport sector is defined.

Keywords: public law principles, sustainable development, transport, rules, sanctions.

Транспорт є одним із ключових об'єктів критичної інфраструктури, оскільки він грає важливу роль у функціонуванні суспільства та економіки [1]. Критична інфраструктура - це системи та об'єкти, без яких не може нормально функціонувати суспільство та економіка, і їх недолік може призвести до серйозних наслідків. Важливість транспорту як об'єкта критичної інфраструктури включає наступні аспекти:

- економічна важливість - транспортна інфраструктура забезпечує пересування товарів та послуг, сприяючи ефективному функціонуванню господарства. Відсутність або недостатність транспорту може призвести до зупинки постачання, втрати прибутків і зниження економічного зростання;

- важливість для національної оборони - транспортна інфраструктура грає важливу роль у забезпеченні можливостей для переміщення військ та забезпечення військових операцій. Вона також може використовуватися для евакуації населення в разі кризи або військового конфлікту;

- зв'язок між регіонами - транспорт дозволяє зв'язувати різні регіони країни та сприяти обміну людьми, товарами та послугами. Це сприяє соціальній та економічній інтеграції;

- громадська безпека - транспортні системи включають в себе пасажирський та вантажний транспорт, і вони мають важливе значення для громадської безпеки. Недоліки у безпеці транспорту можуть призвести до аварій, травм та загибелі людей;

- соціальна важливість - транспорт забезпечує доступ до освіти, медичних послуг, робочих місць та інших суспільних благ. Це має велике значення для якості життя громадян.

Оскільки транспортна інфраструктура є надважливою для суспільства та економіки, її збереження та захист від потенційних загроз, таких як природні катастрофи, терористичні акти або кібератаки, є важливим завданням національної безпеки. Тому влада в багатьох країнах приділяє велику увагу заходам з підвищення стійкості та безпеки транспортної інфраструктури.

Публічно-правові засади безпеки на транспорті визначаються законами та регуляторними актами кожної країни. Основні принципи та норми, які регулюють безпеку на транспорті, можуть включати такі аспекти:

1. Законодавча база - закони та правила, які стосуються безпеки на транспорті, визначають обов'язки та відповідальність учасників дорожнього руху, включаючи водіїв, пасажирів та пішоходів.

2. Сертифікація та ліцензування - учасники дорожнього руху, такі як водії, мають проходити обов'язковий процес сертифікації та ліцензування, щоб довести свою здатність безпечно керувати транспортними засобами.

3. Технічні стандарти - для транспортних засобів встановлюються технічні стандарти, які регулюють безпеку та якість транспортних засобів, включаючи технічний стан автомобілів, гальмівних систем, освітлення та інше.

4. Дорожні знаки та сигнали - для інформування та контролю дорожнього руху встановлюються дорожні знаки та сигнали, які надають водіям та пішоходам необхідну інформацію та вказівки.

5. Відповідальність та покарання - за порушення правил дорожнього руху передбачаються штрафи, судові санкції та інші види відповідальності для тих, хто не дотримується норм безпеки на транспорті.

6. Профілактика та освіта - з метою забезпечення безпеки на транспорті проводяться освітні кампанії та профілактичні заходи, спрямовані на підвищення обізнаності учасників дорожнього руху та зменшення аварійності.

7. Дорожній патруль та правоохоронні органи - для забезпечення дотримання правил безпеки на дорозі і вжиття заходів у разі порушень функціонують дорожні патрулі та правоохоронні органи.

Ці засади можуть різнитися в різних країнах та регіонах, але їх мета завжди одна - забезпечення безпеки учасників дорожнього руху та запобігання аваріям на транспорті. Дотримання цих засад є важливим завданням для збереження життя, майна та покращення загальної безпеки на дорозі [2, с. 95].

Концепція сталого розвитку на транспорті поєднує в собі забезпечення потреб сучасного та майбутнього поколінь у мобільності та перевезеннях, при цьому зменшуючи негативний вплив на довкілля та суспільство. Забезпечення сталого розвитку в транспортному секторі передбачає різні аспекти:

1. Зменшення викидів шкідливих речовин - для зменшення впливу транспорту на забруднення повітря та зміну клімату важливо переходити на чисті технології, такі як електричні автомобілі, гібридні транспортні засоби та використання відновлюваних джерел енергії.

2. Підтримка ефективного використання ресурсів - сталий розвиток вимагає оптимізації використання транспортних ресурсів, таких як інфраструктура та пальне. Це може включати в себе впровадження інтелектуальних систем керування рухом та маршрутизації, що дозволяють зменшити затори та споживання пального.

3. Підтримка громадського транспорту - зменшення кількості особистих (приватних) автомобілів та сприяння використанню громадського транспорту може зменшити затори та негативний вплив на довкілля.

4. Розвиток інфраструктури для велосипедистів та пішоходів - покращення умов для велосипедистів та пішоходів сприяє зменшенню транспортних заторів та забрудненню повітря, а також поліпшує здоров'я населення.

5. Безпека на дорогах – зменшення аварій та травм на дорогах є важливою частиною сталого розвитку на транспорті. Це може бути досягнуто за допомогою поліпшення інфраструктури, збільшення обізнаності учасників дорожнього руху та зменшення швидкості руху в небезпечних ділянках доріг [3, с. 248].

6. Планування та управління міським рухом – ефективне міське планування та управління рухом може зменшити транспортні затори, поліпшити доступність громадського транспорту та зменшити негативний вплив на середовище.

Сталий розвиток на транспорті вимагає спільних зусиль громадян, бізнесу та уряду для створення ефективної, економічної та екологічно збалансованої системи транспорту. Усі зазначені вище аспекти повинні бути урегульовані законодавчо, чітко прописано норми та їх дотримання, а також міра покарання у випадку не відповідності. Така концепція допоможе забезпечити ефективне використання транспорту з точки зору забезпечення національної безпеки, підвищення мобільності, економічного зростання країни, забезпечення потреб сучасного суспільства без шкоди для майбутніхпоколінь та захисту довкілля.

Список використаних джерел:

1. Петровський, Д. Як вітчизняний транспорт допоміг вижити українській економіці та її громадянам під час війни [Електронтй ресурс]. – Режим доступу: https://www.unian.ua/economics/transport/yak-vitchiznyaniy-transport-dopomig-vizhiti-ukrajinskiy-ekonomici-ta-jiji-gromadyanam-pid-chas-viyni-12105600.html

2. Бойко А. В. Адміністративно-правове забезпечення державної транспортної політики в Україні / Дис. на здоб. наук. ступ. д.ю.н. Дніпропетровський державний університет внутрішніх справ. Київ, 2021. 480 с. https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/new_d0872702/37_5/d.pdf

3. Бережна Н. Г. Превентивні заходи як фактор безпеки учасників дорожнього руху / Н.Г. Бережна, Є.В. Бережний // Матеріали 1ої Міжнародної науково-практична конференції “Підвищення надійності машин і обладнання. Increase of Machine and Equipment Reliability”, 17-19 квітня 2019 р. – Кропивницький: ЦНТУ, 2019. – С. 248-249.

УДК 342
Світлана БИЧКОВА
докторка юридичних наук, професорка
провідна наукова співробітниця,
Науково-дослідний інститут приватного права і підприємництва
імені академіка Ф. Г. Бурчака НАПрН України, м. Київ, Україна
e-mail: civilkafedra@gmail.com, ORCID: 0000-0002-8227-2127

ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ЖИТТЮ А ЗДОРОВ'Ю ПРАЦІВНИКІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ЯК ОДНА ІЗ ГАРАНТІЙ ЇХ БЕЗПЕКИ

Анотація: Законодавством України передбачено відшкодування шкоди, завданої життю і здоров'я працівників об'єктів критичної інфраструктури при виконанні ними посадових (службових, професійних) обов'язків у період військової агресії проти України. При цьому у разі загибелі (смерті) зазначених осіб гарантується виплата відповідної одноразової грошової допомоги членам їхніх сімей. За результатами дослідження пропонується змінити законодавчий підхід до визначення таких членів сім'ї через внесення відповідних змін до відповідної правової норми.

Ключові слова: об'єкт критичної інфраструктури, працівник, відшкодування шкоди, одноразова грошова допомога, член сім'ї.

COMPENSATION OF DAMAGE CAUSED TO THE LIFE AND HEALTH OF EMPLOYEES OF CRITICAL INFRASTRUCTURE FACILITIES AS ONE OF THE GUARANTEES OF THEIR SAFETY

Abstract: The legislation of Ukraine provides for compensation for damage caused to the life and health of employees of critical infrastructure facilities during the performance of their official (official, professional) duties during the period of military aggression against Ukraine. At the same time, in the event of death (death) of the specified persons, the payment of the corresponding one-time monetary assistance to their family members is guaranteed. According to the results of the study, it is proposed to change the legislative approach to the definition of such family members by making appropriate changes to the relevant legal norm.

Keywords: critical infrastructure facility, employee, compensation, lump sum, family member.

У ч. 1 ст. 4 Закону України «Про критичну інфраструктуру» задекларовано, що захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України.

При цьому безпека критичної інфраструктури – це стан захищеності критичної інфраструктури, за якого забезпечуються її функціональність, безперервність роботи, відновлюваність, цілісність і стійкість (п. 1 ч. 1 цього Закону).

Гарантувати убезпечення наведених показників без працівників відповідних об'єктів, зрозуміло, є неможливим. Адже навіть в умовах поширення та запровадження високих технологій, штучного інтелекту і т.п., без людини, її знань, умінь, навичок, здатності керувати технологічними процесами, вчасно реагувати на порушення у роботі устаткування тощо, важко уявити стабільність критичної інфраструктури, її безпеку та сталий розвиток.

В умовах воєнного стану в Україні питання безпеки об'єктів критичної інфраструктури набувають неабиякої актуальності і становлять один із пріоритетів, що потребує постійної уваги та реагування на шляху до Перемоги нашої держави.

Але незалежно від акцентів щодо пріоритетності, змінених в умовах воєнних (бойових) дій, бомбардування, авіаударів та інших збройних нападів, незмінним залишається те, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю (ч. 1 ст. 3 Конституції України). При цьому відповідно до ч. 1 ст. 27 Основного Закону України одним із основних обов'язків держави залишається захист життя людини.

Зважаючи на указане, 20 березня 2023 р. було прийнято Закон України «Про одноразову грошову допомогу за шкоду життю та здоров'ю, завдану працівникам об'єктів критичної інфраструктури, державним службовцям, посадовим особам місцевого самоврядування внаслідок військової агресії Російської Федерації проти України» (далі – Закон), що, серед іншого, спрямований на підтримку деяких категорій осіб, які стали особами з інвалідністю у зв'язку з пораненням, каліцтвом, контузією або внаслідок захворювання, пов'язаних з виконанням посадових (службових, професійних) обов'язків у період військової агресії проти України, а у разі загибелі (смерті) зазначених осіб – на підтримку членів їхніх сімей.

Наявність такої допомоги з боку держави допомагає працівникам об'єктів критичної інфраструктури бути впевненими у тому, що у разі настання відповідних негативних наслідків для їх здоров'я і життя держава не залишить напризволяще їх та членів їхніх сімей. А це, своєю чергою, стимулює їх до сумлінного ставлення до забезпечення безпеки відповідних об'єктів.

З огляду на обмеженість обсягу цієї наукової розвідки звернімо в межах обраної тематики, спираючись на аналіз указаного законодавчого акта, на одне суперечливе і доволі сумнівне його положення.

Так, відповідно до ч. 2 ст. 1 Закону у разі загибелі (смерті) осіб, зокрема з числа працівників об'єктів критичної інфраструктури, у встановлених законом випадках одноразова грошова допомога за шкоду життю та здоров'ю призначається і виплачується членам їхніх сімей.

У ч. 3 цієї ж статті наведений перелік осіб, які належать до членів сімей загиблих (померлих) осіб і мають право на одноразову грошову допомогу за шкоду життю, у тому числі працівника об’єкта критичної інфраструктури.

При аналізі зазначеної норми викликає подив виокремлення двох категорій відповідних осіб: один із подружжя, який не одружився вдруге, і повнолітні діти. При чому останніх, навіщось, розподілили на три категорії: а) повнолітні діти, які навчаються за денною або дуальною формою здобуття освіти у закладах загальної середньої освіти, а також у закладах професійної (професійно-технічної), фахової передвищої та вищої освіти (у тому числі у період між завершенням навчання в одному із зазначених закладів та вступом до іншого закладу або у період між завершенням навчання за одним освітньо-кваліфікаційним рівнем та продовженням навчання за іншим, за умови що такий період не перевищує чотирьох місяців), до закінчення цих закладів освіти, але не довше ніж до досягнення ними 23 років; б) повнолітні діти, які не мають (і не мали) своїх сімей; в) повнолітні діти, які мають свої сім’ї, але стали особами з інвалідністю до досягнення повноліття.

Такий підхід законодавця є дещо дискримінаційним. Адже за таких умов відшкодування шкоди позбавлені особи, які мають свою сім’ю, або у випадку з повнолітніми дітьми, якщо вони не навчаються на момент подання заяви про виплату допомоги та не стали інвалідами до досягнення повноліття, навіть ті з них, які мали колись свою сім’ю.

По-перше, незрозумілим є позбавлення права отримати відшкодування за втрату життя особою під час забезпечення нею безпеки об’єкта критичної інфраструктури її близьких осіб тільки на тій підставі, що вони створили свою сім’ю. При цьому необов’язково, що після настання смерті відповідного працівника. По-друге, навіть якщо розглядати одноразову грошову допомогу як таку, яка спрямовується соціально незахищеним верствам населення, перелік, закріплений у ч. 3 ст. 1 Закону, не починає виглядати більш логічним. Адже другий з подружжя, який пережив померлого працівника і не створив сім’ї, необов’язково буде належати до соціально незахищених верств населення, повнолітня ж дитина померлого, яка стала особою з інвалідністю після досягнення повноліття, може бути майже повністю позбавлена засобів для забезпечення свого існування.

Можна і надалі намагатися прослідкувати логіку законодавця при формулюванні подібної норми або наводити приклади осіб, які більше за деяких потребують отримання допомоги у разі загибелі члена своєї сім’ї.

Між іншим, у ч. 2 ст. 38 Закону України «Про розвідку» застосовано інший підхід до визначення членів сім’ї та батьків співробітника кадрового складу, загиблого (померлого) у зв’язку з виконанням ним посадових

(службових) обов'язків, – вони визначаються відповідно до положень Сімейного кодексу України.

На наш погляд, у подібних випадках за основу слід брати те, що особа загинула (померла) за обставин, пов'язаних з виконанням її посадових (службових, професійних) обов'язків, тобто забезпечуючи функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури у період військової агресії проти України. Тому членам сім'ї будь-якого загиблого за таких обставин працівника об'єкта критичної інфраструктури, незалежно від того, чи мають вони свою сім'ю, чи є особами з інвалідністю, чи мають інші доходи, слід гарантувати однакове ставлення держави і наділяти їх правом на відшкодування шкоди, завданої смертю їх близької особи, за рахунок виплати відповідної одноразової грошової допомоги.

Лише у такому разі кожна особа буде відчувати піклування держави, її підтримку і відповідальність за життя кожної «своєї дитини».

У зв'язку із цим пропонується внести зміни до ч. 3 ст. 1 Закону, передбачивши, що до членів сімей загиблих (померлих) осіб, зазначених у ч. 1 цієї статті, належать, у тому числі, другий із подружжя, який пережив померлого, та діти (незалежно від віку, належності до осіб з інвалідністю і наявності у них своїх сімей).

УДК 349.22:331.106

Андрій БІЛОХА
здобувач вищої освіти, третій освітньо-науковий рівень доктор PhD кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна
e-mail:a.i.bilokha@khai.edu, ORCID: 0000-0002-0602-1297

ВИЗНАЧЕННЯ МОЖЛИВОГО РІВНЯ ДОСТУПУ ПРАЦІВНКІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У СФЕРІ ЕЛЕКТРОЕНЕРГЕТИКИ НА ЛОКАЛЬНОМУ РІВНІ ДО ДИСТАНЦІЙНОГО РЕЖИМУ ПРАЦІ

Анотація: Під час написання даних тез автором було досліджено питання важливості та значення критичної інфраструктури вцілому, досліджено нормативно-правові акти, якими регулюється діяльність операторів системи розподілу електричної енергії, як оператора критичної інфраструктури. Також розглянуто питання виведення певного кола працівників, які працюють у структурних підрозділах оператора системи розподілу електроенергії, на дистанційну форму праці.

Ключові слова: критична інфраструктура, оператор системи розподілу електричної енергії, електроенергетика, розподіл електричної енергії, дистанційна робота.

DETERMINATION OF THE POSSIBLE LEVEL OF ACCESS FOR EMPLOYEES OF CRITICAL INFRASTRUCTURE FACILITIES IN THE FIELD OF ELECTRICAL ENERGY AT THE LOCAL LEVEL TO THE DISTANCE WORK MODE

Abstract: During the writing of these theses, the author researched the issue of the importance and meaning of critical infrastructure as a whole, researched legal acts that regulate the activity of operators of the electric energy distribution system, as an operator of critical infrastructure. The question of transferring a certain number of employees working in the structural subdivisions of the electricity distribution system operator to a remote form of work was also considered.

Keywords: critical infrastructure, electric energy distribution system operator, electric power industry, electric energy distribution, distance work.

Вже більше року відважний український народ, його захисники боронять українську землю від російської агресії, яка спровокувала найкровопролитнішу війну в XXI столітті. Під прицілом російських загарбників опинилися не лише важливі об'єкти військової інфраструктури, а й цивільні люди, їх майно, а також не оминула жахлива участь знищення й об'єкти енергетичної інфраструктури. Ще 24-го лютого 2022 року Президентом України був підписаний Указ №64/2022, яким на всій території України було запроваджено воєнний стан. Цим Указом на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30 – 34, 38, 39, 41 – 44, 53 Конституції України. Проте збільшується пильність та приділяється більше уваги об'єктам критичної інфраструктури, так як вони мають велике значення для безперебійного, повного та якісного функціонування органів державної влади, як центральних, так і на місцях, органів місцевого самоврядування, Збройних сил України, Національної гвардії України, органів Національної поліції тощо.

Відповідно до п. 13 ч. 1 ст. 1 Закону України «Про критичну інфраструктуру» № 1882-IX від 16.11.2021 (далі – ЗУ «Про критичну інфраструктуру»), об'єктами критичної інфраструктури є 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. Згідно з ч. 1 ст. 9 ЗУ «Про критичну інфраструктуру», для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг

визначаються сектори критичної інфраструктури. Пунктом другим частини четвертої цієї ж статті енергозабезпечення (у тому числі постачання теплової енергії) віднесено до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України. П. 14 ч. 1 ст. 1 ЗУ «Про критичну інфраструктуру» передбачає визначення поняття оператора критичної інфраструктури, відповідно до якого оператор критичної інфраструктури - юридична особа будь-якої форми власності та/або фізична особа - підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування [1].

Темою дослідження даних тез є визначення можливого рівня доступу працівників об'єктів критичної інфраструктури у сфері електроенергетики на локальному рівні до дистанційного режиму праці.

Насамперед варто зазначити, що дане питання буде розглянуто в контексті діяльності операторів системи розподілу електричної енергії.

У відповідності до п. 56 ч. 1 ст. 1 Закону України «Про ринок електричної енергії» № 2019-VIII від 13.04.2017, оператором системи розподілу є юридична особа, відповідальна за безпечну, надійну та ефективну експлуатацію, технічне обслуговування та розвиток системи розподілу і забезпечення довгострокової спроможності системи розподілу щодо задоволення обґрунтованого попиту на розподіл електричної енергії з урахуванням вимог щодо охорони навколишнього природного середовища та забезпечення енергоефективності (далі – оператор системи) [2].

В обов'язковому порядку всі оператори системи діють на підставі ліцензії на право провадження господарської діяльності з розподілу електричної енергії, виданої відповідно до постанови Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг на території певного регіону, де оператор системи надає споживачам електричної енергії комунальні послуги з розподілу електричної енергії. У свою чергу розподілом електричної енергії вважається процес транспортування електричної енергії від електроустановок виробників електричної енергії до кінцевого споживача в загальному вигляді. При цьому комплекс робіт, які виконуються задля безперебійного розподілу електричної енергії достатньо широкий. До нього можна віднести і забезпечення транзитної системи, тобто нагляд за безперебійною роботою підстанцій, комплексних трансформаторних підстанцій, мереж транспортування електричної енергії, і облаштування електроустановок споживача, нагляд за безпечною роботою цих електроустановок, а також ведення договірної роботи з кінцевими споживачами – юридичними та фізичними особами.

Щодо внутрішньої структури операторів системи варто зазначити, що так як провадження діяльності з розподілу електричної енергії здійснюється в певних регіонах (здебільшого областях), то на місцях забезпечено наявність структурних підрозділів, які здійснюють вищезазначену діяльність в межах міст та районів. Таким чином, структуру оператору системи складає центральний офіс та структурні підрозділи (філії).

Метою даних тез є дослідження можливості введення для працівників структурних підрозділів оператора системи дистанційний режим праці.

Здебільшого робота працівників структурних підрозділів передбачає вчинення механічних дій і присутність на робочому місці або на об'єкті, проте є працівники, які мають можливість працювати віддалено, наприклад: інженери з договірної роботи, економісти, юрисконсульти та інші.

Проте специфікація виконання обов'язків особами, які займають дані посади, здебільшого унеможливлюють переведення їх на дистанційний режим роботи по ряду причин.

По-перше, вся робота таких працівників будується на вмінні користування програмним забезпеченням, яке спеціально створене для виконання певних завдань, і здебільшого ліцензіями на таке програмне забезпечення передбачено обмежену кількість пристроїв для підключення; по-друге, робота працівників, які обіймають вищезазначені посади, зав'язана на взаємодії зі споживачами, а тому вимагає присутності на спеціально створеному робочому місці для надання роз'яснень, відповідей на запитання, які поставлені такими споживачами; по-третє, оперативна взаємодія між працівниками є більш ефективною, коли усі працівники знаходяться в одному визначеному місці, таким чином вирішення робочих питань займає менше часу.

Також у даному випадку важливо оцінити можливість роботодавця в забезпеченні усім необхідним працівника для ефективного виконання останнім поставлених завдань.

Перш за все, варто зазначити, що у відповідності до ч. 1 ст. 60-2 Кодексу законів про працю України від 10 грудня 1971 року (далі – КЗпП України),дистанційною роботою є форма організації праці, за якої робота виконується працівником поза робочими приміщеннями чи територією роботодавця, в будь-якому місці за вибором працівника та з використанням інформаційно-комунікаційних технологій.

Цією ж статтею КЗпП України регламентується обов'язок роботодавця щодо забезпечення працівників, які виконують роботу дистанційно, необхідними для виконання ними своїх обов'язків обладнанням, програмно-технічними засобами, засобами захисту інформації та іншими засобами.

Проте, як буває досить часто, не на всіх підприємствах, де запроваджується дистанційна форма організації праці з тих чи інших причин, є можливість швидко акумулювати все необхідне обладнання і передати його працівнику для виконання роботи, так як здебільшого таке обладнання або не передбачене для частого транспортування з місця на місце, або таке транспортування є незручним, опираючись на технічні характеристики обладнання [3].

При цьому взагалі виключати можливість переведення таких працівників на дистанційний режим праці все ж таки непотрібно. Наразі державою створюються умови для вирішення будь-яких питань в режимі «online»: створюються спеціальні електронні сервіси по типу «Дії», максимально цифровізуються дані, які досі подаються в паперовому вигляді, створюються електронні реєстри, кабінети користувачів, розширюється спектр послуг, які можливо надавати без особистої присутності замовника і виконавця таких послуг.

Таким чином, можна зробити висновок, що наразі запровадження дистанційної форми праці для працівників структурних підрозділів операторів системи неможливе і неефективне з огляду на те, що задля забезпечення безперебійної й стабільної діяльності критичної інфраструктури у сфері електроенергетики, потрібна акумуляція працівників в одному визначеному місці.

Список використаних джерел:

1. Про критичну інфраструктуру, Закону України від 16.11.2021 № 1882-IX. Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#n118(дата звернення 28.10.2023).

2. Про ринок електричної енергії, Закону України від 13.04.2017 № 2019-VIII. Редакція від 03.09.2023. URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text (дата звернення 28.10.2023).

3. Кодекс законів про працю України, Кодекс України від 10.12.1971 № 322-VIII. Редакція від 01.10.2023. URL :https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення 28.10.2023).

УДК 347.732
Алевтина БІРЮКОВА
докторка юридичних наук, доцентка кафедри цивільно-правової політики, інтелектуальної власності та іновацій, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: a.g.biryukova@nlu.edu.ua, ORCID: 0000-0002-2786-543X

ОСОБЛИВОСТІ ПРАВОВОЇ ПРИРОДИ ЛІЗИНГОВИХ ПРАВОВІДНОСИН ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА ДЕЯКИХ КРАЇН ЄВРОПИ

Анотація: Загальновідомо, що лізингові операції є важливим та досить поширеним інструментом економічної діяльності у багатьох країнах світу. Лізингові договори дуже поширені як в США, так і країнах Європи. Ринкові перетворення, що відбуваються в українській економіці, потребують вдосконалення існуючих та пошуку нових форм фінансування капітальних вкладень. Нетрадиційним фінансовим інструментом для вітчизняної практики є лізинг. Він довів свою ефективність у відновлені та розвитку суб‘єктів господарювання провідних країн.Доинамічність розвитку та зростання уваги до сектору лізингових договорів обумовлені тим, лізинг є одним із засобів оптимізації виробничих потужностей та оновлення основних фондів підприємств що , в свою чергу, підвищує якість виробництва та розвиток економіки в цілому.

Ключові слова: Лізингові правовідносини,основні фонди, Європейське законодавство.

FEATURES OF THE LEGAL NATURE OF LEASING RELATIONS UNDER THE LEGISLATION OF UKRAINE AND SOME EUROPEAN COUNTRIES

Abstract: The purpose of this research is to clarify the features of lease agreement under national law and in comparison with the current of European countries in this area.The authors used general scientific and methods of scientific cognition.Under national law, the legal structure of the lease agreement is quite complex,as it combines elements of sale and lease.

Keywords: leasing agreements,civil legislation, European legislation.

На рівні національного законодавства зобов’язання, що виникають на підставі договору лізингу врегульовані нормами ЦКУ , а також Законом України «Про фінансовий лізинг». Основними різновидами лізингу в Україні є фінансовий та оперативний. На сьогодні останній є все менше застосовується , адже логічним те, що суб’єкти господарювання, які є лізингоодержувачами зацікавлені в подальшому викупі такого майна, в той час як відповідно лізингодавець може реалізувати кошти, отримані внаслідок фінансового лізингу методом інвестування в іншій сфері господарської чи іншої діяльності. Ще однією особливістю оперативного лізингу є те, що майну, яке на його

підставі договору передається у користування, властиве багаторазове використання на строк, що є значно меншим, ніж термін його можливої служби.

Цілком характерно на початковому етапі розвитку лізингу є впровадження та розвиток саме фінансового його виду, оскільки клієнти здебільшого зацікавлені в отриманні предмета лізингу у власність наприкінці дії договору лізингу. Використання класичного фінансового лізингу зумовлюється його структурою та перевагами. Лізингодавці найбільше зацікавлені в лізингу високоліквідного обладнання, яке можна легко повернути та перепродати. Яскравим прикладом цього є автомобілі. У портфелях більшості лізингових компаній автомобілі зазвичай є домінуючим предметом фінансового лізингу. Лізинг легкових автомобілів, безумовно, є найбільш розвинутою частиною українського ринку. Другим найбільш розвиненим сектором є сільське господарство. У 2021 році надано в лізинг 650 одиниць сільськогосподарської техніки.

Досвід більш зрілих ринків пропонує типовий сценарій розвитку ринку. Лізинг, як правило, починається з укладання лізингових угод напряму з клієнтами щодо матеріальних та високоліквідних активів. Далі розробляють перші спеціальні (вендорні) програми між виробниками та лізингодавцями. З часом схема вендорного фінансування стає популярною щодо всіх матеріальних активів, і чимало виробників пропонують «готове рішення»; не лише фізичний актив, а й фінанси, послуги, технічне обслуговування та страхування. Співпраця між виробником та лізингодавцем налагоджена у такий спосіб, що компанія, яка фінансує, використовує логотип постачальника, а покупець отримує комплексну послугу продавця без потреби в укладенні окремого договору з лізинговою компанією. З часом вендорні програми розробляють не лише для типових матеріальних активів, але і для нематеріальних активів.

Далі пропонуємо проаналізувати правила, за якими будуються лізингові відносини у ряді країн Європи. Так, варто зазначити, що Іспанія у своєму законодавстві закріплює, що договір фінансового лізингу обов'язково включає в себе право викупу для користувача після завершення договору. До того ж, правова природа лізингових відносин в Іспанії є досить невизначеною, на відміну від України, і дуже багато положень договору залишаються на затвердження їх сторонами., але тільки у випадку, що за умови що загальні рамки, встановлені законом, мораллю і нормами громадського порядку не були перевищені, оскільки в іншому випадку відповідні положення будуть визнані недійсними. У випадку договорів нефінансового лізингу немає визначення (крім загального), і так званий оперативний лізинг не згаданий

конкретно в законодавстві, крім загальних правил, що містяться в Цивільному кодексі.

Відповідно до португальського права фінансовий лізинг є угодою, за якою лізингодавець отримує винагороду за те, що поступається лізингоодержувачу своїм правом на використання активу, придбаного чи виготовленого за прямою вказівкою лізингоодержувача, який може бути викуплений лізингоодержувачем після закінчення строку дії договору за попередньо визначеною ціною. В оперативному лізингу використання активу є домінуючою характеристикою. Актив надається лізингоодержувачу на визначений період часу за визначену ціну. В обох випадках право власності належить лізингодавцю до моменту викупу предмета лізингу лізингоодержувачем або третьою особою. Що стосується фінансової лізингової діяльності, то португальський резидент-лізингодавець є об'єктом контролю та нагляду з боку Португальського центрального банку та має отримати ліцензію для того, щоби здійснювати діяльність як фінансова установа. Усі юридичні особи, правомочні на здійснення фінансових лізингових операцій, регулюються правовим режимом фінансових установ і є, відповідно, об'єктами регуляторних обмежень, як, наприклад, мінімальний установчий капітал, відповідальність акціонерів чи ради правління.

Згідно з п. 89 ч. 1 ст. 1 Закону Угорщини «Про кредитні спілки та фінансові установи» фінансовий лізинг означає правочин, за яким лізингоодержувач набуває правового титулу використання на праві власності рухомого майна або нерухомості, або право від лізингодавця на визначений період часу, відповідно до якого лізингоодержувач: несе всі ризики, що випливають з передачі майна; отримує право на доходи від майна; несе прямі витрати (в тому числі на технічне обслуговування, внаслідок знецінення майна та амортизаційні відрахування); отримує право на передачу йому майна, що є предметом лізингу, у приватну власність – чи на передачу цього права іншій особі – зі спливом строку лізингу, передбаченого у договорі, після сплати основної суми і відсотків у повному обсязі, а також після виплати залишкової вартості, передбачених у договорі.

Отже, проаналізувавши лізингові правовідносини, які знаходяться в процесі формування відповідно до українського законодавства та законодавства країн Європи, можна прийти до висновку, що на сьогоднішній день Україна потребує серйозних змін, зокрема, ми пропонуємо сконцентрувати увагу законодавця на формах реалізації саме фінансового лізингу, адже в умовах розвинку сучасної України потреба в реглюванні оперативного лізингу не є нагальною.

Список використаних джерел:

1. Габріадзе М.Р. Правове регулювання договору лізингу за законодавством України. Науковий вісник публічного та приватного права.Вип.5.Т.1.2019.ст.47-52.
2. Осадко А.С. Правове регулювання лізингових відносин за участю сільськогосподарських товариств. Збірник тез. 2016.Харків
3. Правове регулювання лізингу:досвід Іспанії, Португалії, Болгарії та Угорщини. https:/feao.org.ua/wp/content/uploads/2017/01/FEAO leasing.pdf [in Ukrainian].

УДК 347.1

Тетяна БРОВЧЕНКО
кандидатка юридичних наук, асистентка кафедри цивільно-правової політики, права інтелектуальної власності та інновацій Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна
e-mail: t.i.brovchenko@ nlu.edu, ORCID: 0000-0002-2095-8887

ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: Доповідь присвячена дослідженню терміну «критична інфраструктура», історії появи зазначеного терміну тайого визначення в європейській практиці, а також сучасне визначення об'єктів критичної інфраструктури згідно чинного законодавства України.

Ключові слова: Об'єкти критичної інфраструктури, життєво важливі інтереси, національна безпека, критична інфраструктура.

OBJECTS OF CRITICAL INFRASTRUCTURE

Abstract: The report is devoted to the study of the term "critical infrastructure," history of the appearance of this term and its definition in European practice,as well as a modern definition of objects of critical infrastructure in accordance with current legislation

Keywords: objects of critical infrastructure, vital interests, national security, critical infrastructure.

Ще на початку VII ст. до н.е. один із найвідоміших давньокитайських філософів Сунь Цзи у славнозвісному трактаті «Мистецтво війни» визначив п'ять найвагоміших в означеному контексті об'єктів, які мають ризик бути знищеними ворогом, – це людські ресурси потенційного супротивника, його запаси, обози, склади й загони.[1] Поняття «критична інфраструктура» також формувалося з давніх часів. Чи не першим застосував термін «інфраструктура» Сократ (V ст. до н.е.). «Для того, щоб людина існувала, – стверджував давньогрецький філософ, – їй потрібні тили, які надає суспільство: безпека, соціальний порядок і господарські товари. Однак це вона може отримати в тому випадку, якщо буде поважати концепт суспільства та

власні обов'язки. Основними із цих обов'язків є забезпечення *інфраструктури* (курсив наш. – *авт.*) та послуг, наданих суспільством» [2].

Термін «критична інфраструктура» вперше з'явився у директиві PDD-63 *(Presidential Deci- sion Directive),* яка була підписана президентом Сполучених Штатів Америки Б. Клінтоном у 1996 році. Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі. І найголовніше, закладено вимогу щодо забезпечення безпеки критичних елементів інфраструктури. Згодом питанням критичної інфраструктури та її безпеки почали приділяти увагу в інших країнах, зокрема: Німеччині, Великій Британії, Нідерландах, Чеській Республіці, Словаччині, Польщі, Угорщині та ін. Важливим у цьому про- цесі є те, що у деяких національних законодавствах при визначенні терміна «критична інфраструктура» акцентовано на функціях та послугах. Саме функції та послуги об'єктів критичної інфраструктури, якими забезпечують суспільство, бізнес та державу, є в основі визначення їх критичності, що дає методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту [3, с. 6]. Європейський Союз визначає критичну інфраструктуру як систему, що має вагоме значення для підтримання життєво важливих соціальних функцій. Країни – члени Євросоюзу констатували, що пошкодження критичної інфраструктури, її руйнування або порушення внаслідок стихійних лих, тероризму, злочинної діяльності чи зловмисної поведінки може негативно вплинути на безпеку ЄС і добробут громадян [4].

Одними з перших у Європі розпочали визначати й захищати свою національну критичну інфраструктуру Федеративна Республіка Німеччина й Велика Британія (з 1991 р. та 1999 р. відповідно), де було створено в цей час Федеральне відомство інформаційної безпеки ФРН і Координаційний центр з безпеки національної інфраструктури Великої Британії. Федеральне відомство інформаційної безпеки ФРН невдовзі перейшло до структури МВС країни, з 1998 р. й донині воно є провідним федеральним органом з питань інформаційної безпеки у сфері захисту критичної інфраструктури. Відомство визначило дев'ять секторів критичної інфраструктури за такими галузями: енергетика (електрика, газ, нафта); вода (громадське та комунальне водопостачання); харчування (харчова промисловість, торгівля харчовими продуктами, забезпечення населення доброякісною їжею); інформаційні технології та комунікації; здоров'я (медичне обслуговування, лікарські засоби й вакцини, діагностика та лабораторні дослідження); фінанси і страхування (банки, біржі, страхові компанії, провайдери фінансових послуг); транспорт

(авіація, морське судноплавство, внутрішнє судноплавство, залізничний транспорт, автомобільний транспорт, логістика); держава й адміністрація (уряд та адміністрація, парламент, судові органи, служби екстреної допомоги, зокрема цивільний захист); ЗМІ та культура (радіо, телебачення, друкована й електронна преса, культурна спадщина, пам'ятки архітектури). З огляду на інтенсивне використання інформаційних технологій, до критичної інфраструктури належить також інформаційна інфраструктура [5].

Спершу дев'ять, а згодом – 13 національних секторів КІ визначено у Великій Британії: хімічна галузь, промисловість, оборона, цивільні ядерні комунікації, надзвичайні служби, енергетика, фінанси, продовольство, уряд, охорона здоров'я, космос, вода і транспорт [6].

У межах національної інфраструктури Франції до КІ належать 12 секторів, а саме: громадське управління; збройні сили; судочинство; сільське господарство; електронні комунікаційні системи; аудіо- та відеоінформаційні технології; енергетика, космос і дослідницька діяльність; фінансовий сектор; вода; громадське здоров'я; транспорт і промисловість [7].

В Іспанії КІ охоплює такі сфери: фінанси, електростанції та мережі, зв'язок, сектор охорони здоров'я, продовольство, водосховища, транспорт, аеропорти, морські й інші порти, пам'ятки національних меншин, виробництво, зберігання і транспортування небезпечних вантажів (хімічного, біологічного або ядерного матеріалу).

У Данії, на відміну від інших країн, замість поняття критична інфраструктура використовують словосполучення «критичні функції для суспільства». До них належать такі види діяльності, товари й послуги, що забезпечують стале функціонування суспільства й потребують підтримання та відновлення в разі аварій або катастроф. Зазначені функції зосереджено здебільшого в секторах енергетики, транспорту, інформаційних технологій, телекомунікацій, хімічної промисловості тощо [7].

В Україні критична інфраструктура визначається як сукупність об'єктів критичної інфраструктури. В Законі України Про критичну інфраструктуру, а саме п.13,ч.1,ст.1 визначає об'єкти критичної інфраструктури - 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. Віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю

яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами.

Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що 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. До таких критеріїв належать законодавець відносить:

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 [8].

В ЗУ Про критичну інфраструктуру визначається 4 категорії критичності, в залежності від рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури в залежності від рівня їх важливості для забезпечення окремих життєво-важливих функцій саме:

І категорія критичності - особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

ІІ категорія критичності - життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

ІІІ категорія критичності - важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

IV категорія критичності - необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення [8].

З метою проведення аналізу можливих основних загроз та потенційних негативних наслідків для об'єктів критичної інфраструктури, запобігання та попередження виникнення таких загроз для критичної інфраструктури оператори об'єктів критичної інфраструктури готують і подають на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, відповідного функціонального органу паспорт безпеки на кожний об'єкт критичної інфраструктури. Паспорт безпеки на об'єкт критичної інфраструктури містить інформацію про ідентифікацію об'єкта та заходи щодо його захисту і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв'язок та обмін інформацією з суб'єктами національної системи захисту критичної інфраструктури. Відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом [8].

Список використаних джерел:

1. Сунь-цзи, У-цзи. Мистецтво війни./ пер. з кит. Сергій Лесняк. Видавництво Старого Лева, 2015. 112 с.

2. Fertis D.G., Fertis A. Historical evolutions of infrastructure: 15,000 Years of History. New York: Vantage Press Inc., 1998. 191 p.

3. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. К. : НІСД. 2016. 176 с.

4. European Programme for Critical Infrastructure Protection (EPCIP). URL: https://ec.europa.eu/home-affairs/e-library/glos sary/european-programme-critical_en ; Council

Directive 2008/114/E Cof 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.europa.eu/legal-con tent/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

5. BSI-kritisverordnung (BSI – kritisV). URL: http://www.buzer.de

6. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для Украї- ни : монографія. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2018. С. 24–25.

7. Підюков П.П., Калиновський О.В. Система державного захисту критичної інфраструктури України: генеза, сучасний стан і перспективи оптимізування в умовах подальшого забезпечення національної безпеки України. *Часопис Київського університету права*. 2020. Вип. 4 С. 355-359

8. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. No 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 2.11.2023).

УДК 347.822.4

Алла ГОРДЕЮК
кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: a.hordeiuk@ khai.edu, ORCID: 0000-0001-7423-3673

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ АВІАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Анотація: У роботі проаналізовано нормативні акти, в тому числі прийняті під час воєнного стану в державі, що становлять правове забезпечення безпеки авіації, окреслено її сучасний стан. Зазначено на економічні проблеми в авіаційній сфері, які можливо в повній мірі подолати шляхом поновлення польотів літаків українських авіакомпаній тільки за умовами гарантування максимального захисту таких об'єктів критичної інфраструктури як аеропорти (аеродроми) із дотриманням норм чинного повітряного законодавства України.

Ключові слова: авіаційна галузь, безпека авіації, державна авіація, цивільна авіація, правове забезпечення безпеки авіації, безпека аеропортів (аеродромів), воєнний стан.

THE PROBLEM OF ENSURING AVIATION SAFETY UNDER MARTIAL LAW IN UKRAINE

Abstract: This article analyzes the regulations, including those adopted during the period of martial law in the state, which constitute the legal support for aviation safety, and determines its current state. Economic problems in the aviation sector are pointed out, which can be overcome by resuming flights of Ukrainian airlines, but only with the condition of guaranteeing maximum protection of airports (airfields), observing the norms of the current air legislation of Ukraine.

Keywords: aviation sector, aviation safety, national aviation, Civil aviation, legal support for aviation safety, airport security (airfield), martial law.

Авіаційна галузь є складовою частиною транспортної системи в Україні, яка пов'язана із використанням повітряного простору і її сталий розвиток

визнається в нашій країні як один із найважливіших напрямів в економічному розвитку держави, що було передбачено Національною транспортною стратегією України на період до 2030 р. Враховуючи велике значення авіаційного сектору, забезпечення його безпеки як об'єкта критичної інфраструктури, є першочерговим завданням у мирний час, а тим більш під час воєнного стану, в якому на сьогодні перебуває України з 24 лютого 2022 р. у зв'язку з військовою агресією РФ.

У період правового режиму воєнного стану, що був введений Указом Президента України від 24.02.2022 р. № 2102-IX «Про введення воєнного стану в Україні», з метою забезпечення безпеки авіації, зокрема у сфері цивільної авіації, Державне підприємство з обслуговування повітряного руху України (ДП «Украероруx») 24 лютого 2022 р. призупинило надання послуг з обслуговування повітряного руху в Україні через високий ризик використання повітряного транспорту. А вже 28 лютого 2022 р. ДП «Украероруx» повідомило про настання форс-мажорних обставин через широкомасштабну воєнну агресію РФ проти України, унаслідок чого виконання договорів, контрактів, угод та інших актів у сфері авіаційної діяльності стало неможливим [1; 2]. Таким чином, небо для українських авіакомпаній було закрито, українську цивільну авіацію «приземлили».

У свою чергу Міністерство інфраструктури України видало Наказ від 10.05.2022 р. № 304 «Про забезпечення здійснення протягом періоду воєнного стану в Україні позапланових заходів державного нагляду (контролю) за дотриманням вимог законодавства у галузі цивільної авіації та використання повітряного простору України» [3].

Управління системою авіаційної безпеки здійснює структурний підрозділ Державної авіаційної служби України (далі – ДАСУ), який безпосередньо підпорядковується Голові ДАСУ. Важливою в умовах воєнного стану є Директива ДАСУ з забезпечення діяльності цивільних аеродромів та суб'єктів наземного обслуговування під час воєнного стану в Україні та після його припинення. Директива розроблена узв'язку з унеможливленням виконання у повній мірі експлуатантами цивільних аеродромів та суб'єктами наземного обслуговування в умовах правового режиму воєнного стану та ведення бойових дій на території України вимог діючих авіаційних правил України щодо діяльності цивільних аеродромів та суб'єктів наземного обслуговування [4].

У даному контексті доцільно зазначити, що у Повітряному кодексі України (далі – ПКУ) законодавець виділяє державну та цивільну авіацію (ч. 4 ст. 4 ПКУ). Державна авіація – авіація, що використовує повітряні судна з метою виконанням функцій із забезпечення національної безпеки і оборони

держави та захисту населення, які покладаються на Збройні Сили України, інші військові формування, утворені відповідно до законів України, Міністерство внутрішніх справ України, Національну поліцію України, Службу безпеки України, центральний орган виконавчої влади, що реалізує державну політику у сфері цивільного захисту, органи охорони державного кордону України, митні органи (п. 30 ч.1 ст. 1, ч. 4 ст. 4 ПКУ). Цивільна авіація – авіація, яка використовується для задоволення потреб економіки і громадян у повітряних перевезеннях і авіаційних роботах, а також для виконання польотів у приватних цілях (п. 102 ч.1 ст.1, 4 ч. ст. 4 ПКУ). Із наданих вище понять виходить, що призначення державної авіації полягає зокрема, у забезпечені безпеки цивільної авіації, при цьому поняття державної авіації було змінено законодавцем за однією із останніх на сьогодні редакцій від 29.06.2023 р, тобто під час війни. Відповідно до п. 20 ч. 1 ст. 1 ПКУ безпека авіації – це стан галузі цивільної авіації, за якого ризик завдання збитків людям чи майну знижується до прийнятого рівня у результаті безперервного процесу визначення рівня небезпеки і керування ним та утримується на такому рівні, або знижується далі, у сфері безпеки польотів, авіаційної безпеки, охорони навколишнього природнього середовища, економічної безпеки та інформаційної безпеки [5].

Спираючись на норми вище зазначених нормативних актів, можна зробити висновок, що правове забезпечення безпеки авіації було створено за рахунок видання нових нормативних актів або внесення змін у чинне повітряне законодавство, але на сьогодні актуальним є питання щодо відновлення пасажирських авіарейсів в Україні, чи можливо це здійснювати в умовах загрози ракетних ударів по всій території нашої держави? Чому взагалі постає таке питання, враховуючи всі загрози?

Ще до початку російського вторгнення у лютому 2022 р. в українській авіації спостерігалася криза, яка почалася через пандемію COVID-19 у 2020 р., коли через карантинні обмеження авіакомпаніям всього світу довелося скоротити кількість рейсів або взагалі припинити польоти, що потягнуло значні економічні збитки. Після початку військової агресії РФ, як вже було зазначено, українська цивільна авіації опинилася у стані «приземлення», а небо України закритим, хоча частині українських авіакомпаній вдалося евакуювати свої літаки, що дозволило їм заробляти шляхом передання їх в оренду разом с персоналом європейським авіакомпаніям. Тепер українські літаки (наприклад компанії SkyUp, що зустріла війну на думку експертів найбільш підготовленою) літають у Європі та «зазіхають» на Азію і Південну Америку, що стало можливим, дякуючи підписанню Угоди про спільне небо між Україною та ЄС(Угода між Україною, з одної сторони, та Європейським

Союзом, з іншої сторони, про спільний авіаційний простір від 12.10.2021). Однак більшість авіакомпаній у занепаді, зокрема у стані простою весь повітряний флот «Windrose» та частина флоту МАУ й AzurAirУкраїна, при цьому багато людей опинилися без роботи або не отримають заробітну плату.

Отже, щоб якось виправити край негативну економічну ситуацію в українському авіаційному секторі, і постало питання про можливість поновлення польотів українських бортів. Зокрема мала місце заява керівника компанії Ryanair щодо можливості здійснення польотів цивільної авіації в Україні, які можуть вилітати з аеродромів Львова або Ужгорода. Експерти вважають, що розконсервація польотів можлива у короткі строки, але головним є питання забезпечення безпеки аеропортів та польотів. Так, на думку речника командування Повітряних сил ЗСУ Юрія Ігната, відновлення пасажирських авіарейсів в Україні під час воєнного стану малоймовірне, оскільки загроза ракетних ворожих ударів є по всій території держави, а домовленості щодо створення гуманітарних авіаційних коридорів він вважає неможливими. Всі аеродроми на сьогодні в країні є оперативними, також край проблемним є вирішення питання для держави, що воює, страхування бортів і пасажирів [6].

Отже, враховуючи вище наведене можна підсумувати, по-перше, що в Україні на сьогодні прийняті необхідні оперативні міри з убезпечення цивільної авіації шляхом заборони польотів літаків цивільної авіації, а також були прийняті необхідні, під час воєнного стану, нормативні акти або внесенні відповідні зміни у ті, що були чинними до початку військової агресії РФ, які становлять правове забезпечення авіаційної безпеки у державі. Зокрема зауважено на зміни у понятті державної авіації, що прописано у п. 30 ч. 1 ст.1 ПКУ та у ч. 4 ст. 4 ПКУ, і зроблено висновок, про те, що її призначення, в тому числі, полягає у забезпечені безпеки цивільної авіації, виходячи із змісту зазначених норм [5].

По-друге, щодо відновлення польотів літаків цивільної авіації в Україні, то на наш погляд, це має статися тільки після припинення воєнних дій, тому що гарантувати в умовах постійних обстрілів з боку ворожої держави повну безпеку споживачів послуг цивільної авіації, авіаційного та наземного персоналу, об’єктів критичної інфраструктури, зокрема таких як аеропорти, аеродроми ані органи державної влади, ані державна авіація, ані чинні норми національного законодавства, що регламентують питання авіаційної безпеки, ані будь-які способи цивільного захисту на жаль не здатні, до того ж не спрацює й інститут страхування, враховуючи високий рівень ризиків.

Список використаних джерел:

1. Указ Президента України № 64/2022 «Про введення воєнного стану в Україні»від 24.02.23. р. URL: https://president.gov.ua/documents/642022-41397 (дата звернення 25.10.2023).
2. Як зараз живе українська цивільна авіація.URL. https://delo.ua/transport/krute-pike-yak-zaraz-zive-ukraynska-civilna-aviaciy-i-yak-svidco-vidnovlyatsya-polyoti-pislya-viini-421919/.
3. Про забезпечення здійснення протягом періоду воєнного стану в Україні позапланових заходів державного нагляду (контролю) за дотриманням вимог законодавства у галузі цивільної авіації та використання повітряного простору України: НаказМіністерства інфраструктури України від 10.05.22 № 304URL. https//mtu.gov.ua/documents/2284.html(дата звернення 25.10.2023).
4. Директива ДАСУ з забезпечення безпеки діяльності цивільних аеродромів та суб'єктів наземного обслуговування під час воєнного стану в Україні та після його припинення (SafetyDirective) AGA.SD-05-2022. URL.https//avia.gov.ua/wp-content/uploads/2022/08/AGA.SD-05-2022.pdf (дата звернення 27.10.2023).
5. Повітряний кодекс України19.05.2011 р. № 3393-VI. Редакціявід 21.10.2023 № 3232-IX (дата звернення 27.10.2023).
6. Цивільні авіарейси під час війни.URL.https://supsline.media/amp/538511-dolitae-usudi-u-povitranih-silah-zasteregli-vid-vidnovlenna-civilnoi-fviacii-pid-cas-vijni/.

УДК378:356:355

Ігор ГУБАРЄВ
здобувач вищої освіти другого освітньо-наукового рівня (магістр)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут» , м. Харків, Україна
e-mail: i.o.hubariev@student.csn.khai.edu
Науковий керівник
Вячеслав ХАРЧЕНКО
доктор технічних наук, професор,завідувач кафедри комп'ютерних систем і мереж
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: v.kharchenko@csn.khai.edu, ORCID: 0000-0001-5352-077X

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОПЕРЕДЖЕННЯ ТЕРОРИСТИЧНИХ АТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Характерними рисами розвитку сучасного світу є глобалізація, полікультурність, динамічність розвитку і в той же час нестабільність. За останні кілька років актуалізувалися найбільше серйозні проблеми міжнародного масштабу: економічний криза, локальні війни, що впливають на

сусідні країни, використання глобальної інформаційної мережі Інтернет для пропаганди поглядів терористично налаштованих особистостей та організацій.

Найбільш небезпечними та руйнівними наслідками визначаються терористичні акти, пов’язані із застосуванням зброї, бойових припасів чи вибухових речовин, оскільки створюють реальну загрозу для життя та здоров’я людей, спричиняють руйнування промислових, господарських чи оборонних об’єктів. Складність розслідування названих злочинів обумовлена наступним: стрімкою появою новітніх розробок у сфері озброєння; слабкістю системи контролю переміщення зброї, бойових припасів; корупційні прояви, недоліки організаційно-господарської діяльності в Збройних силах України; великі прогалини у національно-патріотичному вихованні населення; зростання стресового та психологічного навантаження на суспільство, виникнення панічних настроїв, що породжуються наявністю негативних військових, економічних та соціальних чинників; діяльність великої кількості неформальних об’єднань військового типу; збільшення суспільних тенденцій до силового вирішення конфліктів, розповсюдження проявів жорстокості та насилля; низька скоординованість дій силових структур при проведенні антитерористичних операцій; наявність великої бази даних із відкритих масивів Інтернету щодо створення та використання зброї та вибухових пристроїв; наявність у вільному доступі засобів так званого «подвійного» призначення, які можна використовувати як компоненти до створення саморобної зброї чи вибухових пристроїв; значною поширеністю в Інтернеті сайтів із відвертою екстремістської ідеологією тощо [1, с. 189].

Особливою вразливістю щодо терористичних посягань були й будуть об’єкти критичної інфраструктури, посягання на які несе найбільш руйнівний ефект. Саме тому 17 лютого 2017 року Рада Безпеки Організації Об'єднаних Націй одноголосно прийняла резолюцію № 2341 про захист критично важливих об'єктів інфраструктури та розширення можливостей держав щодо запобігання нападам на критично важливі об'єкти інфраструктури та закликала держав-членів протистояти небезпеці терористичних атак на них. У глобальній контртерористичній стратегії ООН, у рамках Розділу II «Заходи боротьби з тероризмом та його запобіганню», держави-члени вирішили «активізувати всі зусилля щодо підвищення безпеки та захисту особливо вразливих об'єктів, таких як інфраструктура та громадські місця, а також реагування на терористичні напади та інші лиха, зокрема в галузі цивільної оборони, визнаючи, що державам може знадобитися допомога для цієї мети [2].

У цьому контексті надійні та точні короткострокові прогнози щодо недержавного тероризму на місцевому рівні є ключовими для політиків щодо націлювання на превентивні заходи. Як зазначають вчені, дослідження збройних конфліктів і повстанців призвело до розробки прогностичних моделей, заснованих на теорії [3; 4], яка включає успішну дослідницьку програму, що застосовує можливості штучного інтелекту для прогнозування конфлікту в точному просторово-часовому масштабі [5, с. 50]. Проте ця важлива інформація, отримана в результаті дослідження збройних конфліктів, ще не знайшла свого шляху в дослідженні тероризму. Дослідження тероризму, загалом, зосереджено на пояснювальних моделях із застосуванням статистичних підходів для фіксації та кількісної оцінки ефектів рушійних сил терористичних атак у просторі та часі [6]. Отже, існує потреба в розробці придатної для інтерпретації моделі моделювання для прогнозування терористичних подій у точному просторовому та часовому масштабах, що може допомогти впроваджувати ефективні заходи та оцінювати та розвивати теорії у відповідних масштабах [7].

Доктор Андре Пайтон із Чжецзянського університету (Китай) разом із колегами знайшов спосіб покращити роботу штучного інтелекту у цій сфері. Вчені розробили структуру для прогнозування терактів у всьому світі, попередньо вивчивши випадки терористичних атак, які сталися в період з 2002 по 2016 роки (тобто протягом 795 тижнів) у 13 регіонах, включаючи всі субконтинентальні регіони, зазначені в Глобальній базі даних про тероризм (GTD), та Західну Африку. Для кожного регіону побудували прогностичні моделі, які дозволяють виявляти, оцінювати та порівнювати роль основних рушійних терористичних сил. Дослідники підготували деревоподібний алгоритм машинного навчання, що інтерпретується, з так званим градієнтним посиленням. Щоб охопити всі регіони світу, потенційно порушені тероризмом протягом тривалого періоду часу, автори розбили регіони на осередки, кожна з яких охоплює територію розміром 50 × 50 км і задали часовий параметр 795 тижнів. Далі в роботу включався деревоподібний алгоритм машинного навчання, що аналізував ймовірності виникнення терактів (і заходів у відповідь) у кожному осередку щотижнево по всьому світу [8].

Як зазначають вчені, машинні алгоритми досить ефективно передбачають події на територіях, які багаторазово піддавалися атакам, проте їм складно будувати прогнози для регіонів, де терактів не було вже довгий час. Такий дисбаланс даних знижує точність моделей, але її можна досягти, застосовуючи додаткові параметри.

Вчені визначили дві основні цілі тероризму: залякування та провокування. У першому випадку терористи намагаються змусити

виконувати свої вимоги, а в другому змусити контратакувати з ними. В обох випадках вони використовують насильство як комунікацію.

Дослідники також виділили 6 основних змінних, які підвищують можливість терактів:

- близькість до столиці, великих міст і доріг для швидшого поширення меседжу.

- географічна перевага терористів - вони часто ховаються у важкодоступних місцях і можуть вибирати цілі для залякування ближче до своєї бази.

- економічна активність регіону - що більш розвинена країна, то більше збитків може завдати теракту.

- імовірність ескалації конфлікту - терористи регулярно намагаються розв'язати локальні війни, щоб потім вербувати нових послідовників.

- політичний режим та показник ВВП – рівень демократичності впливає на вибір терористами стратегії дій.

- локальне закріплення – ймовірність повторення терактів багато в чому залежить від того, чи організація змогла створити осередки в тому чи іншому регіоні [8].

Таким чином, тероризм є загрозою міжнародному миру і безпеці. Для протидії цій загрозі потрібні колективні зусилля на національному, регіональному та міжнародному рівнях на основі поваги міжнародного права та використання усіх ресурсів, у тому числі й можливостей штучного інтелекту для попередження терористичних атак на об’єкти критичної інфраструктури.

Список використаної літератури:

1. Спіцина Г. О., Філіпенко Н. Є. Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 188-191.

2. Защита критически важных объектов инфраструктур от террористических атак: сборник передового опыта. Контртеррористическое управление Организации Объединенных Наций (КТУ ООН). Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (ИДКТК). 2018. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf

3. M. Lim, R. Metzler, Y. Bar-Yam (2007) Global pattern formation and ethnic/cultural violence. Science. P. 1540–1544.

4. A. Zammit-Mangion, M. Dewar, V. Kadirkamanathan, G. Sanguinetti (2012) Point process modelling of the Afghan War Diary. Proc. Natl. Acad. Sci. U.S.A. 109, 12414–12419.

5. H. Hegre, J. Karlsen, H. M. Nygård, H. Strand, H. Urdal (2013) Predicting armed conflict, 2010–2050. Int. Stud. P. 250–270.

6. S. C. Nemeth, J. A. Mauslein, C. Stapley (2014) The primacy of the local: Identifying terrorist hot spots using geographic information systems. J. Polit. P. 304–317.

7. Andre Python, Andreas Bender, Anita K. Nandi, Penelope A. Hancock, Rohan Arambepola, Jürgen Brandsch and Tim C. D. Lucas (2021) Predicting non-state terrorism worldwide. URL: https://www.science.org/doi/10.1126/sciadv.abg4778

8. Комп'ютер проти тероризму: вчені навчили ШІ передбачати теракти по всьому світу. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru.

УДК 349.2

Світлана ГУЦУ
доцентка, к.ю.н., доцентка кафедри права
Національного аерокосмічного університету імені М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: s.gutsu@khai.edu

ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРУ БЕЗПЕКИ ПРАЦІ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: В статті розглянуті сфери виробничої діяльності об’єктів критичної інфраструктури де може бути впровадження технології штучного інтелекту. Визначено ризики для працівників при роботі з ШІ. Приділено увагу нормативному забезпеченню процедури і наслідків застосування ШІ в сфері охорони праці в законодавстві зарубіжних країн. Вироблені пропозиції щодо удосконалення національного законодавства щодо безпеки праці при застосуванні ШІ.

Ключові слова: безпека праці на об’єктах критичної інфраструктури, штучний інтелект, охорона праці.

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF LABOR SAFETY AT CRITICAL INFRASTRUCTURE ENTERPRISES

Abstract: The article examines the spheres of production activity of critical infrastructure objects where artificial intelligence technology can be implemented. Risks for employees when working with AI are identified. Attention is paid to the normative provision of the procedure and consequences of the use of AI in the field of labor protection in the legislation of foreign countries. Proposals have been made to improve national legislation on occupational safety when applying AI.

Keywords: occupational safety at critical infrastructure facilities, artificial intelligence, occupational health and safety.

Світові тенденції до посилення загроз природного і техногенного характеру, активізація терористичної злочинності, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів у східних та південних регіонах України внаслідок збройного конфлікту засвідчують нагальність посилення уваги щодо безпеки праці на об'єктах, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки. Згідно статті 1 Закону України «Про критичну інфраструктуру», об'єкти критичної інфраструктури – 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. Таким чином, праця на таких підприємствах також відзначається особливими умовами праці зумовленими послиненими ризиками для здоров'я і життя працівників.Відомо, що рівень безпеки будь-яких робіт у суспільному виробництві значною мірою залежить від рівня правового забезпечення цих питань, тобто від якості та повноти викладення відповідних вимог в законах та інших нормативно-правових актах. Забезпечення роботодавцем належного рівня гігієни і безпеки праці є вже загальноприйнятим стандартом у законодавстві та правилах охорони праці. Безпечні умови праці є ключовим елементом гідних умов праці для всіх працівників [1].

На сучасному етапі розвитку суспільства штучний інтелект є потужним інструментом безпеки праці, який має значний потенціал у таких сферах, як аналіз даних і тексту, управління ризиками, відеомоніторинг і навчання. Зазвичай ШІ визначається як використання комп'ютерів та/або машин для спроби відтворити людину в прийнятті рішень, вирішенні проблем та інших здібностях. Однак, хоча штучний інтелект може ідентифікувати закономірності та кореляції, йому бракує справжнього розуміння безпеки. Людські знання та досвід у цій сфері залишаються важливими.

Інструменти та методи штучного інтелекту можна застосовувати в багатьох випадках безпеки. Технології безпеки з підтримкою штучного інтелекту включають: розумне обладнання, доповнену реальність (AR) і віртуальну реальність (VR), комп'ютерне бачення, робототехніку, дрони, переносні пристрої, датчики, мобільні програми та аналітичне програмне забезпечення. Апаратні компоненти збирають дані (наприклад, датчики) або виконують дії (наприклад, роботи). Програмні компоненти покладаються на машинне навчання щоб аналізувати шаблони та генерувати прогнози про загрози безпеці. Існує думка, що рішення штучного інтелекту досягають успіху в багатьох випадках, які є критично важливими для безпеки на робочому місці:

збирання, упорядкування та аналіз значних обсягів даних , надання та обробка інформації з таких джерел, як юридичні тексти, моделювання ситуацій, а також моніторинг процесів і засобів.

Одним із прикладів, пов'язаних із безпекою, є використання камер, які можуть визначити, чи носять працівники засоби індивідуального захисту. Зокрема, пристрої можуть стежити за працівниками, які працюють на висоті та мають носити ремені безпеки. «Камери можуть не тільки визначити, чи одягнені на працівників ремені, але й визначити, чи прив'язані ЗІЗ»(засоби індивідуального захисту) [2]. Камери з підтримкою штучного інтелекту можуть відстежувати взаємодію між працівниками та обладнанням, аналізувати стан охорони машин, перевіряти чи знаходяться працівники у визначених зонах чи поза ними, а також виконанувати ергономічної оцінки. Пристрої також можна поєднати з датчиками або носіями, які прикріплені до касок, жилетів або інших предметів. Таке безперервне спостереження за працівниками означає, що фахівцям з безпеки не потрібно покладатися виключно на спостереження, обходи чи перевірки, щоб переконатися, що працівники носять ЗІЗ, або виявити інші проблеми безпеки. Тобто замість разових перевірок, моніторинг здійснюється безперервно. Також камери та/або датчики та переносні пристрої також мають можливість створювати теплові карти, які можуть показувати, де на об'єкті відбуваються дії високого ризику.

Ще одна корисна функція використання ШІ в сфері охорони праці це обробка природної мови. Читання сотень або тисяч звітів і, можливо, мільйонів слів, є трудомістким завданням для людей. Отримання розуміння з усіх цих даних потребує ще більше часу та пропускної здатності. Крім того, звіти можуть складатися з розмовних розповідей або містити неструктуровані дані. Обробка природної мови має можливість отримувати ці звіти та знаходити закономірності, або інциденти, що відбуваються в певний час або в певних частинах закладу. Штучний інтелект підтримує бізнес завдяки своїй здатності практично миттєво аналізувати тисячі елементів даних і документів. Це може допомогти роботодавцю переконатися, що робочі місця відповідають галузевим стандартам, заощаджуючи при цьому значну кількість часу.

Ці нові форми моніторингу та управління працівниками можуть викликати правові, нормативні та етичні питання в сфері охорони та гігієни праці, зокрема щодо психічного і фізичного здоров'я працівників.

Звернемось до досвіду Європейського Союзу в дослідженні впливу технологій на безпеку праці. Так, Європейська комісія у своєму документі «Стратегічна програма ЄС щодо здоров'я та безпеки на роботі 2021-2027 Безпека та гігієна праці в мінливому світі праці» зазначає, що нові технології створюють низку проблем через: збільшення нерегулярності в тому, коли і де

виконується робота; та ризики, пов’язані з новими інструментами та обладнанням. Комісія також запропонувала переглянути Директиву про машини, яка стосується ризиків, пов’язаних із цифровізацією та використанням машин, які також стосуються здоров’я та безпеки працівників [1]. Цікавими для вивчення є результати роботи Європейського агенства з безпеки і гігієни праці (European Agency for Safety and Health at Work) яке оприлюднило 08 жовтня 2022 Звіт «Штучний інтелект для управління працівниками: наслідки для безпеки та гігієни праці» та аналітичний огляд «Вплив штучного інтелекту на безпеку та гігієну праці» 07.01.2021 [3]. В документах йдеться про те, що впровадження автоматичних алгоритмів у виробництво провокує ряд негативних наслідків. Так, працівники можуть відчувати, що їхнє приватне життя порушують, і це стає джерелом тривоги та стресу. Вони можуть не мати змоги робити перерви, коли вони потребують, що може спричинити нещасні випадки та проблеми зі здоров’ям. Нестійкі графіки роботи, що автоматично встановлюються алгоритмами, мають різноманітні негативні впливи на працівників, включаючи посилення конфлікту між роботою та сім’єю, стрес на роботі та невизначеність доходу. Використання на виробництві коботів в спільному робочому просторі може призвести до збільшення ризику нещасних випадків через зіткнення або через обладнання, яке використовується коботами. Надмірна залежність від технологій також може призвести до декваліфікації. Оскільки коботи підключені до Інтернету речей, виникають проблеми з кібербезпекою та пов’язані з цим ризики функціональної безпеки. Працівники, які мають не відставати від темпу та рівня роботи кобота, можуть відчувати тиск, щоб досягти того самого рівня продуктивності.

Отже, ШІ може створювати можливості, але й нові виклики для безпеки та гігієни праці. Роботи, які впроваджують штучний інтелект, стають мобільними, розумними та готовими до співпраці.Таким чином, очікується впровадження систем на основі штучного інтелекту в багатьох різних секторах і середовищах, від виробництва та сільського господарства до сфери послуг і транспорту.

До схожих висновків прийшов і Саміт з безпеки та гігієни праці, який відбувся в Стокгольмі 15-16 травня 2023 року. В кінцевому релізі визнається потенціал штучного інтелекту та робототехніки для створення безпечніших умов і більш здорові робочі місця для всіх [4].В дослідженнях американських науковців «Вплив штучного інтелекту на безпеку та гігієну праці: аналітичний огляд», ми також можемо прослідкувати тенденції і проблеми впровадження штучного інтелекту для сфери безпеки праці. Серед інших проблем вказана

праця констатує наявність розриву у дослідженні штучного інтелекту та безпеки та охорони праці [5].

В Україні Кабінет Міністрів України 19 вересня 2023 року ухвалив розпорядження, яким затвердив Національний план захисту та забезпечення безпеки і стійкості критичної інфраструктури. Вказаний документ документ визначає стратегічні цілі, заходи, завдання для суб'єктів національної системи захисту критичної інфраструктури (КІ), секторальних органів, операторів КІ та інших державних органів. Однією зі стратегічних цілей є «Посилення стійкості національної системи захисту критичної інфраструктури», завданнями якої є Запровадження системи постійного підвищення рівня кваліфікації персоналу операторів критичної інфраструктури. Для реалізації цього завдання у Плані передбачено:

1) підвищення рівня комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, які провадять діяльність із забезпечення безпеки об'єктів критичної інфраструктури та реагування на кризові ситуації на таких об'єктах;

2) проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури.

Отже, посилена увага до забезпечення безпеки самих об'єктів КІ буде сприяти підвищенню рівня безпеки і охорони праці на цих об'єктах. А це, в сучасних умовах неможливо здійснити без запровадження інноваційних технологій і штучного інтелекту.

На наш погляд всі документи і наукові розробки в цій сфері зводяться до наступних рекомендацій і пропозицій:

1. Розробити етичний кодекс для забезпечення справедливості і рівності при впровадженні штучного інтелекту в трудові відносини.

2. Впровадження освітніх програм, які сприяли б рівності навчання працівників роботі з ШІ, , підвищення обізнаності і цифрових навичок.

3. Запрошення до соціального діалогу всіх учасників відносин: розробників, роботодавців, робітників і держави щодо гарантій безпеки праці при впровадженні технологій у виробничий процес.

4. Обов'язкове залучення профсоюзів і трудових колективів у процес впровадження ШІ у робочі процеси, інформування їх про принципи і критерії роботи алгоритмів ШІ.

5. Занепокоєння щодо конфіденційності можна пом'якшити за рахунок підвищення прозорості владних структур, алгоритмічних аудитів і мультидисциплінарних підходів до проектування, впровадження, обслуговування та оцінки штучного інтелекту.

Висновки. Загалом використання штучного інтелекту в трудовому законодавстві та захисті працівників може мати як позитивні так і негативні наслідки. Впровадження технологій ШІ на підприємствах КІ може підвищити ефективність робочого місця шляхом автоматизації певних завдань, дозволяючи працівникам зосередитися на завданнях вищого рівня, які потребують досвіду людини. В той же час впровадження ШІ породжує юридичні проблеми, внаслідок відсутності достатньої правової бази. Існуючи юридичні акти в основному мають декларативний і рекомендаційний характер, що не достатньо для безпечного використання технологій ШІ у трудових відносинах. На наш погляд стандарти і нормативи щодо охорони праці, безпеки і гігієни труда повинні бути переглянуті і доповнені з урахуванням вимог цифрового суспільства і переходу людства до рівня Індустрії 5.0.

Список використаних джерел:

1. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions EU strategic framework on health and safety at work 2021-2027 Occupational safety and health in a changing world of work. EUROPEAN COMMISSION. Brussels, 28.6.2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0323#PP1Contents.
2. Kashyap Kompella How AI can transform industrial safety 05 May 2023 https://www.techtarget.com/searchenterpriseai/tip/How-AI-can-transform-industrial-safety.
3. Summary - Artificial intelligence for worker management: implications for occupational safety and health. URL: https://osha.europa.eu/en/publications/summary-artificial-intelligence-worker-management-implications-occupational-safety-and-health. Impact of artificial intelligence on occupational safety and health. URL: https://osha.europa.eu/en/publications/impact-artificial-intelligence-occupational-safety-and-health.
4. Висновки Саміту з безпеки та гігієни праці, який відбувся в Стокгольмі 15-16 травня 2023 року, можливість проаналізувати стратегічні рамки ЄС щодо здоров'я та безпеки на роботі 2021-2027 - Безпека та гігієна праці в мінливому світі праці. URL : https://ec.europa.eu/social/main.jsp?langId=en&catId=89&newsId=10582&furtherNews=yes
5. Fisher E, Flynn MA, Pratap P, Vietas JA. Occupational Safety and Health Equity Impacts of Artificial Intelligence: A Scoping Review. International Journal of Environmental Research and Public Health. 2023; 20(13):6221. URL : https://doi.org/10.3390/ijerph20136221.

УДК 378:356

Святослав ОХРАМОВИЧ
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: s.i.okhramovych@khai.edu, ORCID: 0009-0003-9851-851X
Владислав ЄМЕЦЬ
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: v.l.yemets@khai.edu, ORCID: 0009-0007-8195-9406
Науковий керівник
Наталія ФІЛІПЕНКО
докторка юридичних наук, професорка,
професорка закладу вищої освіти кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: n.filipenko@khai.edu, ORCID: 0000-0001-9469-3650

ПРОТИДІЯ ЕКСТРЕМІЗМУ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ЯК ЕЛЕМЕНТУ СЕКТОРУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: У тезах надано фактори причин виникнення екстремістських проявів серед здобувачів вищої освіти у закладах вищої освіти на фоні військової агресії та радикалізації суспільства. Звернено увагу та зазначено основні дії щодо зниження екстремістських проявів у ЗВО, що формуються під впливом соціальних, політичних, економічних та інших факторів у здобувачів вищої освіти, найбільш схильних до деструктивного впливу.

Ключові слова: екстремістські прояви, небезпека екстремізму, військова агресія, тероризм.

COMBATING EXTREMISM IN INSTITUTIONS OF HIGHER EDUCATION AS AN ELEMENT OF THE CRITICAL INFRASTRUCTURE SECTOR

Abstract: In theses, the factors of the causes of the emergence of extremist manifestations among students of higher education in institutions of higher education against the background of military aggression and radicalization of society are given. Attention is drawn and the main actions to reduce extremist manifestations in higher education institutions, which are formed under the influence of social, political, economic and other factors among students of higher education, most prone to destructive influence, are noted.

Keywords: extremist manifestations, danger of extremism, military aggression, terrorism.

Екстремізм є однією з складних соціально-політичних проблем сучасного українського суспільства, що пов'язано, в першу чергу, з різноманіттям екстремістських проявів, неоднорідним складом організацій екстремістської спрямованості, які дестабілізують вплив на соціально-політичну обстановку в країні.

Насильницький екстремізм, який йде врозріз з загальнолюдськими цінностями, за своєю природою носить глобальний характер. В його основі – комплекс особистісних, соціальних та ідеологічних чинників, які по різному впливають на поведінку різних людей (п. 59 Плану дій з попередження насильницького екстремізму ГА ООН 2015 р.) [1].

Український фахівець Д.В. Дорохін вважає, що, враховуючи ментальність народу України, багатовікове співіснування на її території різних націй і народностей, безконфліктний розвиток різних релігійних конфесій та інші фактори, стверджувати про масові прояви екстремізму в нашій країні немає підстав [2, с. 4]. Проте не поділяємо думку вченого про те, що екстремістські прояви досить рідко реєструються в Україні [3, с. 20], оскільки офіційні дані правоохоронних органів свідчать про зовсім інше.

Багато вітчизняних дослідників визнають серйозність небезпеки екстремізму. Наприклад, професор В. І. Тимошенко вказує, що нині екстремізм присутній в усіх сферах суспільного життя, він чинить деструктивний вплив на розвиток суспільства, перешкоджає встановленню громадянської злагоди, втіленню в життя конкретної державної політики, у тому числі й проведенню соціально-економічних перетворень [4, с. 24]. А. В. Носач розглядає екстремістську діяльність в Україні як головну загрозу суверенітету та територіальній цілісності України. На фоні військової агресії, радикалізації суспільства на перший план, як зазначає вчений, виходить проблема протидії екстремістській діяльності. Екстремізм становить значну небезпеку для політичної і правової систем будь-якої держави [5, с. 19]. С. Я. Лихова та Ю. В. Лобода звертають увагу на те, що прояви екстремізму, навіть незначні – це вже серйозна проблема для будь-якої держави, тому боротьба з цим явищем повинна стати завданням номер один для нашої країни [6, с. 182].

Здійснення екстремістської, терористичної та іншої радикальної чи насильницької діяльності суперечить як положенням Конституції України, так і законодавству України загалом, зокрема Закону України «Про основи національної безпеки», який визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування безпеки особи, суспільства й держави від зовнішніх та внутрішніх загроз в усіх сферах життєдіяльності [7].

Під впливом соціальних, політичних, економічних та інших факторів у здобувачів вищої освіти, найбільш схильних до деструктивного впливу, легше формуються радикальні погляди та переконання. Таким чином, студенти дуже часто поповнюють лави екстремістських та терористичних організацій, які активно використовують молодь у своїх політичних інтересах.

Середовище закладів вищої освіти, яке складають переважно молоді люди, у силу своїх соціальних характеристик та гостроти сприйняття навколишнього оточення, є тією частиною суспільства, в якій найшвидше відбувається накопичення та реалізація негативного потенціалу.

Протягом останніх років у низці закладів вищої освіти активізувалися неформальні молодіжні угруповання, почастішали випадки нападу на іноземних студентів. За даними низки соціологічних досліджень, нині змінилася як динаміка нападів, так і тактика подібних акцій. Наголошується на тривожній тенденції збільшення смертельних наслідків внаслідок націоналістично мотивованого насильства. Дані тенденції прагнуть використати у своїх інтересах представники партій та рухів, які активно розігрують «націоналістичну карту», розкручуючи колабораціоналіські настрої.

Причинами виникнення екстремістських проявів серед здобувачів вищої освіти у ЗВО можна виділити такі фактори:

1. Загострення соціальної напруженості (характеризується комплексом соціальних проблем, що включає проблеми рівня якості освіти, зниження авторитету викладачів (особливо на це впливає корупційна складова), «виживання» на ринку праці тощо).

2. Криміналізація низки сфер суспільного життя.

3. Вплив російської пропаганди та зміна ціннісних орієнтирів.

4. Використання мережі Інтернет у протиправних цілях тощо.

При організації профілактичної роботи важливо враховувати соціально-економічні та вікові особливості здобувачів вищої освіти.

Молоді люди, продовжуючи освіту, залишають школу, сім'ю, їдуть до іншого міста чи регіону, опиняючись у ситуації свободи і соціальної незахищеності. У результаті молода людина мобільна, готова до експериментів, участі в акціях, мітингах. При цьому готовність до подібних дій посилюється через його низьку матеріальну забезпеченість, у зв'язку з чим участь у проплачених акціях протесту може розглядатися як допустима можливість додаткового заробітку. Пошук ідентичності, спроби закріпитися в житті ведуть до невпевненості, бажання сформувати коло близьких за духом людей, знайти відповідального за всі біди та невдачі. Таким колом цілком

може стати екстремістська субкультура, неформальне об'єднання, політична радикальна організація, тоталітарна секта чи колабораційне об’єднання.

У зв'язку з цим основні дії щодо зниження екстремістських проявів у закладах вищої освіти мають бути орієнтовані на:

– оптимізацію соціального середовища ЗВО, в якому перебувають здобувачі вищої освіти, її покращення, створення в ньому просторів для конструктивної взаємодії, стимулювання у студентів позитивних емоцій від участі в навчальному процесі, від аналізу досяжних перспектив, а також від досвіду вирішення реальних побутових та соціальних проблем;

– формування механізмів оптимізації молодіжного екстремістського поля, розроблення методів його руйнування, організацію на його місці конструктивних соціальних зон;

– створення механізмів ефективного впливу на процес соціалізації особистості здобувачів вищої освіти, включення їх до соціокультурного простору закладів вищої освіти та соціуму в цілому.

Підсумком такої роботи має стати формування толерантної, відповідальної, успішної особистості, орієнтованої на соціальні цінності та патріотизм, які є стрижневими, основоположними для формування національної свідомості нинішніх і прийдешніх поколінь.

Список використаних джерел:

1. План дій щодо запобігання насильницькому екстремізму. Документ ГА ООН A/70/674 від 24 грудня 2015 р. URL: https://undocs.org/pdf?symbol=ua/A/70/674
2. Дорохін Д.В. Кримінологічна характеристика та запобігання релігійному екстремізму: автореф. … дис. канд. юрид. наук: 12.00.08. Київ, 2019. 25 с
3. Дорохін Д.В. Кримінологічна характеристика та запобігання релігійному екстремізму: дис. … канд. юрид. наук: 12.00.08. Київ, 2019. 276 с.
4. Тимошенко В.І. Політико-правова характеристика екстремізму. ScienceRise: Juridical Science. 2017. № 2 (2). С. 21-25.
5. Носач А.В. Демократизація та уніфікація правотворчості у сфері протидії поширенню екстремістської діяльності як головної загрози суверенітету та територіальній цілісності України. Право та державне управління: зб. наук. пр. 2019. № 2 (35). Том 1. С. 18-32.
6. Лихова С.Я., Лобода Ю.В. Кримінальна відповідальність за вчинення екстремістських злочинів. Наукові праці Національного авіаційного університету. Серія: Юрид. вісник «Повітряне і космічне право». 2017. № 2. С. 182-187.
7. Гелемей М. О. Екстремізм в Україні: стан і сучасні тенденції. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/7247954d-bf9c-4109-b0dd-93fafe594a5b/content

Ігор ЗЕЛІНСЬКИЙ
Заступник Голови Державної авіаційної служби України,
державний службовець другого рангу

ЦИВІЛЬНА АВІАЦІЯ УКРАЇНИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Повномасштабне військове вторгнення Російської Федерації на територію України створило безпрецедентні виклики не лише для нашої держави, але й для усього цивілізованого світу. І одними із ключових завдань, що мали вирішуватися в цих умовах, було забезпечення стабільності роботи усього державного апарату і всебічний захист критичної інфраструктури.

Слід зазначити, що відповідно до частини першої статті 5 Закону України «Про критичну інфраструктуру» метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. При цьому транспортне забезпечення належить до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України.

Частиною другою статті 9 Закону України «Про правовий режим воєнного стану» передбачено, що Кабінет Міністрів України, інші органи державної влади, військове командування, військові адміністрації, Верховна Рада Автономної Республіки Крим, Рада міністрів Автономної Республіки Крим, органи місцевого самоврядування здійснюють повноваження, надані їм Конституцією України, цим та іншими законами України. Саме тому з початком повномасштабного вторгнення та у зв'язку із закриттям повітряного простору України вкрай важливим було забезпечити інституційну спроможність Державної авіаційної служби України як уповноваженого органу з питань цивільної авіації та вжити усіх можливих заходів для функціонування галузі.

У цих умовах галузь цивільної авіації зазнала надзвичайно великих втрат, що пов'язано, зокрема, із неможливістю виконання польотів цивільними повітряними суднами на території України. Як наслідок – фінансові збитки, майнові втрати, відтік персоналу, скорочення робочих місць, призупинення діяльності деяких суб'єктів авіаційної діяльності тощо.

Проте, незважаючи на всі складнощі і проблеми, галузь цивільної авіації функціонує та відіграє важливу роль для забезпечення національних інтересів і підтримання економіки України.

Так, ще на початку 2023 року Державною авіаційною службою України здійснювалися наглядові повноваження відносно 512 суб'єктів авіаційної діяльності та 886 повітряних суден, які внесені до Державного реєстру цивільних повітряних суден України. Ряд українських авіакомпаній здійснюють свою операційну діяльність за межами України, у тому числі в європейському регіоні, продовжуючи експлуатувати свій наявний флот цивільних повітряних суден. Щонайменше 100 льотнопридатних цивільних повітряних суден (літаки і вертольоти) наразі експлуатуються/готові до експлуатації за межами України. На сьогодні 10 українських авіаперевізників виконують повітряні перевезення та авіаційні роботи в Африканському регіоні, експлуатуючи при цьому 52 повітряні судна.

Деякі з українських авіаперевізників виконують перевезення товарів військового призначення та подвійного використання, що здійснюється, зокрема, для потреб Збройних Сил України та в інтересах національної безпеки і оборони.

За таких умов українські суб'єкти авіаційної діяльності зберегли свій потенціал і можливості, робочі місця та спеціально підготовлений кваліфікований персонал. Зокрема, на початку цього року кількість сертифікованого персоналу з технічного обслуговування становила 2196 осіб, осіб з діючими свідоцтвами льотного екіпажу – 7760.

Для підтримання льотної придатності повітряних суден продовжують здійснювати свою діяльність схвалені Державіаслужбою 105 організацій з технічного обслуговування, 23 організації з управління підтриманням льотної придатності та 10 організацій з підготовки до технічного обслуговування. В Україні також продовжують функціонувати схвалені Державіаслужбою 39 організацій розробників, 26 організацій виробників авіаційної техніки та 55 навчальних закладів з підготовки льотного складу (дані наведено станом на початок 2023 року).

Вищевикладене свідчить про те, що Державній авіаційній службі України як центральному органу виконавчої влади, який реалізує державну політику у сфері цивільної авіації та використання повітряного простору України, вдалося належним чином організувати роботу свого персоналу з урахуванням при цьому безпекового фактору, окремі робочі процеси забезпечувалися в дистанційному форматі. Давно впроваджені система електронного документообігу та єдина інформаційна система Державної авіаційної служби України максимально спростили ведення діловодства та

створили умови для оперативного опрацювання та оформлення документів, необхідних вітчизняним суб'єктам для провадження авіаційної діяльності.

Важливе значення має довіра до України з боку інших держав та міжнародних авіаційних організацій. Проактивна міжнародна підтримка України та Державної авіаційної служби України дозволила вперше за всю історію цивільної авіації виключити у 2022 році Російську Федерацію зі складу Ради Міжнародної організації цивільної авіації (ІСАО).

Також окремої уваги заслуговує те, що у 2022 році в рамках участі української делегації у 41-й сесії Асамблеї ІСАО Президент Ради ІСАО відзначив досягнення Державної авіаційної служби України у системі нагляду за безпекою цивільної авіації в Україні. Відповідний сертифікат було вручено під час відкриття Асамблеї, що стало можливим завдяки успішному проходженню аудиту на відповідність Стандартам та Рекомендованій практиці ІСАО у 2020 році. За результатами цього аудиту було суттєво покращено показники відповідності вищезазначеним Стандартам за усіма напрямками: авіаційна безпека, безпека польотів, льотна придатність, тощо. Слід зазначити, що, не дивлячись на теперішні обставини, Державна авіаційна служба України продовжує здійснювати нагляд за діяльністю галузі як в Україні так і за її межами у відповідності до норм ІСАО, в повній мірі виконуючи свої зобов'язання.

Крім того, Європейською Комісією 08 листопада 2023 року оприлюднено звіт щодо проведеної оцінки реформ в Україні в межах Пакета розширення Європейського Союзу. У контексті оцінки стану справ у галузі цивільної авіації Європейською Комісією, зокрема, відзначено, Державна авіаційна служба України продовжує підтримувати належний рівень нагляду за безпекою польотів за схваленими українськими авіаперевізниками. З 2017 року Україна досягла значного прогресу у наближенні національного законодавства до законодавства Європейського Союзу у галузі авіації.

Таким чином, в умовах правового режиму воєнного стану переважна більшість схвалених українських суб'єктів авіаційної діяльності продовжує здійснювати свою операційну діяльність, адаптувавшись при цьому до існуючих на сьогодні умов. Провідну роль у процесі забезпечення безпеки авіації відіграє Державна авіаційна служба України, яка відповідно до частини другої статті 10 Повітряного кодексу України здійснює комплекс заходів, спрямованих на запобігання виникненню авіаційних подій, шляхом:

1) встановлення критеріїв безпеки авіації;

2) встановлення необхідного рівня безпеки авіації;

3) здійснення аналізу та визначення існуючого рівня безпеки авіації;

4) проведення планових та позапланових перевірок, інспектування суб’єктів та об’єктів авіаційної діяльності;

5) встановлення строків і здійснення контролю за проведенням коригуючих дій суб’єктами авіаційної діяльності;

заборони, скасування, тимчасового припинення або зміни виконання будь-яких видів польотів і авіаційної діяльності у разі виявлення загрози безпеці авіації або їх невідповідності встановленим стандартам і авіаційним правилам України;

7) анулювання, тимчасового припинення дії сертифікатів, свідоцтв, ліцензій, дозволів, обмеження прав, наданих цими документами, скасування погодження кандидатур згідно з частиною десятою цієї статті;

8) накладення штрафів та вжиття інших заходів щодо забезпечення безпеки авіації.

На сьогодні ключовим пріоритетом для забезпечення розвитку галузі цивільної України є поступове впровадження Угоди між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони, про спільний авіаційний простір, що ратифікована Законом України 17 лютого 2022 року № 2067-IX. Метою цієї Угоди є поступове створення спільного авіаційного простору між Україною та Європейським Союзом і його державами-членами, що ґрунтується, зокрема, на ідентичних правилах у сфері безпеки польотів, авіаційної безпеки, організації повітряного руху, захисту навколишнього середовища, захисту прав споживачів, систем комп’ютерного бронювання, а також на ідентичних правилах стосовно соціальних аспектів. З цією метою ця Угода встановлює обов’язкові правила, технічні вимоги, адміністративні процедури, базові експлуатаційні стандарти та імплементаційні норми, що застосовуються між Сторонами.

УДК 340
Ангеліна ЗМІЄВСЬКА
студентка 6 курсу, групи 7-96Пр1 гуманітарно-правового факультету
Національного аерокосмічного університету
імені М.Є.Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: 5737141@stud.nau.edu.ua
Наталія ФЕДОСЕНКО
кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового
факультета Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: n.fedosenko@khai.edu

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ ВИМОГ ДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: У тексті розглядається питання створення державної системи захисту критичної інфраструктури в Україні, зокрема в контексті паспортизації наявних небезпечних об'єктів. Зазначено, що ідентифікація та паспортизація цих об'єктів є ключовими завданнями в роботі з безпечною критичною інфраструктурою. Тези також містить інформацію про створення Державного реєстру представлених небезпечних об'єктів в Україні та його актуальних даних. Підкреслюється важливість формалізації вимог для оцінки готовності власників об'єкта критичної інфраструктури забезпечити їх безпеку та стійкість функціонування.

Ключові слова: критична інфраструктура, паспортизація, державна система захисту, оцінка готовності, безпека об'єктів, рєстрація об'єктів

REGULATORY AND LEGAL FRAMEWORK FOR THE DEVELOPMENT OF REQUIREMENTS FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract: The text deals with the issue of creating a state system for the protection of critical infrastructure in Ukraine, in particular in the context of certification of existing hazardous facilities. It is noted that the identification and certification of these facilities are key tasks in the work with safe critical infrastructure. The thesis also contains information on the creation of the State Register of Presented Hazardous Objects in Ukraine and its current data. The importance of formalising requirements for assessing the readiness of critical infrastructure owners to ensure their safety and sustainability is emphasised.

Keywords: critical infrastructure, certification, state protection system, readiness assessment, security of facilities, registration of facilities

У Концепції створення системи захисту критичної інфраструктури вказується на вирішення питань, пов'язаних із визначенням, описом та класифікацією об'єктів інфраструктури, які є критичними для національної безпеки [1].

На сьогоднішній день існуючі системи забезпечення безпеки для окремих галузевих об'єктів відповідають обмеженим вимогам та процедурам, які застосовуються в цих аспектах, але це робиться лише для певних видів загроз. Наприклад, у цивільному захисті, відповідно до Закону України "Про об'єкти підвищеної небезпеки" [2] передбачено вимоги щодо оцінки безпеки об'єктів підвищеної небезпеки. Ця процедура включає в себе аналіз ступеня небезпеки та оцінку рівня ризику для таких об'єктів. Крім того, цей документ передбачає комплекс заходів, які мають бути прийняті суб'єктом господарської діяльності з планування запобігання аваріям, а також для готовності локалізувати, ліквідувати аварії та їх дослідження.

У контексті захисту об'єктів критичної інфраструктури від терористичних загроз важливо відзначити, що в рамках системи фізичного захисту, на основі результатів оцінки, розробляються документи, які в певному розумінні аналогічні паспорту показано небезпечного об'єкта (ПНО). Проте, вони мають більший охоплення, розглядають аспекти оцінки різноманітних загроз.

У системі забезпечення фізичної ядерної безпеки існує процедура, встановлена Порядком проведення оцінки вразливості ядерних установок і матеріалів. Цей документ обов'язковий для дійових організацій та інших ліцензіатів, які мають право на створення та забезпечення безперервного функціонування системи фізичного захисту ядерних установ і матеріалів або системи фізичного захисту ядерних матеріалів I та II категорій під час їх перевезення. Основні завдання, які вирішуються в рамках цієї оцінки вразливості, включають виявлення виявлених об'єктів для можливих незаконних втручань, аналіз можливих радіаційних наслідків таких дій, оцінку ризиків та розробку рекомендацій щодо введення системи фізичного захисту ядерних установок і матеріалів, а також системи фізичного захисту ядерних установок і матеріалів. матеріали при їх перевезенні у відповідність до чинного законодавства.

Наприклад, звіт про оцінки вразливості, крім загальних відомостей про об'єкт та виявлених джерел небезпеки, містить звітний опис можливих загроз [3], сценарії можливих дій проявлених правопорушників та оцінку спроможності системи фізичного захисту та плану взаємодії об'єкта впоратися з виявленими загрозами [4].

У сфері формування бази даних щодо захисту рівня об'єктів, на сьогоднішній день, найбільш підходящим методом для вирішення завдань у сфері безпеки критичної інфраструктури є процес паспортизації наявних небезпечних об'єктів, який створюється Державною архівною службою України.

Згідно з "Положенням про паспортизацію наявного небезпечного об'єкта" [5], проводиться ідентифікація та паспортизація таких об'єктів шляхом створення та видання паспорта наявного небезпечного об'єкта. Паспорт наявного небезпечного об'єкта є документом певного стандарту, який містить систематизовану інформацію про конкретний фактично небезпечний об'єкт. Ця інформація містить загальну характеристику об’єкта, дані про небезпечні природні умови та технологічні процеси, інформацію про основні джерела ризику та об’єкти впливу надзвичайних ситуацій, документацію щодо аварійно-рятувальних заходів та інше. Різні види показано небезпечних об'єктів із певною формою паспортів, таких як шахти, водосховища, магістральні трубопроводи, родовищі корисних копалин і т.д. Процес ідентифікації вашого небезпечного об’єкта визначає виявлення джерел і факторів ризику на об’єкті, на підставі якого об’єкт виявляється визнаним небезпечним.

Процес реєстрації деяких небезпечних об’єктів в Україні було розпочато після ухвали Постанови Кабінету Міністрів України, яка затвердила «Положення про Державний реєстр потенційно небезпечних об’єктів»[5]. На сьогодні Реєстр наявних небезпечних об’єктів є автоматизованою інформаційно-довідковою системою, яка відповідає для збору та обробки інформації про вказані небезпечні об’єкти. У базі даних Реєстру зберігається актуальна інформація про понад 26 тисяч таких об'єктів. Серед них є підприємства, родовищі нафти та газу, магістральні трубопроводи та їх відгалуження, гідротехнічні споруди, вугільні шахти, автозаправні станції, кар'єри, мости, віадуки, шляхопроводи, сухопутні тунелі, підземні станції та метрополітени та інші.

З урахуванням викладеного вище, важливо підкреслити, що встановлення чітких вимог для оцінки готовності власників об’єктів критичної інфраструктури для забезпечення їх безпеки та стійкості функціонування є цілком можливим. Безумовно, процес паспортизації об’єктів критичної інфраструктури є одним із ключових елементів у побудові державної системи безпеки критичної інфраструктури в Україні.

Список використаних джерел:

1. Про схвалення Концепції створення державної системи захисту критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-p#Text (дата звернення: 27.10.2023).

2. Про об'єкти підвищеної небезпеки. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text (дата звернення: 27.10.2023).

3. Про затвердження Порядку функціонування державної системи фізичного захисту. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1337-2011-п#Text (дата звернення: 27.10.2023).

4. Про затвердження Правил фізичного захисту ядерних установок та ядерних матеріалів. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/z1067-06#Text (дата звернення: 27.10.2023).

5. Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1288-2002-п#Text (дата звернення: 27.10.2023).

УДК 340

Дмитро КАЛЮЖНИЙ
здобувач вищої освіти третього (наукового) рівня кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: dmitrijkoluznyj555@gmail.com

СУЧАСНІ ІНФРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ

Анотація: розглянуто поняття сучасних інформаційних технологій, їх значення та вплив у різних сферах життя. Дана стисла характеристика базових понять напрямків сучасних ІТ. Проаналізовано сфери використання інформаційних технологій в роботі правоохоронних органів та наведено проблеми та перспективи їх правового регулювання. Зазначено вплив сучасних ІТ на життя та діяльність громадян та наголошено на необхідності правильного правового регулювання усіх сфер використання сучасних інформаційних технологій.

Ключові слова: сучасні інформаційні технологій (ІТ), правове регулювання, перспективи розвитку ІТ, проблеми правового регулювання ІТ, безпека.

MODERN INFORMATION TECHNOLOGIES IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES: PROBLEMS AND PROSPECTS OF LEGAL REGULATION

Abstract: The article deals with the concept of modern information technologies, their importance and impact on various spheres of life. The author gives a brief description of the main concepts of modern IT areas. The author analyzes the areas of use of information technology in the work of law enforcement agencies, and presents the problems and prospects of their legal regulation. The author notes the impact of modern IT on the life and activities of citizens and emphasizes the need for proper legal regulation of all areas of modern information technology.

Keywords: modern information technologies (IT), legal regulation, prospects for IT development, problems of legal regulation of IT, security.

Сучасні інформаційні технології (ІТ) представляють собою широкий спектр інструментів, методів та технологій, що використовуються для збору, обробки, зберігання, передачі та аналізу інформації. ІТ включають у себе різні елементи, такі як комп'ютери, програмне забезпечення, мережі, сучасні комунікаційні засоби та інші технології [1, с. 411]. Вони впливають на різні сфери суспільного життя, від бізнесу та науки до медицини та освіти. Технології революціонізують способи спілкування, розвитку та забезпечення послуг, відкривають нові можливості для інновацій і покращення якості життя, відіграють ключову роль в діяльності правоохоронних органів, сприяючи підвищенню ефективності, безпеки та швидкості їх роботи.

У роботі правоохоронних органів ІТ використовуються в наступних аспектах:

1. Електронна база даних: Правоохоронні органи використовують електронні бази даних для зберігання і доступу до інформації що стосується кримінальних записів, підозрюваних, свідків, об'єктів інтересу тощо. Це допомагає в ідентифікації та викритті злочинів.

2. Відеоспостереження: Камери відеоспостереження використовуються для контролю публічних місць та об'єктів і допомагають в попередженні та розкритті злочинів.

3. Аналітика даних: Інструменти аналітики даних допомагають правоохоронцям аналізувати великі обсяги інформації для виявлення злочинних зв'язків та закономірностей.

4. Електронні засоби зв'язку: Сучасні комунікаційні технології, включаючи радіо, мобільний зв'язок та шифровану комунікацію, дозволяють правоохоронцям оперативно обмінюватися інформацією та координувати дії.

5. Підвищення кібербезпеки: Завдяки комп'ютерам та спеціалізованому програмному забезпеченню правоохоронці відстежують та запобігають кіберзлочинам та кібератакам.

6. Використання соціальних мереж: Правоохоронці можуть аналізувати дані з соціальних мереж для виявлення злочинів, моніторингу організованих груп і стеження за зловмисниками.

7. Геопросторовий аналіз: Використання геопросторових технологій допомагає визначити місцезнаходження подій та ресурсів, що полегшує реагування на надзвичайні ситуації та злочини.

8. Технічні засоби ідентифікації: Використання технічних засобів, таких як сканери відбитків пальців, розпізнавання обличчя та інші біометричні методи ідентифікації, допомагає встановити особи та виявити злочинців.

Такі інформаційні технології сприяють підвищенню продуктивності та ефективності правоохоронних органів, а також сприяють покращенню безпеки

громадян і забезпеченню справедливості у суспільстві. Однак, важливо також дотримуватися високих стандартів захисту приватності та прав людини під час використання цих технологій.

Використання інновацій у діяльності органів правопорядку є особливо важливим елементом для ефективного попередження та розслідування правопорушень, створення умов для недопущення негативних тенденцій у суспільстві, сталого розвитку економіки та політичної стабільності. Безумовно, питання використання інноваційних технологій у діяльності правоохоронних органів пов’язане з необхідністю законодавчого врегулювання цієї сфери, вироблення правового підґрунтя, механізмів і умов застосування ІТ правозахисними органами.

Так, в Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР у сфері правоохоронної діяльності передбачено створення якісно нової організації специфічних режимів зберігання та оброблення інформації, зв'язок з міжнародними правоохоронними органами забезпечать реалізацію активної, наступальної стратегії в боротьбі з правопорушеннями, корупцією, організованою злочинністю, застосування нових інформаційних технологій у розкритті кримінальних правопорушень [2].

У 2007 році Кабінет Міністрів України схвалив Концепцію Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю [3]. Метою Програми названо «створення єдиної інформаційно-телекомунікаційної системи правоохоронних органів (далі - система), що сприятиме реалізації державної політики з питань боротьби із злочинністю, а саме забезпечить створення умов для поліпшення координації організаційних, профілактичних, оперативно-розшукових заходів, а також підвищить ефективність інформаційно-аналітичного забезпечення правоохоронної діяльності за рахунок удосконалення інформаційної взаємодії шляхом використання сучасних захищених інформаційно-телекомунікаційних систем і проведення стандартизованих (уніфікованих) процедур обміну інформацією.

Розпорядженням Кабінету Міністрів України від 22.10.2014 р. №1118-р «Питання реформування органів внутрішніх справ України» було схвалено розроблені Міністерством внутрішніх справ Стратегію розвитку органів внутрішніх справ України та Концепцію першочергових заходів реформування системи Міністерства внутрішніх справ. Згідно з Концепцією запровадження сучасних технологій у діяльності правоохоронців такі: впровадження систем електронного документообігу та автоматизованих інформаційно-пошукових систем, удосконалення електронних баз даних, широке використання систем

відеонагляду за правопорядком, використання терміналів реєстрації відвідувачів, упровадження системи безготівкової оплати штрафів.

Важливим для подальшого розвитку залучення ІТ в діяльність правоохоронних органів є ухвалення в 2017 році Закону України «Про основні засади забезпечення кібербезпеки України» [4] і розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. Про схвалення Концепції розвитку штучного інтелекту в Україні [5].

На підставі аналізу зазначених документів можна визначити наступні перспективи використання сучасних інформаційних технологій в діяльності правоохоронних органів:

1. Покращення ефективності. Сучасні інформаційні технології допомагають правоохоронцям ефективніше виявляти, розслідувати та запобігати злочини;
2. Підвищення безпеки громадян. Інформаційні технології дозволяють правоохоронним органам краще відповідати на загрози та надзвичайні ситуації, що сприяє безпеці громадян;
3. Запобігання кіберзлочинам. Сучасні технології дозволяють правоохоронцям реагувати на кіберзлочини та попереджувати їх;
4. Підвищення прозорості. Інформаційні технології можуть сприяти підвищенню прозорості та відкритості в діяльності правоохоронних органів;
5. Оптимізація ресурсів. Використання інформаційних технологій допомагає правоохоронним органам оптимізувати витрати та ресурси;
6. Глобальна співпраця. Інформаційні технології дозволяють правоохоронним органам співпрацювати та обмінюватися інформацією з правоохоронцями з інших країн у боротьбі з міжнародними злочинами.

Сучасний світ, новітні технології, їх розвиток – не зупинити. Інформаційні технології, простір інтерне речей – це наше сьогодення в якому ми живемо і до якого ми звикли. Їх використання додає комфортності у наше життя, але, одночасно, і усвідомлення можливості використання особистих даних (інформації) кіберзлочинцями, які є новим віянням 21 століття. Таким чином, до проблем використання сучасних ІТ можна віднести:

- приватність і права людини: використання інформаційних технологій в правоохоронній діяльності може порушувати права на приватність та захист особистих даних громадян. Це може бути особливо актуально в контексті масового збору та аналізу даних;
- заборона зловживання: недостатній контроль за використанням інформаційних технологій може призводити до зловживань інформацією та зловживанням владою з боку правоохоронних органів;

- кіберзлочини: зростають загрози кіберзлочинів, які можуть бути спрямовані як на правоохоронців, так і на громадян. Це вимагає постійного вдосконалення кіберзахисту та законодавства щодо кіберзлочинів [6, С. 15];

- брак стандартизації: у багатьох країнах відсутні одночасні стандарти для зберігання та обробки інформації в правоохоронних органах, що може створювати проблеми при обміні інформацією;

- технічні обмеження: наявність старих або несумісних інформаційних систем у правоохоронних органах може обмежувати їхню можливість використовувати сучасні технології.

Загалом, правоохоронні органи повинні бути свідомими та розуміти як потенційні переваги, так і ризики використання сучасних інформаційних технологій. Правильне правове регулювання цього процесу може допомогти забезпечити оптимальне використання цих технологій для підтримки правопорядку та захисту громадян.

Список використаних джерел:

1. Бережна Н. Г. Інтернет речей в транспортній системі / Н.Г. Бережна, Волкова Т. В., Кутья О. В. Монограф, 2020. С. 411-413.
2. Про Концепцію Національної програми інформатизації: Закон України Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.182. URL : https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text
3. Про схвалення Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю: Розпорядження Кабінету Міністрів України від 19 вересня 2007 р. N 754-р. URL : https://zakon.rada.gov.ua/laws/show/754-2007-%D1%80#Text
4. Про основні засади забезпечення кібербезпеки України: Закон України Відомості Верховної Ради, 2017, № 45, ст. 403.URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. Про схвалення Концепції розвитку штучного інтелекту в Україні.URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
6. Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукраїнського науково-практичного семінару (28 листопада 2019 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 140 с. (у авторській редакції) https://er.dduvs.in.ua/xmlui/bitstream/handle/

УДК [347.53:341.53]:347.471.03
Ганна КОЛІСНИКОВА
кандидатка юридичних наук, доцентка кафедри
цивільно-правової політики, права інтелектуальної власності та інновацій
Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна
e-mail: g.v.kolisnykova@nlu.edu.ua, ORCID: 0000-0002-9309-4282

ВІДШКОДУВАННЯ МАЙНОВОЇ ШКОДИ ЮРИДИЧНИХ ОСІБ ВНАСЛІДОК ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Анотація: В статті розглядається питання щодо проєкту Закону України за яким шкода, що завдана майну юридичній особі під час збройної агресії Російської Федерації, підлягає відшкодуванню (реальна шкода або прямі збитки та упущена вигода або непрямі збитки).

Ключові слова: відшкодування шкоди, юридична особа,реальні збитки або прямі збитки, упущена вигода або непрямі збитки.

COMPENSATION OF PROPERTY DAMAGE TO LEGAL ENTITIES AS A CONSEQUENCE OF THE ARMED AGGRESSION OF THE RUSSIAN FEDERATION

Abstract: the article considers the issue of the draft Law of Ukraine according to which damage caused to the property of a legal entity during the armed aggression of the Russian Federation is subject to compensation (real damage or direct losses and lost profit or indirect losses).

Keywords: damages, legal entity, actual damages or direct damages, lost profit or indirect damages.

В статті1 протоколу до Конвенції про захист людини і основоположних свобод, передбачено, що кожна фізична або юридична особа має право мирно володітисвоїм майном. Ніхто не може бути позбавлений своєї власності інакше як в інтересах суспільства і на умовах, передбачених законом і загальними принципами міжнародного права [3, ст. 1].

Юридичною особою є організація, створена і зареєстрована у встановленому законом порядку, яка наділена цивільною правоздатністю і дієздатністю та може бути позивачем та відповідачем у суді [1, ст. 80].

Майнова шкода, завдана неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або **юридичної особи,** а також шкода, завдана майну фізичної або **юридичної особи,** відшкодовується в повному обсязі особою, яка її завдала. [1, ст. 1166]. На практиці відшкодовується саме реальні збитків або прямі збитки,упущена вигода, або непрямі збитки не відшкодовується, так наприклад, за Статутом

залізниць відшкодовується фактично завдані збитки, а саме реальні збитків або прямі збитки, щодо упущеної вигоди, або непрямих збитків, відшкодування не передбачено, хоча друга сторона може вимагати упущену вигоду, або непрямі збитки.

В проекті Закону України «Про відшкодування шкоди завданої потерпілому внаслідок збройної агресії Російської Федерації» (далі- Закону України), передбачає відшкодування завданої майнової шкоди - (збитки) втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням майна, а також витрати, які особа зробила або мусить зробити для відновлення свого порушеного права (реальні, або прямі збитки) та доходи, **які особа могла б реально одержати за звичайних обставин, якби її право не було порушене (упущена вигода, або непрямі збитки**) [3, с. 1]. Це буде новелою вітчизняного цивільного законодавства, де держава, відшкодує саме упущену вигоду, або непрямі збитки юридичній особі приватного права.

Внаслідок збройної агресії Російської Федерації під визначенням потерпілий визнаються - фізична особа, якій збройною агресією Російської Федерації завдано моральної, фізичної та/або майнової шкоди; **юридична особа приватного права.**

В проектстатті 26 Закону України передбачено, що шкода заподіяна майну **юридичної особи**, фізичної особи підприємця внаслідок збройної агресії Російської Федерації:

1. Шкода заподіяна майну юридичної особи, фізичної особи-підприємця внаслідок збройної агресії Російської Федерації розраховується з урахуванням: - вартості втраченого, знищеного чи пошкодженого майна; - упущеної вигоди; - втрат від неоплачених товарів, робіт та послуг, наданих та спожитих на тимчасово окупованих територіях. Як ми вже зазначали відшкодування збитків в **формі упущеної вигоди, або непрямих збитків** для юридичної особи приватного права є новим і досить приємним фактом.[3, ст. 26] Але виникає питання, чи всі юридичні особи приватного права її отримають? На нашу думку отримання відшкодування збитків, а саме упущеної вигоди, або непрямих збитків юридичною особою приватного права, необхідно буде скоріше заявити свої вимоги, написати заяву до відповідальної особи це Кабінет Міністрів, при ньому буде створено спеціальний Фонд і та юридична особа приватного права, яка вчасно заявить свої вимоги щодо отримання упущеної вимоги або непрямих збитків їх отримає.

Задля розрахування вартості втраченого, знищеного чи пошкодженого майна, буде створено спеціальний Фонд, який буде мати повноваження щодо розрахунку відшкодування вартості цієї реальної шкоди. Щодо упущеної вигоди, то цей втрачений прибуток , який не отримала юридична особа у

зв’язку з оголошенням воєнного стану на всій території України. Щодо розрахування розміру відшкодування, як майнової так, а може і моральної шкоди, то ми можемо застосувати форму Гудвілу– нематеріального активу, вартість якого визначається як різниця між ринковою ціною та балансовою вартістю активів підприємства як цілісного майнового комплексу, що виникає в результаті використання найкращих управлінських якостей, домінуючої позиції на ринку товарів, послуг, нових технологій тощо.

Окрім форми Гудвілу, розмір шкоди, майнової та немайнової шкоди, може бути доведений довідками відділу бухгалтерії про зменшення вартості нематеріальних та матеріальних активів, доведений шляхом проведення судової експертизи, експертної оцінки, результатами проведення перевірок контролюючих органів тощо.

В п. 2 цієї статті зазначено, що методика розрахунку розміру шкоди завданої майну юридичної особи, фізичної особи-підприємця внаслідок збройної агресії Російської Федерації встановлюється Кабінетом Міністрів України. Як ми розуміємо, то це буде відбуватись наступним чином, а саме через спеціально створений Фонд спільно з міжнародними експертами, які будуть вирішувати який саме розмір відшкодування майнової шкоди, а саме збитків в формі реальних або прямих збитків, упущених або непрямих збитків отримає юридична особа приватного права, чи можливо вимагати відшкодування моральної (немайнової) шкоди, це питання дискусійне.

Список використаних джерел:

1. Цивільний кодекс України(Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст. 356). https://zakon.rada.gov.ua/laws/show/435-15#Text .

2. Протокол до Конвенції про захист прав людини і основоположних свобод зі змінами, внесеними Протоколом№11 (994 536).

3. Проект ЗАКОНУ УКРАЇНИ Про відшкодування шкоди завданої потерпілому внаслідок збройної агресії російської федерації.

УДК 349.2:331.1
Дмитро КОРНІЛОВ
здобувач вищої освіти другого року навчання третього освітньо-наукового рівня
доктор PhD кафедри права групи 081-702-2 Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут» м. Харків, Україна
e-mail: d.s.kornilov@khai.edu, ORCID: 0000-0002-4595-6271
Науковий керівник:
Алла ГОРДЕЮК
кандидатка юридичних наук, доцентка, доцентка кафедри права гуманітарно-правовогофакультету Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: alla.law.gor@gmail.com, ORCID: 0000-0001-7423-3673

ЗНАЧЕННЯ СОЦІАЛЬНОГО ДІАЛОГУ ДЛЯ СТАБІЛЬНОГО ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Анотація: в статті розглядається вплив повномасштабної війни в Україні на трудові відносини. Зазначається, що військова агресія РФ призвела до дефіциту ресурсів, зниження ефективності роботи об'єктів критичної інфраструктури та відповідних змін у сфері праці. Розглядається значення соціального діалогу як важливого інструменту для вирішення конфліктних ситуацій та забезпечення стабільності функціонування об'єктів критичної інфраструктури в умовах воєнного стану у державі.

Ключові слова: соціальний діалог, об'єкт критичної інфраструктури, колективний договір, робочий час.

THE SIGNIFICANCE OF SOCIAL DIALOGUE FOR THE STABLE FUNCTIONING OF CRITICAL INFRASTRUCTURE FACILITIES IN CONDITIONS OF MARTIAL LAW IN UKRAINE

Abstract: The article explores the impact of the full-scale war in Ukraine on labor relations. It is noted that the military aggression of the Russian Federation has led to a shortage of resources, a decrease in the efficiency of critical infrastructure facilities, and corresponding changes in the field of labor. The importance of social dialogue is discussed as a crucial tool for resolving conflicts and ensuring the stability of critical infrastructure facilities in the conditions of a state of war in the country.

Keywords: social dialogue, critical infrastructure facility, collective agreement, working hours.

Повномасштабна війна в Україні з лютого 2022 року наклала свій відбиток на всі сфери звичного життя українців. Дефіцит продуктів харчування, електричної та теплової енергії, питної води, ліків, нафтопродуктів є лише частиною наслідків жахливих військових злочинів російської федерації проти цивільного населення. З такими проблемами

зіткнулися абсолютно всі люди, які залишилися та проживають в Україні незалежно від регіону. Окрім того, наявність в достатній кількості зазначених товарів безпосередньо впливає і на ефективність наших військових, які безперервно боронять країну від окупантів. За таких обставин ефективність роботи об'єктів критичної інфраструктури стає одним з найголовніших питань життєдіяльності країни.

Звичайно ефективність роботи об'єктів критичної інфраструктури з початку війни суттєво впала. Серед причин можна виділити такі зовнішні чинники як активні бойові дії, знищення інфраструктури, велика інфляція, мобілізація, повітряні тривоги, погіршення міжнародної та внутрішньої логістики, віялові відключення електричної енергії тощо. До внутрішніх чинників можна віднести відтік кваліфікованої робочої сили, неефективність роботи працівників тощо. І якщо зовнішні чинники не залежать від нашої волі, то внутрішнім чинникам ми можемо протистояти за допомогою застосування певних правових інструментів, передбачених чинним законодавством, що застосовувалися для стабілізації, зокрема трудових відносин у мирний час. На нашу думку, одним з таких інструментів може бути застосування соціального діалогу на національному галузевому та локальному рівнях.

Взагалі, щодо визначення ролі соціального діалогу в системі трудових, соціальних та економічних відносин приділено достатньо уваги такими науковцями як Громадська Н., Мазярко І., Ченшова Н., Іванюк Н., Арсентьєва О., Трюхан О., Юрков М., Петроє О., Чанишева Г. тощо.

Відповідно до ст. 1 Закону України «Про соціальний діалог в Україні» (далі – Закон 2862-VI),Соціальний діалог - процес визначення та зближення позицій, досягнення спільних домовленостей та прийняття узгоджених рішень сторонами соціального діалогу, які представляють інтереси працівників, роботодавців та органів виконавчої влади і органів місцевого самоврядування, з питань формування та реалізації державної соціальної та економічної політики, регулювання трудових, соціальних, економічних відносин [1].

Як зазначають Ченшова Н. та Іванюк Н., соціальний діалог – це інформаційна та комунікативна взаємодія, особливий соціокультурний механізм, основне спрямування якого – забезпечення взаємодії різних соціальних суб'єктів. Узгодити всі соціально-економічні інтереси між індивідуальними суб'єктами дуже складно, тому більшість сучасних проблем у сфері трудового права вирішується за участю колективних суб'єктів шляхом соціального діалогу [2, с. 116].

Погоджуючись з Мазярко І., можна зазначити, що соціальний діалог стосується визначення і зближення позицій суб'єктів трудових відносин, що в кінцевому підсумку (за умови його дієвості й ефективності) приводить до

формування такої системи регулювання (на макрорівні) та управління (мікрорівень), за якої рівень якості й розвитку трудових відносин оптимальні та задовольняють усіх їх учасників [3, с. 144].

Відповідно до ст. 3 Закону 2862-VI, соціальний діалог здійснюється на принципах:

- законності та верховенства права;
- репрезентативності і правоможності сторін та їх представників;
- незалежності та рівноправності сторін;
- конструктивності та взаємодії;
- добровільності та прийняття реальних зобов'язань;
- взаємної поваги та пошуку компромісних рішень;
- обов'язковості розгляду пропозицій сторін;
- пріоритету узгоджувальних процедур;
- відкритості та гласності;
- обов'язковості дотримання досягнутих домовленостей;
- відповідальності за виконання прийнятих зобов'язань.

Відповідно до п.13 ч.1 ст. 1 Закону України «Про критичну інфраструктуру» (далі – Закон 1882-IX), об’єкти критичної інфраструктури - 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 [4].

Частина 4 ст. 9 Закону 1882-IX передбачає, що до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров’я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність [4].

Відповідно до Постанови КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» від 28.04.2023 року № 415, безпосередній доступ до інформації, що міститься в Реєстрі об'єктів критичної інфраструктури є обмеженим [5].

Одним з перших законів, прийнятих Верховною Радою України з початку повномасштабного вторгнення є Закон України «Про організацію трудових відносин в умовах воєнного стану». Частинами 1, 2 ст. 6 зазначеного Закону передбачено, що нормальна тривалість робочого часу у період дії воєнного стану може бути збільшена до 60 годин на тиждень для працівників, зайнятих на об'єктах критичної інфраструктури (в оборонній сфері, сфері забезпечення життєдіяльності населення тощо).

Для працівників, зайнятих на об'єктах критичної інфраструктури (в оборонній сфері, сфері забезпечення життєдіяльності населення тощо), яким відповідно до законодавства встановлюється скорочена тривалість робочого часу, тривалість робочого часу у період дії воєнного стану не може перевищувати 40 годин на тиждень [6].

Як бачимо, цією нормою законодавець не закріпив обов'язок відповідних суб'єктів господарювання на збільшення нормальної тривалості робочого часу, а лише передбачив можливість її імплементації за необхідності. Окрім того, законодавчого закріплення збільшення тривалості робочого часу для об'єктів критичної інфраструктури не достатньо для впровадження їх у роботу. Так, ч. 2 ст. 7 Закону України «Про колективні договори і угоди» передбачено, що до змісту колективного договору належить зокрема тривалість робочого часу [7]. Таким чином, якщо в підприємствах, установах, організаціях наявний колективний договір, то впровадження таких нововведень можливе лише через внесення відповідних змін до колективного договору на підставі взаємної згоди сторін. Саме завдяки існуванню соціального діалогу в діяльності об'єктів критичної інфраструктури, сторона працівників може впливати на тривалість робочого часу, унеможлививши його одностороннє збільшення, якщо цього не вимагають об'єктивні обставини.

Отже, соціальний діалог є дуже дієвим інструментом регулювання трудових, соціальних та економічних відносин. Застосування та ефективне використання такого інструменту на об'єктах критичної інфраструктури дозволяє дійсно покращити ефективність роботи відповідного суб'єкта

господарювання та унеможливити погіршення становища працівників. Передбачені чинним законодавством принципи соціального діалогу є важливими та необхідними не тільки для працівників, а й для роботодавців та держави в цілому, особливо у період воєнного стану.

Список використаних джерел:

1. Про соціальний діалог в Україні : Закон України від 23.12.2010 № 2862-VI. Редакція від 27.05.2022. URL: https://zakon.rada.gov.ua/laws/show/2862-17#Text (дата звернення 01.11.2023).
2. Ченшова Н.В., Іванюк Н.В. (2015). Особливості соціального діалогу в країнах Європейського Союзу. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція,* (16), с. 116-119.
3. Мазярко І.С. (2015). Особливості формування та реорганізація соціального діалогу в межах створення дієвої системи соціального партнерства у торгівлі. *Підприємництво і торгівля: збірник наукових праць,* (19), с. 142-145.
4. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text(дата звернення 01.11.2023).
5. Постанова КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» від 28.04.2023 року № 415. Редакція від 28.04.2023. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text(дата звернення 01.11.2023).
6. Про організацію трудових відносин в умовах воєнного стану:Закон України від 15.03.2022 № 2136-IX. Редакція від 19.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2136-20#Text (дата звернення 01.11.2023).
7. Про колективні договори і угоди: Закон України від 01.07.1993 № 3356-XII. Редакція від 11.12.2022. URL: https://zakon.rada.gov.ua/laws/show/3356-12#Text (дата звернення 01.11.2023).

УДК 351.862.4
Іван ЛАВРОВ
ад'юнкт докторантури та ад'юнктури
Національної академії Національної гвардії України, м. Харків, Україна
e-mail: johnapleased417@gmail.com, ORCID: 0009-0005-0706-3711
Сергій БЄЛАЙ
доктор наук з державного управління, професор,
заступник начальника навчально-наукового центру з організації освітнього процесу – начальник науково-методичного відділу
Національної академії Національної гвардії України, м. Харків, Україна
e-mail: belwz3@ukr.net, ORCID: 0000-0002-0841-9522

ПЕРСПЕКТИВНІ ДОСЛІДЖЕННЯ У ФОРМУВАННІ ПРАКТИЧНИХ ОСНОВ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Анотація:Актуалізовано питання стосовно перспективних досліджень системи захисту об'єктів критичної інфраструктури на рівні держави. Розглянуто важливість захисту об'єктів критичної інфраструктури та систем, які є фундаментальними для національної безпеки. Запропоновано використання анкетування як інструменту для збору даних щодо стану та вразливості об'єктів критичної інфраструктури, аналізу цих даних та ідентифікації слабких місць. Обґрунтовано напрями подальших наукових досліджень у сфері захисту об'єктів критичної інфраструктури України.

Ключові слова: критична інфраструктура, сектор безпеки і оборони, кризові ситуації, державна безпека, система захисту.

PROSPECTIVE RESEARCH IN DEVELOPING PRACTICAL FOUNDATIONS OF THE CRITICAL INFRASTRUCTURE OBJECTS PROTECTION IN UKRAINE

Abstract: The issues related to prospective research on the critical infrastructure protection system at the state level have been addressed. The importance of safeguarding critical infrastructure objects and systems essential for national security has been discussed. The utilization of surveys as a tool for collecting data on the condition and vulnerabilities of critical infrastructure objects, as well as the analysis of this data and the identification of weaknesses, has been proposed. The directions for further scientific research in the field of protecting critical infrastructure objects in Ukraine have been substantiated.

Keywords: critical infrastructure, security and defense sector, crisis situations, state security, protection system.

Поняття «критична інфраструктура» на сьогодні введено до законодавчих та деяких інших нормативних актів багатьох держав. І хоча його розуміння в різних країнах та в окремих документах дещо відрізняється, проте такі відмінності не можна вважати суттєвими. Загальним є те, що терміном

«критична інфраструктура», зазвичай, охоплюються об’єкти інфраструктури, системи, їх частини та сукупність яких, є важливими для економіки, національної безпеки та оборони та порушення функціонування яких, може завдати шкоди життєво важливим національним інтересам [1, с. 1]. Крім того, функціонування критичної інфраструктури та її об’єктів у мирний час пов’язується із загальною підтримкою життєво важливих функцій в суспільстві, захистом базових потреб його членів і формуванням у них внутрішнього відчуття безпеки й захищеності, а у воєнний час – із забезпеченням рівня життєдіяльності в країні в наближеному до мирного часу стані та створенням умов для надання гідної відсічі агресору.

Сучасні тенденції у зміцненні захисту об’єктів критичної інфраструктури від фізичних та кіберзагроз свідчать, що будь-яке зволікання чи бездіяльність у процесі реформування цього сектору може призвести до серйозних наслідків. Це загрожує не лише економіці, національній безпеці та обороні, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. В таких випадках, це може становити загрозу навіть існуванню України як незалежної держави. [2, с. 3]

Незважаючи на значну кількість наукових праць, недостатньо вивченими є практичні основи захисту об’єктів критичної інфраструктури, їх структура та зміст відповідно до сучасних запитів. Одним із способів підвищити стійкість цих об'єктів є визначення актуальних проблемних питань та шляхів їх вдосконалення на основі проведення експертного опитування, що дозволяє зібрати інформацію про стан та вразливість об'єктів. За результатами оцінювання доречно буде визначати ступінь конкретних негативних і позитивних чинників на процес захисту критичної інфраструктури.

Експертне оцінювання доречно провести у формі, яке визначається як систематичний збір, аналіз та оцінка даних, пов'язаних з об'єктами критичної інфраструктури для визначення ризиків та підвищення їх стійкості.Дослідження планується проводити з респондентами офіцерського складу Національної гвардії України, Служби безпеки України, Управління державної охорони України з метою визначання найбільш вагомих факторів впливу на досліджувані компоненти. Під час вибору респондентів буде враховано бойовий досвід, вікові особливості, досвід служби та ін. чинники.

Після збору даних важливо провести їх аналіз та визначити слабкі місця та вразливості об'єктів. Це дозволить розробити конкретні рекомендації для підвищення стійкості та запобігання можливим загрозам. Вважається, що комплексний аналіз даних анкетування допоможе ідентифікувати пріоритетні об'єкти для захисту.Інформація, зібрана шляхом анкетування, може бути

використана для навчання та підготовки персоналу до різних сценаріїв кризових ситуацій.

З метою розкриття сутності проблем щодо захисту об'єктів критичної інфраструктури подальші наукові дослідження будуть спрямовані на оброблення даних та визначення методик для коригування зазначеного процесу.

Список використаних джерел:

1. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX.URL: https://zakon.rada.gov.ua/laws/main/1882-20#Text – 22.03.2023 р.

2. Лавров І.С., Бєлай С.В. Теоретичні засади формування системи захисту об'єктів критичної інфраструктури України. Честь і закон. 2023. №2(85). С. 5-11.

УДК 343.9

Тетяна ЛАЗАРЕВА
здобувач другого (магістерського) рівня вищої освіти спеціальності 262 «Правоохоронна діяльність» Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: t.lazareva@khai.edu, ORCID: 0009-0009-3827-6102
Сергій ЛУКАШЕВИЧ
кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: s.lukashevych@khai.edu, ORCID: 0000-0001-8386-6237

ЗАПОБІГАННЯ ТЕРОРИСТИЧНИМ ЗАГРОЗАМ КРИТИЧНІЙ ІНФРАСТРУКТУРІ УКРАЇНИ

Анотація: В доповіді піддано аналізу теоретичні та нормативно-правові засади запобігання та протидії тероризму, актуалізовано проблеми, пов'язані з військовою агресією рф проти України. Зазначено що, здійснюються додаткові необхідні заходи безпеки та сталого розвитку критичної інфраструктури в умовах воєнного стану, звернуто увагу на те, що масштабність руйнівних наслідків матимуть тривалі наслідки для держави і позначаться на функціонуванні всіх секторів критичної інфраструктури.

Ключові слова: критична інфраструктура, воєнний стан, тероризм, безпека.

DESTROYED BY TERORIST THREATS CRITICAL INFRASTRUCTURE OF UKRAINE

Abstract: The report analyzed the theoretical and regulatory principles of preventing and countering terrorism, updated the problems related to the military aggression of the Russian Federation against Ukraine. It was noted that additional necessary measures for security and sustainable development of critical infrastructure are being implemented under martial law

conditions, attention was drawn to the fact that the magnitude of the destructive consequences will have long-term consequences for the state and will affect the functioning of all sectors of critical infrastructure.

Keywords: critical infrastructure, military posture, terrorism, security.

Безпека критичної інфраструктури в умовах воєнного стану набула нового забарвлення внаслідок військової агресії російської федерації проти України. Пошкодження або порушення функціонування критичної інфраструктури завдає значної шкоди життєво важливим галузям господарства та функціонуванню державних інституцій й суспільства взагалі, призводить до трагічних наслідків тощо. Тому безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану повинна стояти на першому місті для системи державного управління та захисту держави.

Проблеми тероризму досліджувались та досліджуються багатьма науковцями – як українськими, так і зарубіжними. Зокрема варто зазначити роботу В. Ємельянова (1997 р.) [1, с. 37], який розглядає тероризм як: «одноразово здійснюваний акт або серію подібних актів не тотального, а навпаки, локального характеру, як явище кримінально – правової властивості, і його насильство з метою примушування до яких-небудь дій на фоні створеного стану страху не загального, а місцевого значення ...».Дослідження тероризму, здійснене В. Мокляком (2016 р.) [2с.148], ілюструє певну ґенезу розуміння цього явища, його сутності й форм прояву: «тероризм як складний багатоаспектний феномен досліджується низкою суспільних наук: філософією, соціологією, а також комплексом юридичних наук (кримінальним правом, міжнародним правом, адміністративним правом, кримінологією),має різні законодавчі підходи до поняття тероризму та ознак складів терористичних злочинів у національних правових системах. Визначення тероризму в законодавчих актах низки країн суттєво різняться між собою, до того ж вони не завжди відповідають міжнародним актам щодо протидії тероризму не сприяють розробці однозначного тлумачення.Поняття тероризму також має пряме або непряме визнання справедливості боротьби народів за своє визволення при наявності суперечних міжнародно-правових принципів: право націй на самовизначення, з одного боку, та непорушність існуючих кордонів – з іншого…».

Аналогічної думки дотримується багато західних дослідників тероризму. Так, професор О'Белленс у збірнику «Міжнародний тероризм в сучасному світі» [3, с. 415-416] зазначає, що «тероризм, котрий розвивається і поширюється під парасолькою атомного глухого кута, починає справляти все більший вплив на зміни світового балансу сил. Тероризм, політично обґрунтований, добре спланований і розумно спрямований, може виступити у

ролі заміни засобів створення ситуації домінування, котрого в нормальній обстановці можна досягти лише використанням регулярних військових сил. Масштаби тероризму в такому контекстісуттєво зростають. Тероризованими можуть бути цілі нації, уряди і народи. Такі акції, як викрадення, захоплення заручників тощо, як мікро прояв тероризму, потенційно здатного на значно більше. Крім того, необхідно враховувати, що терористичні дії дешевші порівняно з регулярними воєнними діями..».

Однак, поза увагою дослідників залишались проблеми, пов’язані з терористичними загрозами, викликаними військовою агресією російської федерації проти України та визнанням рф країною-агресором.

Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. Згідно з визначенням, яке міститься в законодавстві України (ст.1), «тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей.

Технологічний тероризм – кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру…».

На це звертає увагу Рада національної безпеки і оборони України, яка в своєму рішенні № 695/2023 від 17 жовтня 2023 року зазначає: «…Кабінету Міністрів України забезпечити у десятиденний строк виконання робіт та заходів із належного інженерного та фізичного захисту (зокрема, щодо протидронового захисту, систем оповіщення, укриттів для персоналу, розміщення запасних/дублювальних пунктів управління у захищених місцях) об'єктів критичної інфраструктури, збільшення кількості та посилення обороноздатності вогневих груп зі складу Збройних Сил України та Національної гвардії України, які здійснюють протиповітряне прикриття,

охорону і оборону об'єктів критичної інфраструктури. Вжити у десятиденний строк вичерпних заходів зі створення операторами критичної інфраструктури на відповідних об'єктах умов щодо:

– захисту персоналу об'єктів критичної інфраструктури, організації та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій;

– створення резервів обладнання, запасних частин тощо для своєчасного відновлення пошкоджених об'єктів і захисних споруд, контролю за дотриманням графіків ремонту необхідного обладнання;

– створення страхового фонду документації на унікальне обладнання та архівування критичних баз даних (їх частин), зокрема з використанням хмарних послуг;

– забезпечення об'єктів критичної інфраструктури джерелами електроживлення (електрогенераторами) та необхідним обсягом палива для їх стійкого і безперебійного функціонування;

– дотримання вимог законодавства про зберігання небезпечних хімічних речовин і хімічної продукції та поводження з ними;

– можливості оповіщення населення, яке потрапляє в зону можливого ураження, про виникнення надзвичайної ситуації на відповідному об'єкті…».

Указом Президента України № 64/2022 від 24 лютого 2022 року «Про введення воєнного стану в Україні» у зв'язку з військовою агресією Російської Федерації проти України на підставі пропозиції Ради національної безпеки і оборони України, відповідно до пункту 20 частини першої статті 106 Конституції України, Закону України «Про правовий режим воєнного стану» визначено першочергові заходи забезпечення безпеки критичної інфраструктури та визначено суб’єктний склад такої діяльності, зокрема, Військовому командуванню (Генеральному штабу Збройних Сил України, Командуванню об'єднаних сил Збройних Сил України, командуванням видів, окремих родів військ (сил) Збройних Сил України, управлінням оперативних командувань, командирам військових з'єднань, частин Збройних Сил України, Державної прикордонної служби України, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, Національної гвардії України, Служби безпеки України, Служби зовнішньої розвідки України, Управління державної охорони України) разом із Міністерством внутрішніх справ України, іншими органами виконавчої влади, органами місцевого самоврядування запроваджувати та здійснювати передбачені Законом України «Про правовий режим воєнного стану» заходи і повноваження, необхідні для забезпечення оборони України, захисту безпеки населення та інтересів держави. Державній службі України з надзвичайних ситуацій невідкладно разом з обласними, державними адміністраціями,

іншими державними органами, установами, підприємствами, організаціями всіх форм власності привести єдину державну систему цивільного захисту, її функціональні та територіальні підсистеми у готовність до виконання завдань за призначенням в особливий період [7].

Військово-цивільні адміністрації у сфері захисту критичної інфраструктури забезпечують програми безпеки та стійкості критичної інфраструктури, програми підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій та мають плани взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури. Створені спеціальні програми навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування з урахуванням вимог Закону України «Про критичну інфраструктуру».

Таким чином здійснюються додаткові необхіднізаходи безпеки та сталого розвитку критичної інфраструктури в умовах воєнного стану. Також, враховуючи введення в дію воєнного стану, ускладняються завдання безпеки всіх секторів критичної інфраструктури. На даний час, дякуючи іноземним партнерам України, для захисту об’єктів паливно-енергетичного сектору застосовуються воєнні засоби захисту такі як ППО, які запобігають руйнації об’єктів критичної інфраструктури. З іншого боку, запобігання та спецзаходи які проводять всі органи державної влади та органи воєнної адміністрації стосовно зменшенню уразливості таких об’єктів та протидію тяжкості можливих негативних наслідків надихає суспільство та кожного громадянина України боротися за своє життя, та життя оточуючих. Масштабність руйнівних наслідків матимуть тривалі наслідки для держави і позначаться на функціонуванні всіх секторів критичної інфраструктури. Та боротьба за збереження державного суверенітету та цілісність держави є фундаментальною складовою боротьби всього українського суспільства.

Список використаних джерел:

1. «Злочини терористичної спрямованості» / В. П. Ємельянов, 1997, «Рубікон», https://library.nlu.edu.ua/POLN_TEXT/KNIGI-2013/Emelynov_zlochunu_1997.pdf

2. «Сучасний тероризм як соціальне явище: сутність та форми прояву» / Мокляк В. В., 2016 М, http://www.irbis-nbuv.gov.ua/ASPB/1475620

3. O’Balance. Terrorism : The new growth form of warfare / O’Balance // International terrorism in the contemporary world / Livingstone M., Kress L., Wanek M. L., 1978. P. 415–416.

4. Конституція України від 28.06.1996 р. № 254к/96-ВР. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua

5. Закон України Про критичну інфраструктуру/ (Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022).

6. Закон України "Про боротьбу з тероризмом" / (Із змінами, внесеними згідно із Законом № 2997-IX від 21.03.2023).

7. Указ Президента України №64/2022 від 24 лютого 2022 року «Про введення воєнного стану в Україні», https://www.president.gov.ua/documents/642022-41397

УДК 378:356:355

Олексій ЛИТВИНОВ
доктор юридичних наук, професор,
в.о. ректора Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
ORCID: 0000-0003-2952-8258

КОНЦЕПЦІЯ КОМПЛЕКСНОЇ БЕЗПЕКИ СУЧАСНОГО УНІВЕРСИТЕТУ

Анотація. У доповіді розглянуті основні питання розроблення та впровадження у життя Концепції комплексної безпеки сучасного закладу вищої освіти, під якою розуміється сукупності передбачених законодавством заходів, що проводяться керівництвом і співробітниками ЗВО у взаємодії з представниками військово-цивільних адміністрацій, правоохоронними органами, громадськими організаціями, з метою забезпечення його безпечного функціонування, а також готовності до дій у надзвичайних ситуаціях.

Ключові слова: заклади вищої освіти, Концепція безпеки університету, безпекове середовище.

На зламі тисячоліть проблеми розвитку вищої освіти мають особливе значення для нашої країни. В умовах протидії збройній агресії тривають процеси подолання управлінської та економічної кризи, лібералізації суспільного ладу і формування громадянського суспільства. Багатий досвід, набутий у попередні роки, свідчить про те, що в управлінні різними ресурсами навчального закладу (матеріальними, фінансовими, освітніми) найважливіше значення має саме організація підготовки майбутніх педагогічних кадрів, що відбувається як комплекс освітніх заходів на основі постановки перед викладачами новітніх цілей і завдань, їх орієнтації в корпоративних цінностях, координації спільної праці, стимулювання їх активності й ініціативи, навчання з метою підвищення якісної ефективності праці кожного окремого співробітника [1].

Але зараз, в умовах збройної агресії РФ проти України, одним із найважливіших питань сталого розвитку закладів вищої освіти (далі – ЗВО) є

створення,розбудова і розвиток безпекового середовища як для здобувачів вищої освіти, так і для усіх його співробітників. Як повідомляється на ресурсі Міністерства освіти і науки України, станом на 31 липня 2023 року ворожою армією 3554 закладів освіти зазнали бомбардувань та обстрілів, 339 – зруйновано повністю [2]. У таких умовах забезпечення комплексної безпеки закладів вищої освіти є необхідною умовою їх функціонування, розвиту, та врешті решт, виживання. Це можливе лише шляхом застосування комплексного підходу, що поєднує в собі заходи навчання безпечної поведінки у різноманітних надзвичайних ситуаціях, впровадження фізичних і технічних засобів охорони тощо.

Комплексна безпека закладів вищої освіти – це стан захищеності об'єкта, що охороняється, від реальних і прогнозованих загроз військового, техногенного, природного та соціального характеру. Вона досягається за умови функціонування системи забезпечення комплексної безпеки як сукупності передбачених законодавством заходів, що проводяться керівництвом і співробітниками ЗВО у взаємодії з представниками військово-цивільних адміністрацій, правоохоронними органами, громадськими організаціями, з метою забезпечення його безпечного функціонування, а також готовності до дій у надзвичайних ситуаціях.

Все вищесказане дозволяє зробити висновок про те, що проблеми забезпечення безпеки освітнього закладу повинні вирішуватися в комплексі, із використанням науково-прикладних розробок у цій сфері. Це потребує розробки та реалізації «Концепція забезпечення безпеки університету». Звісно, її положення тісно перегукуються із вимогами «Концепції безпеки закладів освіти», схвалених Кабінетом Міністрів України [3]. Вона представляє комплексне стратегічне бачення створення безпечного освітнього середовища у закладах освіти та організацію в них рівних, належних і безпечних умов здобуття освіти та викладання.

Концепція забезпечення безпеки університету – це система поглядів, керівних ідей, принципів, прийнятих до вирішення завдань із забезпеченням всебічної та надійної безпеки освітнього середовища. Вона може бути представлена у вигляді певної віртуальної моделі, що допомагає зрозуміти, що є система безпеки університету, враховуючи питання її ефективності, реальності, технічної оснащеності, економічної доцільність тощо. Реально працююча Концепція безпеки університету повинна чітко показувати природу виникнення небезпек і загроз, визначати конкретні параметри елементів системи безпеки здобувачів вищої освіти та співробітників ЗВО, механізмів, шляхів та способів захисту їх від потенційно небезпечних та надзвичайних ситуацій.

Із цього випливають такі завдання забезпечення безпеки сучасного університету: формування готовності керівництва, науково-педагогічних працівників, адміністрації та здобувачів вищої освіти до небезпечних та надзвичайних ситуацій та до протидії їм, що досягається вивченням видів небезпек та способів їх подолання; раннє виявлення ознак та причин небезпечних та надзвичайних ситуацій, їх запобігання та усунення причин їх виникнення; забезпечення умов та можливостей для самозахисту, порятунку та захисту інших людей; правове, організаційне та технічне забезпечення системи безпеки; формування навичок безпечної поведінки при виникненні небезпечних та надзвичайних ситуацій; формування культури безпеки здобувачів вищої освіти, педагогів та всього персоналу закладу вищої освіти.

Для ефективного вирішення поставлених завдань необхідним є:

1) створення достатньої кількості захисних споруд цивільного захисту; підвищення рівня їх відповідності вимогам мінімальної/максимальної місткості таких об'єктів та кількості евакуаційних виходів (із врахуванням потреб осіб з інвалідністю та інших маломобільних груп населення), наявності водопостачання, водовідведення, вентиляції, обігріву, освітлення, засобів зв'язку та Інтернету, засобів надання медичної допомоги, доступності для співробітників, здобувачів вищої освіти та цивільного населення;

2)посилення встановленого порядку організації охорони закладів вищої освіти, зокрема із залученням органів Національної поліції (наприклад, із встановленням кнопок тривожної сигналізації в усіх ключових приміщеннях університету) та забезпечення взаємодії у питаннях надання ЗВО превентивних поліцейських послуг, спрямованих на попередження вчинення правопорушень; налагодження належної організації пропускного режиму із використанням стаціонарних металодетекторів та систем контролю доступу тощо;

3)підтримання належного рівня координації зі Спеціалістом із безпеки в освітньому середовищі [4];

4) забезпечення високого рівня дотримання вимог законодавства з питань пожежної й техногенної безпеки закладів вищої освіти; запровадження зручної мовної системи сповіщення людей про небезпеку та управління евакуацією під час пожежі та інших надзвичайних ситуацій;

5) у взаємодії з профільними спеціалістами впровадження навчання науково-педагогічних працівників, адміністрації та здобувачів вищої освіти навичкам дій в умовах надзвичайних ситуацій, бойових дій,надання домедичної допомоги, забезпечення психологічної підтримки; запровадження обов'язкового підвищення їх кваліфікації;

6) розроблення ефективних протоколів безпеки, як певного набору процедур, якими повинні керуватися керівництво і співробітники ЗВО та здобувачі вищої освіти щодо певної небезпечної ситуації. З огляду на ризики безпеки, таких протоколів в університеті має бути декілька, зокрема щодо дій під час евакуації учасників освітнього процесу в разі нападу, ризику нападу на заклад освіти або іншої небезпеки, перебування в укритті, поводження під час навчання онлайн, офлайн та за мішаною формою навчання;

7) найширше залучення до створення безпекового середовища не тільки співробітників ЗВО, а й здобувачів вищої освіти, які у ньому займаються, шляхом створення «волонтерського руху» в цій галузі й надання йому офіційного статусу. Використання отриманих від студентів даних зменшить ризики під час екстремальних явищ і забезпечить безпеку для особистості, суспільства, економіки і держави, сприятиме розвитку якостей особистості, спрямованих на безпечну поведінку в навколишньому середовищі. Крім цього, будуть досягатися цілі формування культури безпеки волонтерів вирішенням таких завдань:формування правильних, з точки зору забезпечення безпеки життєдіяльності, поведінкових мотивів;розвитку якостей особистості, спрямованих на безпечну поведінку в військовим загрозам;

8) запровадження інших заходів відповідно до нових безпекових умов.

Безумовно, усі складові Комплексної програми забезпечення безпеки університету взаємопов’язані. Не можна забезпечити один із напрямків, не створивши умов для виконання іншого, і навпаки.

Таким чином, наявність Комплексної програми забезпечення безпеки університету дозволить створити сучасні, належні та безпечні умови для всебічного розвитку ЗВО, здобуття освіти, організації безпечного освітнього середовища, зокрема в умовах військової агресії Російської Федерації проти України.

Список використаних джерел:

1. Литвинов Олексій (2023) Університетська арена думок. Про корпоративну культуру і не лише про неї. URL: https://www.facebook.com/profile.php?id=61551406107546
2. 3554 закладів освіти зазнали бомбардувань та обстрілів, 339 з них – зруйновано. Профспілка працівників освіти і науки України. URL: https://pon.org.ua/novyny/10470-3554-zakladiv-osvity-zaznaly-bombarduvan-ta-obstriliv-339-zruinovano.html
3. Концепція безпеки закладів освіти. Схвалена розпорядженням Кабінету Міністрів України від 7 квітня 2023 р. № 301-р. URL: https://zakon.rada.gov.ua/laws/show/301-2023-p#Text
4. Про реалізацію експериментального проєкту «Спеціаліст із безпеки в освітньому середовищі». Постанова кабінету Міністрів України від 15 серпня 2023 р. № 867. URL: https://www.kmu.gov.ua/npas/pro-realizatsiiu-eksperymentalnoho-proektu-spetsialist-iz-bezpeky-v-osvitnomu-t150823

УДК 343.3
Сергій ЛУКАШЕВИЧ
кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: s.lukashevych@khai.edu, ORCID: 0000-0001-8386-6237
Анатолій СТЕПАНЮК
доктор юридичних наук, професор, професор кафедри права гуманітарно-правового факультету Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: astepaniyk@ukr.net, ORCID: 0000-0002-0877-6319

ЗАХИСТ ТА СТІЙКІСТЬ ЯК ВИЗНАЧАЛЬНІ КАТЕГОРІЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Розглянуто теоретичні засади та нормативне закріплення понять захист та стійкість. Піддано аналізу практичні сенси розмежування цих понять в царині забезпечення захисту та стійкості критичної інфраструктури України як в умовах миру, так й під час воєнного стану. Визнано, що необхідною складовою захисту та стійкості є як дотримання діючих нормативно-правових приписів, так й розроблення перспективного законодавства. Визнано, що одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості національної критичної інфраструктури по відношенню до усього спектру загроз і ризиків як складової національної безпеки України.Наголошено,що прийняття та впровадження заходів Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, розробленого адміністрацією Держспецзв'язку, сприятиме безперебійній роботі об'єктів критичної інфраструктури різних категорій, забезпечить захист від загроз та підвищення стійкості критичної інфраструктури, що сприятиме її безперебійному функціонуванню.

Ключові слова: національна безпека, безпека критичної інфраструктури, захист критичної інфраструктури, стійкість критичної інфраструктури.

PROTECTION AND SUSTAINABILITY AS DETERMINING CATEGORIES OF THE SECURITY OF CRITICAL INFRASTRUCTURE

Abstract. The article considers the theoretical foundations and regulatory framework for the concepts of protection and resilience. The practical implications of distinguishing between these concepts in the field of ensuring the protection and resilience of Ukraine's critical infrastructure both in peace and during martial law are analysed. It is acknowledged that a necessary component of protection and resilience is both compliance with existing regulatory and legal requirements and development of perspective legislation. It is acknowledged that one of the priorities of Ukraine's security policy should be to improve the security and resilience of the national critical infrastructure against the full range of threats and risks as a component of Ukraine's national security. It is emphasised that the adoption and implementation of the measures of the National Plan for the Protection and Ensuring the Security and Resilience of Critical Infrastructure, developed by the Administration of the State Service for Special Communications, will facilitate the smooth operation of critical infrastructure facilities of various categories, provide

protection against threats and increase the resilience of critical infrastructure, which will contribute to its uninterrupted functioning.

Keywords: national security, critical infrastructure security, critical infrastructure protection, critical infrastructure resilience.

Підвищення стійкості національної та європейської критичної інфраструктури визначено одним із пріоритетів безпекової політики ЄС та закріплено в рішеннях Ради ЄС, спрямованих на посилення заходів із підвищення стійкості КІ [1].

Забезпечення національної безпеки сьогодні стало одним із найактуальніших питань для нашої держави. Це пов'язано не тільки із розв'язанням війни проти України, але й динамікою соціальних, економічних, політичних і навіть технологічних процесів, що відбуваються у світі. Тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних та міліарних загроз, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів України внаслідок збройної агресії російської федерації зумовлюють актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

Мета захисту критичної інфраструктури в Україні випливає із визначення критичної інфраструктури і полягає в забезпеченні постачання населенню, суспільству, бізнесу і державі життєво важливих товарів та послуг. Для виконання зазначеної функції критичної інфраструктури, необхідно гарантувати безперебійне стале функціонування об'єктів критичної інфраструктури у визначених режимах, мати спроможність запобігати руйнуванню чи завданню невиправної шкоди, припиненню функціонування або втраті контролю над об'єктами критичної інфраструктури внаслідок дії всіх чинників, та забезпечувати швидке відновлення їх функціонування, у разі, якщо воно було перерване.

Ключовими поняттями для забезпечення безперебійного функціонування критичної інфраструктури є «захист» та «стійкість». Як зазначено в законі України «Про критичну інфраструктуру»: «Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України» [3].

Останніми роками у розвинених країнах світу посилюється тенденція щодо розширення контексту заходів, пов'язаних із забезпеченням функціонування критичної інфраструктури: питання захисту (безпеки) критичної інфраструктури розглядаються разом із питаннями її стійкості.

При цьому, питанням забезпечення стійкості приділяється дедалі більше уваги у порівнянні з питаннями захисту. Таке зміщення акценту проблематики обумовлене тим, що сучасне безпекове середовище характеризується появою нових загроз та небезпек на тлі швидких процесів еволюції та трансформації існуючих загроз. Також слід ураховувати можливість випадків їх різноманітних комбінацій. За таких умов, жодна створена система захисту (безпеки) не може у повній мірі забезпечити захист від усіх загроз і небезпек. Адже поки триває розбудова системи захисту, розрахованої на певні загрози, у світі з'являються нові загрози і небезпеки.

Тому дедалі більше уваги приділяється стійкості критичної інфраструктури – її здатності бути готовою та адаптуватися до умов, що змінюються, а також протистояти змінам і швидко відновлюватися після порушень функціонування. Стійкість включає здатність протистояти та відновлюватися після навмисних атак в тому числі терористичного та/або міліарного характеру, техногенних аварій або загроз, які мають природне походження, та інших інцидентів.

Указом Президента від 27 вересня 2021 р. було затверджено Концепцію забезпечення національної стійкості, розраховану до 2025 р., в якій зазначено, що: «національна стійкість – здатність держави і суспільства ефективно протистояти загрозам будь-якого походження і характеру, адаптуватися до змін безпекового середовища, підтримувати стале функціонування, швидко відновлюватися до бажаної рівноваги після кризових ситуацій» [7].

Поняття «стійкість» по відношенню до критичної інфраструктури поки не знайшло нормативного закріплення, але в узагальненому вигляді поняття «стійкість» характеризує реакцію об'єкта на певні зовнішні подразники, його здатність адаптуватися до їх впливів без значної втрати функціональності, базуючись на загальній теорії систем, у т. ч. закономірностях формування та функціонування складних систем [5 , с. 21-22].

Вищезгаданий закон України «Про критичну інфраструктуру» є основним нормативно-правовим актом, який визначає сучасну парадигму державної політики у сфері захисту та стійкості критичної інфраструктури в умовах воєнного стану в тому числі. Визначаючи суб'єктів захисту та стійкості критичної інфраструктури ст. 7 закону виділяє певні рівні державного управління національною системою захисту критичної інфраструктури:

1) загальнодержавний рівень – здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з цим Законом, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

2) регіональний та галузевий рівні управління – здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

3) місцевий рівень управління – здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями в умовах військового стану), органами місцевого самоврядування в межах повноважень;

4) об’єктовий рівень управління – здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

Ще з 2020 року на Державну службу спеціального зв’язку та захисту інформації України була покладена функція формування переліку та реєстру об’єктів критичної інформаційної інфраструктури. Створення реєстру об’єктів критичної інформаційної інфраструктури – необхідна умова для аналізу рівня захисту таких об’єктів та проведення роботи з його посилення там, де він може бути недостатнім. 18 жовтня 2022 року Верховна Рада ухвалила в цілому проект закону «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України», яким функції уповноваженого органу з питань захисту критичної інфраструктури України покладено також на Держспецзв'язку [2].

Після ухвалених законодавчих змін Держспецзв'язку забезпечить створення повного ланцюжка захисту: формування реєстру об’єктів критичної інформаційної інфраструктури, наповнення реєстру об’єктів критичної інформаційної інфраструктури та подальшу щоденну роботу з посилення стійкості таких об’єктів і держави загалом.

При цьому слід мати на увазі, що 19 вересня 2023 року Кабінет міністрів України ухвалив розпорядження, яким затвердив Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, розроблений адміністрацією Держспецзв’язку [6]. Цей план визначає стратегічні цілі, заходи, завдання для суб’єктів національної системи захисту критичної інфраструктури, секторальних органів, операторів критичної інфраструкктури та інших державних органів. Виконання Національного плану, який розрахований на три роки, сприятиме безперебійній роботі об’єктів критичної інфраструктури різних категорій, забезпечить захист від загроз та підвищення

стійкості критичної інфраструктури, що сприятиме її безперебійному функціонуванню. Слід погодитись, що одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості національної критичної інфраструктури по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки.

Отже натепер в Україні формується злагоджена система захисту та забезпечення стійкості критичної інфраструктури, визначена як на рівні суб'єктного складу, так і на рівні діючого та перспективного законодавства.

Список використаних джерел:

1. Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR. en) 15623/22. URL: https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf
2. Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України». // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text (дата звернення: 01.11.23).
3. Закон України «Про критичну інфраструктуру». // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.11.23).
4. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 01.11.23).
5. Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf .
6. Розпорядження КМ України «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» від 19 вересня 2023 р. № 825-р // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 01.11.23).
7. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про запровадження національної системи стійкості"» // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/479/2021#Text (дата звернення: 01.11.23).

УДК 629.7.062
Павло МАКАРОВ
аспірант кафедри аерогідродинаміки
Національного аерокосмічного університету
ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна
e-mail: p.makarov_khai@gmx.com, ORCID: 0009-0008-6415-8970

РОЗРОБКА ТЕХНОЛОГІЙ ВІДНОВЛЕННЯ ЕНЕРГЕТИЧНОГО ОБЛАДНАННЯ АВІАЦІЙНОЇ ТЕХНІКИ З ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ

Анотація: У цій доповіді викладено важливість безперебійної роботи електрогенеруючого обладнання сучасного літака, проведено аналіз переходу з механічних та гідравлічних приводів управління системами літаків на електричні. Розглянуто проблему необхідності відновлення електрообладнання літаків у стислий термін.

Ключові слова: електрогенеруюче обладнання, привод, електричний літак, генератор.

DEVELOPMENT OF THE TECHNOLOGIES FOR RECOVERY OF ENERGY EQUIPMENT OF AIRCRAFT USING MODERN METHODS

Abstract: This report outlines the importance of uninterrupted operation of the power generating equipment of a modern aircraft, analyses the transition from mechanical and hydraulic drives of aircraft control systems to electric ones in modern aviation. Considered the problem of the need to restore aircraft electrical equipment in a short period.

Keywords: power generating equipment, actuator, electric plane, generator.

Рух аерокосмічної промисловості до збільшення кількості електричного обладнання обумовлений довгостроковими амбіціями переходу до повністю «електричних» літаків. Мотивація до перетворення механічних, пневматичних і гідравлічних систем на електричні зумовлена бажанням оптимізувати характеристики літака, зменшити витрати на технічне обслуговування та експлуатацію, підвищити ефективність використання палива та зменшити викиди. Приводи літаків виконують такі важливі функції, як регулювання кермом висоти, елеронами, закрилками, спойлерами, шасі, відкриття та закриття вантажних люків та відсіків зброї. Технологія приводу починаючи з ручних систем, таких як кабелі та стрижні, поступово просунулася до систем з гідравлічним приводом. Сучасною тенденцією є переведення приводів на електричні (крокові двигуни) з електронними системами управління. Живлення цих електричних приводів та електронних систем керування відбувається за рахунок електроенергії від генераторів літака.

Розглянемо систему електропостачання літака. Вона складається з систем змінного та постійного струму. Система електропостачання змінного

струму включає первинну систему з живленням від генераторів з вбудованим приводом, встановлених на кожному двигуні. При наземних операціях електропостачання змінним струмом здійснюється від генератора допоміжної силової установки. Кожен генератор забезпечує трифазне живлення напругою 400Гц. Електропостачання постійним струмом здійснюється шляхом перетворення змінного струму на постійний. Системи акумуляторів утворюють додатковий і резервний джерела постійного струму.

Типовий чотириполюсний генератор з шунтовою обмоткою з самозбудженням, який використовується в сучасному типі турбогвинтових цивільних транспортних літаків розроблений для забезпечення вихідної потужності 9 кіловат при безперервному струм 300 ампер у діапазоні швидкості від 4500 до 8500 об/мін. У своїй основній формі конструкція складається з п’яти основних вузлів, а саме: ярма, якоря, двох кінцевих рам і щіткового механізму.

Аналіз технічного стану генератора літака виконується відповідно до технічного посібника з експлуатації літака і включає: візуальний огляд, високовольтні випробування, вимірювання опору ізоляції та визначення коефіцієнту поляризації, а також рівня часткових розрядів.

Вібрація, теплові та електричні фактори (напруга, часткові розряди, вихрові струми в осерді статора), що діють на електричні приводи та генератори літаків, призводять до прискореного старіння електричної ізоляції та втрати нею своїх властивостей, що, в свою чергу, призводить до виходу з ладу генеруючого обладнання та неможливості подальшого використання літака без проведення ремонтних робіт.

Для забезпечення безпечного та безперебійного функціонування авіаційної техніки дуже часто виникає необхідність виконувати ремонти у стислий термін, що є досить складною задачею, яка вимагає пошуку вже використовуємих технологій з інших галузей машинобудування.

Технології відновлення електрогенеруючого обладнання на території України отримали свій найбільший розвиток та практичне застосування в галузі енергетичного машинобудування (гідрогенератори-двигуни). Елементи конструкцій гідрогенераторів працюють в умовах складного навантаження, викликаного спільною дією інерційних сил від обертання ротора, сил тяжіння, складальних навантажень, що виникають від посадок деталей з натягом, а також температурних навантажень. Обертання ротора, нерівномірність електромагнітного поля та гідравлічний вплив на турбіну призводять до виникнення вібрації усієї конструкції, що є схожим з впливом вібрацій, які обумовлені власними коливаннями конструкції літака. Вимоги надійності та міцності, що пред'являються в області будування та ремонту гідроагрегатів у

зв'язку з високими навантаженнями, дозволили вдосконалити ці технології та відпрацювати їх на практиці.

Отримані знання та практичні напрацювання в галузі енергетики у сукупності з використанням сучасних методів математичного моделювання дозволять успішно перенести їх до галузі літакобудування, що надасть можливість здійснювати складний ремонт електрообладнання авіаційної техніки на підприємствах України у стислий термін та є вкрай важливим під час воєнного стану.

Список використаних джерел:

1. Valavi M., Nysveen A., Nilsen R., Le B. J., Devillers E. Analysis of magnetic forces and vibration in a converter-fed synchronous hydrogenator. *2017 IEEE Energy Conversion Congress and Exposition (ECCE)*, Cincinnati, OH, USA, 2017, P. 1838-1844. URL: https://doi.org/10.1109/ECCE.2017.8096018.
2. Li J., Chen D., Liu G., Gao X., Miao K., Li Y., Xu B. Analysis of the gyroscopic effect on the hydro-turbine generator unit. Mechanical Systems and Signal Processing. *2019, Vol. 132, P. 138-152, ISSN 0888-3270.* URL: https://doi.org/10.1016/j.ymssp.2019.06.020.
3. Tretiak O.; Kritskiy D.; Kobzar I.; Arefieva M., Nazarenko V. The Methods of Three-Dimensional Modeling of the Hydrogenerator Thrust Bearing. *Computation 2022*, 10, 152. URL:https://doi.org/10.3390/computation10090152.
4. Tretiak, O.; Kritskiy, D.; Kobzar, I.; Arefieva, M.; Selevko, V.; Brega, D.; Maiorova, K.; Tretiak, I. Stress-Strained State of the Thrust Bearing Disc of Hydrogenerator-Motor. *Computation 2023, 11, 60.* URL: https://doi.org/10.3390/computation11030060

УДК 347.777

Є. НІКІТІНА, М. ЦВІТАЙЛО
Студенти 2-го курсу групи 726Ю
Національного аерокосмічного університету
ім. М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: nikitina2003liza@gmail.com; cvitajlomahail@gmail.com
Науковий керівник
Алла ГОРДЕЮК
кандидатка юридичних наук, доцентка, доцентка кафедри права
гуманітарно-правового факультету Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: alla.law.gor@gmail.com, ORCID: 0000-0001-7423-3673

ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ПРАВА І ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО НЕЇ У МИРНИЙ ЧАС ТА В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Анотація: У роботі визначено правовий статус інформації як об'єкта права, проаналізовано нормативні акти, що регулюють питання забезпечення доступу до неї у

мирний час та в умовах воєнного стану в Україні. Зазначено на те, що питання доступу до інформації в умовах воєнного стану потребує збалансованого підходу, за яким має бути враховано забезпечення прав на інформацію громадян та юридичних осіб, але таким чином, щоб відповідна транспаретність не загрожувала національній безпеці.

Ключові слова: інформація, право на інформацію,доступ до інформації, воєнний стан.

INFORMATION AS AN OBJECT OF LAW AND SPECIFICS OF ENSURING ACCESS TO IT IN PEACETIME AND UNDER MARTIAL LAW IN THE STATE

Abstract: The article defines the legal status of information as an object of law and analyzes the regulations governing access to information in peacetime and under martial law in Ukraine. It is noted that the issue of access to information under martial law requires a balanced approach that should take into account the rights to information of citizens and legal entities, but in such a way that the relevant transparency does not threaten national security.

Keywords: information, right to information, access to information, martial law.

У сучасному світі інформатизація суспільства та держави є об’єктивним процесом, що активно розвивається, завдяки стрімкому розвитку інформаційних технологій, які на сьогодні є невіддільною частиною інфраструктури людства. Тому дослідження в тематичних напрямах «інформаціїя об’єкта права» та «права на інформацію суб’єктів правовідносин» є актуальним та доцільним як в мирний час, так і в умовах воєнного часу, коли інформаційні технології позиціюють як об’єкт критичної інфраструктури, що потребує особливого захисту, а забезпечення кібербезпеки є одним із викликів часу. У даному контексті вважаємо доцільним зосередити увагу на питанні правового регулювання доступу до інформації в умовах воєнного стану в нашій державі.

Вивченню інформації як об’єкта права та забезпеченню права на неї суб’єктів права, приділяли увагу у своїх працях такі науковці як О.А. Баранова, О.В. Дзера, О.А. Підопригора, Л.В. Федюк, О.І. Харитонова та інші. Але дискусія щодо цивільно-правового осмислення «інформації» як самостійної правової категорії, її правової природи, властивостей та оперування інформацією як об’єктом права (інформаційного права) залишається незавершеною і потребує подальших досліджень, а у воєнний час загострилися питання доступу до інформації та її захисту.

Термін «інформація» походить від латинського «information» (виклад, тлумачення, уявлення, ознайомлення, повідомлення) і неоднозначно дефініюється в наукових джерелах. У загальному розумінні інформація – це певні відомості, сукупність певних даних.

Згідно зі ст. 200 Цивільного кодексу України (далі – ЦКУ) інформація визначається як нематеріальний об'єкт цивільних прав, а саме як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [1]. Інформація як об’єкт цивільних прав може існувати у матеріальному світі та цифровому середовищі, що обумовлює її форму, особливості набуття, здійснення та припинення цивільних прав і обов’язків щодо них.

Забезпечення доступу до інформації є важливим аспектом гарантування прав людини в мирний час. Це дозволяє громадянам отримувати інформацію, яка є необхідною для їхнього розвитку та підтримки їхніх прав і свобод. Зокрема, право на інформацію може бути використане для захисту прав на здоров'я, освіту та рівність у громадському житті. Також доступ до інформації допомагає громадськості контролювати діяльність державних органів компаній, що забезпечує більшу прозорість і відповідальність. У зв'язку з цим, важливо мати законодавство та механізми забезпечення доступу до інформації, які передбачатимуть транспарентність для всіх суб'єктів інформаційних відносин.

Насамперед право на отримання інформації гарантується Конституцією України (далі – КУ), а саме зазначається, у ст. 34 Основного Закону, де прописано що кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, а також гарантується свобода думки та слова, преси та інших засобів масової інформації [2]. Особисте немайнове право фізичної особи на інформацію, як право, що забезпечує її соціальне буття визначається ст. 302 ЦКУ, де прописано, що фізичні особи мають право вільно збирати, зберігати, використовувати й поширювати інформацію [1].

Також важливу роль у забезпеченні права на інформацію відіграє Закон України «Про інформацію», який визначає, що основними принципами інформаційних відносин є гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; правдивість і повнота інформації; правомірність одержання, використання, поширення, зберігання та захисту інформації. Принцип гарантованості права на інформацію, закріплений у статтях 5, 6 Закону України "Про інформацію", визначає необхідність захисту інформації, яка передається та отримується усіма людьми для реалізації своїх прав, свобод та законних інтересів. Відповідно до законодавства держава забезпечує доступ до інформації та гарантує її отримання. Однак, право на інформацію може бути обмежене в інтересах національної безпеки, охорони здоров'я населення, захисту прав та репутації інших людей та багато інших окремо. Тому, важливо надати баланс між

доступом до інформації та потребою у її обмежені для забезпечення стабільності та безпеки суспільства [3].

Отже, виходячи з вище наведеного, інформація як об'єкт права має нематеріальну природу, її правовий статус регламентується КУ, ЦКУ, ЗУ «Про інформацію», в яких, як правило, містяться норми, що позитивно регулюють інформаційні відносини, передбачаючи право доступу до інформації, та обмежуючи його у встановлених законом випадках, зокрема відповідно Закону України «Про державну таємницю», де стаття 8 зазначає перелік інформації, що належить до державної таємниці, а саме інформація про сфери: оборони, економіки, науки та техніки, зовнішніх відносин, державної безпеки та охорони правопорядку [4].

На сьогодні у зв'язку із введенням в Україні воєнного стану Указом Президента України № 64/2022 «Про введення воєнного стану в Україні» від 24.02.23 р.» тимчасово можуть обмежуватись деякі конституційні права та свободи людини та громадянина, включаючи право на інформацію [5].

У переліку заходів правового режиму воєнного стану, передбаченому ст. 8 Закону України «Про правовий режим воєнного стану» від 12.05.2015, зазначається що військове командування разом із військовими адміністраціями (у разі їх утворення) можуть самостійно або із залученням органів виконавчої владизапроваджувати та здійснювати в межах тимчасових обмежень конституційних прав і свобод людини й громадянина такі обмеження щодо інформації: «забороняти роботу приймально-передавальних радіостанцій особистого і колективного користування та передачу інформації через комп’ютерні мережі» (п. 11 ст. 8). Також вищезазначений закон в ч. 10 ст. 9 визначає, що у період дії воєнного стану на акти органів місцевого самоврядування, військово-цивільних адміністрацій та військових адміністрацій, а також їх посадових осіб не поширюються вимоги щодо строку оприлюднення проєктів нормативно правових актів [6].

У підзаконних актах, наприклад, у Наказі № 73 міністерства оборони України «Про організацію взаємодії між Збройними силами України, іншими складовими сил оборони та представниками ЗМІ на час дії правового режиму воєнного стану» від 03.03.2022 року встановлені заборони на розголошення окремих категорій інформації, які на період дії правового режиму воєнного стану та з метою запобігання витоку інформації до противника було визначено у Переліку інформації, що забороняється розголошення всіх даних, що стосуються військових частин, їхнього розташування, чисельності, озброєння та бойової техніки, операцій та інших деталей, що стосуються національної оборони та безпеки (пункти 1-24), розголошення якої може призвести до обізнаності противника про дії Збройних Сил України, інших складових сил

оборони, негативно вплинути на хід виконання завдань за призначенням під час дії правового режиму воєнного стану встановлює, яку інформацію не можна розголошувати ЗМІ [7].

Однак, на наш погляд, введення воєнного стану не є достатньою причиною для обмеження права на інформацію у широкому спектрі, оскільки вірогідна інформація про події у державі в сучасних реаліях відіграє провідну роль. Звісно це не торкається інформації, яка може бути обмеженою в доступі, а її поширення передбачатиме загрозу суспільству та державі. На такі випадки передбачається обмеження права на інформацію, і ці випадки мають бути прямо передбачені законом.

Таким чином, слід зазначити, що інформація є об'єктом, на який поширюється активний попит у суспільстві. Велике значення відкритого доступу до неї полягає в тому, що такий підхід сприяє здійсненню прав людини та громадянина в мирний час. Але під час війни право на інформацію і доступ до неї може обмежуватися збоку держави, задля можливості запровадження та здійснення заходів правового режиму воєнного стану, в інтересах забезпечення безпеки країни та населення, об'єктів критичної інфраструктури (підприємства економіки та транспорту, фінансові установи, електронні комунікації, продовольство, комунальне господарство), що є стратегічно важливими. Саме тому питання доступу до інформації в умовах воєнного стану в Україні потребує збалансованого підходу, за яким має бути враховано забезпечення прав на інформацію громадян та юридичних осіб, але таким чином, щоб відповідна транспаретність не загрожувала національній безпеці.

Список використаних джерел:

1. Цивільний кодекс України від 15.01.200р.435-IV.Редакція від 05.10.2023.URL.:https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення 23.10.23).
2. Конституція України від 28.06.1996 р. 254к/96-ВР.Редакція від 01.01.2020. URL.:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 23.10.23).
3. Закон України «Про інформацію» від 02.10.1992 р. 2657-XII.Редакція від 27.07.2023.URL.:https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 23.10.23).
4. Закон України «Про державну таємницю» від 21.01.1994 р.3855-XII. Редакція від 31.03.2023.URL.:https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 29.10.23).
5. Указ Президента України «Про введення воєнного стану в Україні» від 24.02.23 р. 64/2022. Редакція від 17.08.2023.URL.:https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення 29.10.23).
6. Закон України «Про правовий режим воєнного стану» від 12.05.2015р.389-VIII.Редакція від 19.10.2023. URL.:https://zakon.rada.gov.ua/laws/show/389-19#Text(дата звернення 29.10.23).

7.Наказ Міністерства оборони України «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» від 03.03.2022.№ 73. URL.:https://ips.ligazakon.net/document/MUS36785?an=2 (дата звернення 30.10.23).

УДК 342

Ганна ПЕТРОВА
студентка 2-го курсу магістратури групи 767 пдм
Національного аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: gureeva2104@gmail.com
Науковий керівник
Сергій ЛУКАШЕВИЧ
кандидат юридичних наук, доцент кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна,
e-mail: s.lukashevych@khai.edu, ORCID: 0000-0001-8386-6237

ВИКОНАВЧЕ ПРОВАДЖЕННЯ ЩОДО СТЯГНЕННЯ БОРГУ ЗА ПОСЛУГИ ЕЛЕКТРОПОСТАЧАННЯ ПІД ЧАС ВОЄННОГО СТАНУ

Анотація: Українська електроенергетика є критичною інфраструктурою, важливою для економіки та національної безпеки. Порушення функціонування цього сектору може завдати серйозної шкоди державним інтересам. Стаття розглядає правовий аспект примусового стягнення заборгованості за електроенергію в умовах воєнного стану, підкреслюючи важливість обов'язковості виконання судових рішень відповідно до закону.

Ключові слова: виконавче провадження, електроенергетика, воєнний стан.

ENFORCEMENT PROCEEDING REGARDING DEBTS FOR THE SUPPLY OF ELECTRICITY IN CONDITIONS OF MARTIAL LAW

Abstract: Ukrainian electric power industry is a critical infrastructure that is important for the economy and national security. Violation of the functioning of this sector can cause serious damage to state interests. The article examines the legal aspect of enforcement collection of electricity debt under martial law, emphasizing the importance of mandatory execution of court decisions and protection of rights and interests in accordance with the law.

Keywords: enforcement proceeding, electric power, martial law.

Згідно із Законом України «Про критичну інфраструктуру» об’єктами критичної інфраструктури є 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. Цим же Законом визначається, що одними з життєво важливих послуг, порушення яких призводить до негативних наслідків для національної безпеки України, є, в тому числі, послуги з енергозабезпечення

Крім того, до Переліку секторів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109, входить і паливно-енергетичний сектор, в тому числі підсектор електроенергетики, до якого відносяться об'єкти, які надають послуги виробництва електричної енергії, забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку, управління системами передачі та енергопостачання, розподіл електричної енергії [1].

З початком повномасштабного вторгнення об’єкти енергетичної інфраструктури стали мішенями для ракетних атак ворога, з метою порушення обороноздатності, функціонування банківських систем, системи надання гуманітарної та медичної допомоги, роботи зв’язку та транспорту, тощо. Пошкодженні лінії електропередачі, трансформаторні підстанції, мережі, що перебувають у критичному стані, відновлюються в максимально короткі терміни завдяки героїчним зусиллям працівників галузі. У таких обставинах зростає важливість своєчасної оплати спожитої електроенергії, адже біля 20 % тарифу – це витрати на експлуатацію мереж, їх ремонт та підтримання в належному стані.

Одночасно, у зв’язку з наслідками воєнних дій у вигляді спаду економіки, втратою робочих місць, закриття бізнесів, рівень заборгованості за послуги електропостачання збільшився у порівнянні з періодом до 24 лютого 2022 року. Наприклад, за даними ПрАТ «Харківенергозбут» у лютому-березні 2022 року рівень оплати електропостачання сягнув лише 31 % [3].

А на Дніпропетровщині станом на 1 серпня 2023 року заборгованість жителів області за спожиту електроенергію складає більше ніж 700 мільйонів гривень. При цьому, протягом року, лише 30% споживачів розраховуються за електроенергію вчасно та в повному обсязі [6].

У зв’язку з необхідністю стягнути з боржників ці кошти підприємства-постачальники електроенергії звертаються за захистом порушеного права до суду.

Обов'язковість судових рішень є однією з ключових принципів судової системи, яка закріплена в Конституції України (стаття 129). Держава має зобов'язання забезпечити виконання судових рішень відповідно до чітко визначеного законом порядку. Також в Основному Законі (стаття 129-1) передбачено, що судове рішення є обов'язковим до виконання, і це підкреслює важливість додержання цього принципу [2]. Крім того, і Цивільний процесуальний кодекс України, і Господарський процесуальний кодекс України визначають обов'язковість судових рішень основними принципами.

Таким чином, право на судовий захист не обмежується лише розглядом справи та прийняттям обґрунтованого законного рішення. Воно також

передбачає, що судовий захист має бути спрямованим на відновлення порушених прав та свобод і гарантувати виконання судового рішення. Це означає, що судова система повинна забезпечувати справедливий результат та захищати права та інтереси, а також вживати заходів для забезпечення виконання судових рішень.

Важливо підкреслити, що виконання судових рішень має бути невідворотним і однозначним, оскільки в іншому випадку це може призвести до дискредитації самої ідеї правосуддя і підірвати довіру до судової системи. Правосуддя не завершується лише моментом винесення рішення, важливо, щоб це рішення було дійсно виконане.

Отже, наступним кроком у випадку відсутності добровільного погашення заборгованості за постачання електроенергії стає звернення до органів державної виконавчої служби та приватних виконавців для примусового стягнення.

Відповідно до статті 1 Закону України «Про виконавче провадження», виконавче провадження як завершальна стадія судового провадження і примусове виконання судових рішень та рішень інших органів (посадових осіб) - сукупність дій визначених у цьому Законі органів і осіб, що спрямовані на примусове виконання рішень і проводяться на підставах, у межах повноважень та у спосіб, що визначені Конституцією України, цим Законом, іншими законами та нормативно-правовими актами, прийнятими відповідно до цього Закону, а також рішеннями, які відповідно до цього Закону підлягають примусовому виконанню [4].

Унаслідок вторгнення Російської Федерації та введення воєнного стану на території України, Верховною Радою були внесені необхідні зміни до багатьох законів України, в тому числі і ті, що вплинули на сферу виконавчого провадження.

Наразі, виконавче провадження щодо примусового стягнення заборгованості за постачання електричної енергії здійснюється у відповідності до Закону України «Про виконавче провадження», Інструкції з організації примусового виконання рішень, затвердженої Наказом Міністерства юстиції України № 512/5 від 02.04.2012 та інших нормативно-правових актів з урахуванням змін, що були прийняті з огляду на воєнний стан. Останні зміни до ЗУ «Про виконавче провадження» були внесені 11 квітня 2023 року.

Головним міфом стосовно виконання рішень щодо заборгованості за електричну енергію зі споживачів-фізичних осіб стало те, що під час дії воєнного стану борги за житлово-комунальні послуги не стягуються. Насправді ж абзацом 22 пункту 10-2 Прикінцевих та перехідних положень Закону України «Про виконавче провадження» передбачено зупинення у

період дії воєнного стану вчинення виконавчих дій з виконання рішень про стягнення з фізичної особи заборгованості за житлово-комунальні послуги, в тому числі за постачання електроенергії, лише на території територіальних громад, що належать до територій, на яких ведуться активні бойові дії, або тимчасово окупованих територій відповідно до Переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією, затвердженого Наказом Міністерства з питань реінтеграції тимчасово окупованих територій України 22 грудня 2022 року № 309, або якщо стягнення заборгованості за такі послуги здійснюється щодо нерухомого майна, яке є місцем постійного проживання такої фізичної особи і було знищено або пошкоджено внаслідок воєнних (бойових) дій.

Також, новелою є встановлена абзацом 7 пункту 10-2 Прикінцевих та перехідних положень Закону України «Про виконавче провадження» можливість фізичних осіб-боржників користуватися коштами, на які накладено арешт, в межах суми, яка не перебільшує дворазового розміру мінімальної заробітної плати, кожного місяця. Крім того, з арештованого рахунку можна здійснювати видаткові операції, пов’язані зі сплатою податків, зборів. На додаток, абзацом 19 пункту 10-2 Прикінцевих та перехідних положень Закону України «Про виконавче провадження» припиняється звернення стягнення боргів з пенсій, стипендій.

Що стосується боржників, які є юридичними особами, та самозайнятих осіб, які використовують найману працю фізичних осіб, вони також можуть використовувати кошти, на які накладено арешт органами ДВС, приватними виконавцями, з метою виплати заробітної плати в розмірі не більше п’яти розмірів мінімальної заробітної плати на місяць на одного працівника такої юридичної особи чи самозайнятої особи, а також для сплати податків, зборів та єдиного внеску на загальнообов’язкове державне соціальне страхування.

Також абзацом 22 пункта 10-2 Прикінцевих та перехідних положень Закону України «Про виконавче провадження» передбачено зупинення у період дії воєнного стану в Україні, вчинення виконавчих дій у виконавчих провадженнях з виконання рішень щодо боржників, якими є підприємства оборонно-промислового комплексу, органи військового управління, з’єднання, військові частини, вищі військові навчальні заклади, військові навчальні підрозділи закладів вищої освіти, установи та організації, які входять до складу Збройних Сил України.

Окремо пунктом 10-3 Прикінцевих та перехідних положень ЗУ «Про виконавче провадження» встановлено особливості щодо виконавчих проваджень, де боржником є акціонерне товариство «Укрзалізниця» - зупиняється вчинення виконавчих дій та заходів примусового виконання

рішень щодо такого боржника, а також підлягають зняттю всі арешти на кошти і майно АТ «Укрзалізниця».

Були прийняті також і зміни, які стосуються усіх споживачів-боржників за виконавчими провадженнями. Так, передбачено, що на час воєнного стану заборонено відкриття проваджень та вжиття заходів примусового виконання на території територіальних громад, що належать до територій, на яких ведуться активні бойові дії, або тимчасово окупованих територій відповідно до Переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією, затвердженого Наказом Міністерства з питань реінтеграції тимчасово окупованих територій України 22.12.2022 № 309 [4].

З огляду на вищевказані зміни можна зробити висновок, що вони були направлені на те, щоб підтримати рівень життєдіяльності населення, особливо тих, хто безпосередньо зіткнувся з наслідками воєнних дій, забезпечити надходження в бюджет необхідних податків та зборів, безперебійну виплату заробітної плати на підприємствах-боржниках, забезпечення сталого функціонування юридичних осіб оборонної сфери та стратегічно важливих підприємств.

З іншого боку, своєчасна оплата постачання електроенергії та стягнення боргів за цю послугу надзвичайно важлива, адже багато галузей повсякденного і виробничого життя є енергозалежними, і вони не можуть собі дозволити відмовитися від цієї послуги. У випадку невчасної оплати рахунків, борги доведеться компенсувати з державного бюджету, що може призвести до відволікання фінансових ресурсів від інших важливих сфер, таких як оборона.

Підсумовуючи вищевказане, необхідно підкреслити, що зміни в інституті примусового виконання рішень є тимчасовими і спрямовані на забезпечення життєдіяльності країни під час воєнного стану. Важливо відзначити, що ці зміни в законодавстві будуть діяти лише під час воєнного стану, оскільки це особливий правовий режим із власними обмеженнями. Проте, законодавець намагається забезпечити максимальний баланс між захистом національних інтересів та життєдіяльності населення в цей період, забезпечуючи виконання судових рішень та підтримуючи принципи правової держави**.**

Список використаних джерел:

1. Деякі питання об'єктів критичної інфраструктури : Постанова КМУ від 09.10.2020 р. № 1109 : станом на 11.05.2023. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text .

2. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
3. Новини ПрАТ "Харківенергозбут". від 25.04.2022. URL: https://zbutenergo.kharkov.ua/media_centre/news/shanovni-spozhyvachi-prat-harkivenergozbut.
4. Про виконавче провадження : Закон України від 02.06.2016 р. № 1404-VIII : станом на 18 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1404-19#Text
5. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX : станом на 5 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text .
6. Шостак В. Жителі Дніпропетровщини заборгували за електроенергію понад 700 мільйонів гривень. Суспільне. Новини. URL: https://suspilne.media/574067-ziteli-dnipropetrovsini-zaborguvali-za-elektroenergiu-ponad-700-miljoniv-griven/.

УДК 342

Карина ПУРИК
студентка групи 7-96пр1, гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник
Світлана ГУЦУ
к.ю.н, доцентка, доцентка кафедри права
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: karinapurik33@ukr.net

АКТУАЛЬНІ ПРОБЛЕМИ ВИЗНАЧЕННЯ ЗМІСТУ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Анотація. У статті визначено зміст і характерні ознаки правового режиму воєнного стану, передбаченого чинним законодавством. Зазначається, що процедура і підстави введення воєнного стану на території України не відповідали реальним умовам, що склалися внаслідок збройної агресії РФ проти нашої держави. Для усунення цих недоліків було прийнято низку нормативних актів, що врегулювали цю сферу. Однак відсутність системного підходу і узгодженості між державними органами управління заважають мінімізувати наявні загрози та ризики територіальній цілісності і недоторканності України.

Ключові слова: воєнний стан, правовий режим, національна безпека, обмеження прав людини.

CURRENT PROBLEMS OF THE UNDER THE LEGAL REGIME OF THE MILITARY STAND

Abstract: The article defines the content and characteristic features of the legal regime of martial law provided for by the current legislation. It is noted that the procedure and grounds for imposing martial law on the territory of Ukraine did not correspond to the real conditions that arose as a result of the armed aggression of the Russian Federation against our state. To eliminate these shortcomings, a number of normative acts regulating this sphere were adopted. However, the lack of a systematic approach and coordination between state management bodies hinders the minimization of existing threats and risks to the territorial integrity and inviolability of Ukraine.

Keywords: martial law, legal regime, national security, restrictions on human rights.

Починаючи з 2014 року, у зв’язку із російською збройною агресією проти нашої держави, українськими політиками, громадськими діячами, у засобах масової інформації порушуються питання щодо необхідності введення в Україні правового режиму воєнного стану. Водночас, як показала практика, законодавче врегулювання питання введення правового режиму воєнного стану не відповідало умовам, що склались під час російської збройної агресії проти України. Саме тому було ініційовано внесення суттєвих змін до законодавства для правового забезпечення протидії збройній агресії РФ, зокрема й у питанні запровадження правового режиму воєнного стану.

Відповідно до статті 1Закону України «Про правовий режим воєнного стану» воєнний стан - це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень [1].

24 лютого 2022 року у зв'язку з військовою агресією російської федерації проти України Указом Президента України № 64/2022 [2] введено воєнний стан із 05 години 30 хвилин 24 лютого 2022 року строком на 30 діб.Строк дії воєнного стану в Україні продовжувався Указами Президента України ще декілька разів.

Досліджуючи сутність та зміст правового режиму воєнного стану слід зазначити, що:

- воєнний стан це особливий правовий режим, який встановлюється в державі або в окремих її територіях. Уведення правового режиму надає особливі повноваження, тобто особливі права, органам виконавчої влади, військовому командуванню, органам місцевого самоврядування щодо повноважень, встановлених їм законодавством для мирного часу і створює необхідні умови для здійснення наданих їм цих особливих повноважень;

- особливі повноваження органам державної влади, військовому командуванню, органам місцевого самоврядування потрібні для відвернення загрози або відсічі збройної агресії проти України;

- уведення правового режиму воєнного стану не означає оголошення війни. Воєнний стан – реакція на існуючу загрозу суверенітету і територіальній цілісності та на збройну агресію;

- уведення правового режиму воєнного стану передбачає тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень;

- відповідно до сучасного міжнародного права введення воєнного стану державою, яка стала жертвою агресора, не буде перешкоджати наданню їй військової й інших видів допомоги;

- з уведенням правового режиму воєнного стану (наряду з мобілізацією) у державі настає особливий період. Особливий період – період, що настає з моменту оголошення рішення про мобілізацію (крім цільової) або доведення його до виконавців стосовно прихованої мобілізації чи з моменту введення воєнного стану в Україні або в окремих її місцевостях та охоплює час мобілізації, воєнний час і частково відбудовний період після закінчення воєнних дій [3].

Статтею 3 Указу Президента України «Про введення воєнного стану в Україні» визначено, що у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30-34, 38, 39, 41-44, 53 Конституції України, а також вводитися тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану».

Зміст правового режиму воєнного стану, порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб визначаються нормами Закону України «Про правовий режим воєнного стану». Військовому командуванню в умовах воєнного стану надається право разом з органами виконавчої влади, військовими адміністраціями та органами місцевого самоврядування запроваджувати та здійснювати заходи правового режиму воєнного стану. Для цього військове командування наділяється правом видавати обов'язкові до виконання накази і директиви з питань

забезпечення оборони, громадської безпеки і порядку, здійснення заходів правового режиму воєнного стану.

В умовах воєнного стану щодо фізичних осіб можуть бути запроваджені певні обмеження:

1) запроваджувати трудову повинність для окремих категорій працездатних осіб, які не залучені до роботи у сфері забезпечення життєдіяльності населення, оборонній сфері і не забронювані за підприємствами, установами та організаціями.

Порядок запровадження трудової повинності регламентовано Порядком залучення працездатних осіб в умовах воєнного стану до суспільно корисних робіт в умовах воєнного стану, затвердженим Постановою Кабінету Міністрів України від 13.07.2011 № 753 [4]. Так, до суспільно корисних робіт можуть бути залучені виключно працездатні особи віком від 16 років, які не мають обмежень за станом здоров'я до роботи в умовах воєнного стану (безробітні та інші незайняті особи; працівники функціонуючих в умовах воєнного стану підприємств (за погодженням з їх керівниками); особи, зайняті в особистому селянському господарстві; студенти вищих, учні та слухачі професійно-технічних навчальних закладів; особи, які забезпечують себе роботою самостійно.

2) запроваджувати комендантську годину;

3) встановлювати особливий режим в’їзду і виїзду, обмежувати свободу пересування громадян, іноземців та осіб без громадянства, а також рух транспортних засобів;

4) перевіряти документи в осіб, а в разі потреби проводити огляд речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян, за винятком обмежень, встановлених Конституцією України.

Виходячи з вище сказаного, можна зазначити, що до чинного законодавства було внесено значну кількість змін, спрямованих на удосконалення організації та здатності ефективно працювати в умовах воєнного стану, які сприяли б можливості усувати чи мінімізувати наявні загрози та ризики територіальній цілісності і недоторканності України. Проте внесення змін до чинного законодавства не завжди здійснювалося планомірно та системно, що не сприяло вирішенню широкого кола питань, пов'язаних із забезпеченням національної безпеки і оборони України.

Список використаних джерел:

1. Про правовий режим воєнного стану: Закон України. Відомості Верховної Ради, 2015, № 28, Ст. 250. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.

2. Про затвердження Указу Президента України «Про введення воєнного стану в Україні»: Закон України від 24 лютого 2022 року № 2102-IX. URL:https://zakon.rada.gov.ua/laws/show/2102-20#Text.

3. Про оборону України: Закон України. Відомості Верховної Ради України. – 1992, № 9, Ст.106. URL:https://zakon.rada.gov.ua/laws/show/1932-12#Text

4. Про затвердження Порядку залучення працездатних осіб до суспільно корисних робіт в умовах воєнного стану: Постанова Кабінету Міністрів України від 13 липня 2011 року № 753. URL: https://zakon.rada.gov.ua/laws/show/753-2011-%D0%BF#Text

5. Гуцу С. Ф. Особливості дистанційної праці і її впровадження в надзвичайних умовах//Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук: збірник матеріалів доповідей учасників міжнародної науково-практичної конференції. (Харків-Рига, 31 травня 2022 р.). Харків, 2022. С. 70-73

УДК 342

Дмитро РАСПУТНІЙ
здобувач вищої освіти ступеня доктора філософії (PhD)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
ORCID: 0000-0002-2920-4854

ЗАГАЛЬНІ ТА ГАЛУЗЕВІ ЗАСАДИ БЕЗПЕКИ ТА СТАЛОГО РОЗВИТКУ В СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: У даній статті розглядається вплив воєнного стану на процес трансформації, розвитку та реалізації безпекових функцій при забезпеченні безпеки об’єктів критичної інфраструктури. Основні принципи, та основоположні документи для формування безпеки на об’єктах критичної інфраструктури. Тенденції розвитку, та трансформація наявної системи.

Ключові слова: Критична інфраструктура, Кадрова безпека, Економічна безпека Інформаційна безпека, Фізична безпека, інженерно-технічні споруди.

GENERAL AND SECTOR-SPECIFIC PRINCIPLES OF SECURITY AND SUSTAINABLE DEVELOPMENT IN CRITICAL INFRASTRUCTURE SECTORS

Abstract: This article explores the impact of a state of war on the process of transformation, development, and implementation of security functions in ensuring the safety of critical infrastructure objects. It delves into the fundamental principles and key documents shaping security on critical infrastructure sites. The trends in development and the transformation of the existing system are also examined.

Keywords: Critical infrastructure, Personnel security, Economic security, Information security, Physical security, Engineering structures.

Вступ

Значення критичної інфраструктури для суспільства та економіки полягає у її ключовій ролі у забезпеченні функціонування суспільства та підтриманні економічної стійкості країни.

Згідно з «Законом україни про критичну інфраструктуру» об’єкти критичної інфраструктури - 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].

Тобто Критична інфраструктура об'єднує різноманітні сектори, такі як енергетика, транспорт, водопостачання, телекомунікації, охорона здоров'я, фінанси та інші, які є життєво важливими для суспільства та економіки.

А отже, критична інфраструктура є основою суспільства та економіки, і її безпека та сталий розвиток є важливим завданням для забезпечення добробуту громадян та стійкості держави особливо під час війни.

Основна частина

Термін КІ- далі, критична інфраструктура, вперше з’явився у директиві PDD-63 (Presidential Decision Directive), яка була підписана президентом Сполучених Штатів Америки Б. Клінтоном у 1996 році. [4]

Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі.

КІ– це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [2, с. 7].

З огляду на зазначене, видається логічним та доцільним поняття «критичну інфраструктуру України» розглядати як сукупність об’єктів незалежно від форми власності.

Європейський підхід формування архітектури безпеки

Згодом з формуванням Європойської асоціації сталі та вуглю, а пізніше трансформації її до «ЕС» питанням критичної інфраструктури та її безпеки почали приділяти увагу в інших країнах, зокрема: Німеччина, Велика Британія, Нідерланди, Чеська Республіка, Словаччина, Польща, Угорщина та інші. В подальшому така зацікавленість країн учасниць у об’єднанні трансформувалась до утворення низки політичних наднаціональних проєктів, та затвердження організації **European Programme for Critical Infrastructure Protection** (**EPCIP**)

На данний момент, країни європейського союзу формують консультативний оргна разом з іншими країнами НАТО, **Цільова група НАТО - ЄС з питань стійкості критично важливої інфраструктури.**

Це викликано тим, що дедалі більшу загрозу КІ становить диверсійна діяльність та використання саме організованої злочинності (далі – ОЗУ), як інструмент для впливу на діяльність КІ.

Це видозмінює принцип побудування архітектури безпеки навколо об'єкту критичної інфраструктури.

Розвиток забезпечення безпеки об'єктів критичної інфраструктури в Україні

Основоположним документом, для розвитку принципів організації безпеки критичної інфраструктури, тим паче враховуючи безперестанний рух нашої країни до заходу це "ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ"

Однак не дивлячись на принципи що були закладені в цьому документі. Теорія зазвичай, стикається з проблемами реалізації на практиці.

Досліджуючи дану тему необхідно зауважити, що те на скільки великим пластом є сама критична інфраструктура, на стільки і обширним є перелік загроз для неї. Тому передбачити все, майже не можливо.Через це багато об'єктів критичної інфраструктури, адаптуються під умови сьогодення на прикладах аналогічних підприємств що зазнали ураження від ворожих дій.

На разі достеменно невідомо повний перелік усіх організаційних засад та дій що використовується для захисту безпеки критичної інфрасткутури органами безпеки, розвідки та контррозвідки, армії та генеральним штабом.

Однак перш за все на підприємствах такого типу не враховуючи в приватній властності вони знаходяться або в державній, як правило використовують наступні підходи із забезпечення безпеки:

- Кадрова безпека,
- Економічна безпека,
- Інформаційна безпека,
- Фізична безпека.

Багато проблем було утворено особами що були залучені до дій проти нашої держави. А саме під впливом третіх осіб або організацій такі особи передавали данні про стан наших критично важливих об'єктів, що й призводило в подальшому до влучань по таким об'єктам.

З моменту початку війни, багато підприємств дедалі більше приділяють уваги саме фізичній безпеці, через постійну, потенційну, небезпеку ураження, а враховуючи досвід отриманий того річ, така загроза повністю реальна.

В першу чергу підприємства, почали підсилювати свої інженерно-технічні споруди, та вдосконалювати системи фізичного захисту.

Почались розбудови та зміни устрою підприємств. Подекуди на деяких підприємствах було прийнято ряд дій за для перенесення уразливих до ворожих дій елементі під землю, а подекуди критично важливі вузли тепло та енерго постачання прийнято було рознести та децентралізувати.

Прикладом такого підходу слугує Проект Закону про внесення змін до Закону України "Про комбіноване виробництво теплової та електричної енергії (когенерацію) та використання скидного енергопотенціалу" щодо розвитку високоефективної когенерації.

Основною проблемою сталого функціонування органів забезпечення безпеки повстала проблема закриття багатьох баз даних.

Зараз завдяки роботі та доволі швидкій адаптації органів розвідки, та правоохоронних органів, взаємодії багатьох профільних міністерств. Доступ до деякої частини таких баз було відновлено, або була знайдена заміна. Тому безпекові органи підприємств відновили в більшій мірі свої дії, та набули нового досвіду з принципів рекрутингу нових робітників.

З приводу економічної безпеки відбулося теж немало змін, органи безпеки підприємст повинні були моніторити економічну діяльність підприємств за відсутності електронних баз даних що безперечно ускладнювало роботу. Це подекуди блокувало дію таких органів, а іноді примушувала відкочуватись до досвіду минулих поколінь та співпрацювати через своїх інформаторів та перевірених контрагентів, хоч і співпрацюючи на невигідних умовах.

А це в свою чергу призводило до завищення цін за товари або послуги, та махінацій у торгах. Однак з плином часу, доступ до більшої половини таких інформаційних баз було відновлено. А навички нового досвіду використовуються навіть з відновленням доступу до таких баз.

Тенденції розвитку та інтеграції

Українськими законотворцями було ухвалено план зі сталого розвитку підприємств критичної інфраструктури, де було вказано на доктринальному рівні план розвитку підприємств, та нових підходів з реалізації безпеки.

В якому здебільшого була акцентована увага саме на подальшій співпраці з міжнародними безпековими органами та консультативними нарадами. Це тим більше крокує нога в ногу з новим підходом до розбудови нової системи захисту критичної інфраструктури, а саме обрати власну стратегію забезпечення національної стійкості та визначити при цьому єдиний комунікаційний пункт для обміну інформацією для контактів з іншими об’єктами КІ регіону та іншими країнами-членами.

Що дасть змогу реагувати саме на актуальні проблеми того регіону, де розташовується об’єкт КІ, та діяти в залежності від ситуації і вже в другу чергу опиратись на дії партнерів.

Все це приводить до роздумів що до того, як буде далі інтегруватись критична інфраструктура України у європейський економічний простір.

Такі зміни в цілому будуть плекати інтерес до інвестицій у об’єкти такого плана. Що надалі буде стимулювати зростання обсягів енергетики, транспортних хабів та інших об’єктів у нашій державі, адже економіка та ринок не терплять пустоти. А Україна свого часу була величезним хабом та брамою до Европи на шляху з Азії.

Однак не дивлячись на все це, на скільки буде приємним інвестеційний клімат, залежить вже саме від нас, та реалізації концепцій що закладуються в законодавстві.

Висновок

Дедалі більше з розглядом нормотворчих актів та документів що використовуються як основоположні для розвитку безпеки КІ ми можемо бачити розвиток у напрямку взаємодії та подальшої інтеграції до системи сумісної взаємодії з Европою. Дедалі більше будуть інтегруватись на підприємствах саме стандарти НАТО та формування сумісного безпекового контуру такого типу об’єктів.

Однак необхідно не забувати і про те що країни НАТО ніколи не зтикалися з прямим протистоянням таким країнам агресорам як наш супротивник.

Тож це нова ступінь в розвитку забезпечення безпеки. Де Українські органи безпеки, та українські спеціалісти зможуть трансформовувати загальний підхід до забезпечення безпеки

На скільки реальним є поняття сталого розвитку критичної інфраструктури в умовах війни дуже важко оцінити, не дивлячись на це я міг би мовити про те що, однозначно наша держава, та критична інфраструктура вийде видозміненою з цих всіх подій.

Логічним буде уявити формування єдиного консультативного органу, та комунікаційної системи з формування оборони та безпеки. Ліричним відступом було б мовити про формування бастіонів навколо, або з таких об’єктів.

Вивчення способів та методів ураження, вивчення витрати на безпеку, та співвідношення їх з потенційними втратами об’єктів. Аналіз ризиків та внесення коректив до вже реалізованих проектів та нововведення вже з отриманих даних.

Список використаних джерел:

1. Про критичну інфраструктуру та її захист : проєкт Закону України. URL: https://zakon.rada.gov.ua

2. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. К. : НІСД. 2016. 176 с.

3. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпекова діяльність: системний підхід. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2017. Вип. 1. С. 154–163.

4. Presidential Decision Directive (PDD NSC-63) May 22, 1998, [Електронний ресурс]. – Режим доступу: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

UDC 342

Olena RUBAN

Ph.D. (Law), Department of Civil Law Policy, Intellectual Property and Innovations
YaroslavMudryi National Law University, Kharkiv, Ukraine
e-mail: ruban281984@gmail.com, ORCID: 0000-0002-8602-0517

PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST CYBER-ATTACKS

Abstract: Considered how cyber-attacks affect government institutions, private enterprises and individuals. Special attention is paid to consideration of possible ways of legislative protection of enterprises classified as critical infrastructure, including energy, telecommunications, media and finance, as they are the main targets during armed conflicts. The scientific theses examine changes in the legislation of Ukraine and foreign countries that regulate the issue of protecting critical infrastructure objects, in particular, from cyber-attacks.

Keywords: critical infrastructure, protection of critical infrastructure, cyber attacks, damage caused by cyber-attacks.

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Анотація: Розглянуто як кібератаки впливають на державні установи, приватні підприємства та окремих осіб. Особливу увагу приділено розгляду питань щодо можливих шляхів законодавчого захисту підприємств, віднесених до категорії критичної інфраструктури, включаючи енергетику, телекомунікації, медіа та фінанси, оскільки вони є основними цілями під час збройних конфліктів.У наукових тезах досліджено зміни у законодавстві України та зарубіжних країн які регулюють питання захисту обєктів критичної інфраструктури, зокрема і від кібератак.

Ключові слова:критична інфраструктура, захист критичної інфраструктури, кібер атаки, шкода завдана кібератаками.

In June 2017, the encryption virus known as NotPetya targeted the infrastructure of major companies, including Nova Poshta, Naftogaz, Kyivenergo, banks, gas stations, and mobile operators. This cyberattack resulted in the disruption of numerous systems. In December 2020, the narrative of a meticulously orchestrated cyber operation surfaced, making headlines in leading media outlets in the United States and worldwide. The SolarWinds software, which is utilized by government agencies and employees of large corporations, fell victim to this virus compromise. Around 18,000 users were affected, and the estimated cost of the damage caused by this attack is roughly $100 billion.

Since the start of the war, Ukraine has been subjected to many cyberattacks impacting government agencies, private enterprises, and individuals. Special consideration should be given to businesses categorized as critical infrastructure, including energy, telecommunications, media, and finance, as they are prime targets in times of armed conflicts. The business community and individuals need to be prepared to confront these challenges.

June 14, 2022, marked a watershed moment in Canadian data protection history: the first reading of a federal cyber security law of general application aimed at protecting critical infrastructure. Until now, Canada has had an adequate (if not exemplary) privacy law regime, but little in the way of legislation of general application addressing cyber security outside of the privacy law regime. Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act, and making consequential amendments to other Acts* [1], takes two important steps beyond the requirements of existing privacy laws:

1. It amends portions of the federal *Telecommunications Act* to authorize the government to impose obligations on telecommunications service providers to "secure the Canadian telecommunications system," and more broadly,

2. It implements the *Critical Cyber Systems Protection Act* (the CCSPA), which empowers the government to designate services or systems as vital and to impose data protection obligations on their operators, require mandatory reporting of cyber security incidents, and facilitate threat information exchange "between relevant parties."

The CCSPA also establishes summary and indictable criminal offenses for violations of provisions of the CCSPA. (For example, failure to respond to requests for information is a summary offense, while failure to establish, implement, and maintain a cyber security program may be an indictable offense.)

The CCSPA does not appear to impose obligations directly on vendors or suppliers servicing vital services and systems. However, it *does* seek to address "risks associated with supply chains and the use of third-party products and services"

by holding the operators of vital services and systems responsible for supplier/vendor vulnerabilities by requiring operators to:

1. Establish cyber security programs to "identify and manage" risks "associated with the designated operator's supply chain and its use of third-party products and services";

2. Provide regulators with notice of material changes in operators' supply chains or use of third-party products and services;

3. Take "reasonable steps" to mitigate risks associated with supply chains and use of third-party products and services; and

4. Keep records of such steps taken.

While not made explicit by the statute, it seems reasonable to expect that management of supplier and vendor-associated risks will include imposing contractual obligations on suppliers and vendors in respect of cyber security preparedness, and the granting of audit rights to operators to ensure compliance. Such steps are common tools in privacy statutes.

If passed in a form substantially similar to the proposed bill, Bill C-26 will take Canada a step further into the sphere of countries taking serious legislative measures to protect critical infrastructure from cyber-attacks.

Since the commencement of the war, Ukraine must enhance cybersecurity measures, the Ukrainian parliament promptly revised criminal and criminal procedural legislation within the first month of the war. These revisions improved the grounds and procedures for holding cybercriminals accountable. The changes were implemented through two laws:

1. The Law “On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine “On Electronic Communications” to Enhance Pretrial Investigations 'on Hot Tracks' and Counter Cyber Attacks” No. 2137-IX [2], dated March 15, 2022.

2. The Law "On Amendments to the Criminal Code of Ukraine to Strengthen the Fight Against Cybercrime in the Context of Martial Law"No. 2149-IX [3], dated March 24, 2022, which came into effect on April 3, 2022.

Law No. 2149-IX is designed to fortify measures against cybercrimes during wartime. It defines the concept of cybercrime and elucidates its significance during military conflicts. Cybercrimes can have the objectives of destabilizing the country's situation, pilfering confidential information, paralyzing state institutions, and causing other forms of material damage.

The law also outlines the liability for cybercrimes and establishes corresponding penalties. Its primary objective is to reinforce the capabilities of the cybersecurity system, ensure the reliability of digital services, and effectively combat cybercrime in wartime conditions. Moreover, the fundamental legal criteria

for the offense under Article 361 of the Criminal Code have shifted from requiring specific consequences to merely the commission of the act itself.

These changes simplify the proceedings and facilitate a more effective response to cybercrime. Law No. 2149-IX is geared towards strengthening cybersecurity and ensuring an efficient fight against cybercrime during wartime, addressing the pressing needs of the modern information age.

According to the European Union Agency for Cyber Security (ENISA) [4], during 2020 and 2021, a change in the situation regarding cyber threats was observed. The number of attacks on so-called "home offices" has increased significantly. This means that attacks were directed at programs that allow you to create a single corporate network and personal offices of employees, allowing them to work remotely. Examples of such programs are various CRM systems, "cloud" services, and other applications. As a result, the threat of data breaches to businesses has increased, rising from 8.7% in 2020 to 81% in the second quarter of 2021.

There are several reasons why the IT structures of private and public corporations have become the object of attacks. One of them is ransom demand. This scenario became famous, for example, due to the attack on the American pipeline company Colonial Pipeline in May of this year, when their systems were blocked by malware and the attackers demanded a ransom for access to them. This attack resulted in financial losses (the company paid approximately $4.4 million in ransom) and public panic, leading to higher gasoline prices and fuel shortages. Colonial Pipeline provides 45% of fuel supplies for the entire East Coast of the United States, so a long shutdown can lead not only to business but also to serious political and social crises.

ENISA specialists also note that over the past two years, not only the number of ransomware has increased, but also the amount of ransom demanded by attackers for unlocking systems. For example, in 2019, the largest buyout amount was $15 million, and in a year, it increased to $30 million. In 2021, hackers demanded $50 million from Acer and Quanta Computer. Therefore, ENISA experts predict a further increase in the financial "appetite" of cyber criminals, which may reach 100 million dollars in 2022. Cyber-attacks have become a significant source of income for many illegal groups.

Another reason for attacks is an attempt to seize control of objects. For example, in the US, on February 5, 2021, hackers hacked the water treatment plant system in the city of Oldsmar, Florida [5], in an attempt to increase the level of chemicals (sodium hydroxide) in the drinking water to toxic levels.

The hackers were spotted in time and the chemical level in the water was restored to safe values. However, this case showed how important critical infrastructure facilities are for our lives.

The third reason for attacks is damage to work and systems. There are examples of such attacks both abroad and in Ukraine. From the first attack on Ukraine's energy systems in December 2015 to attacks on the CEC election system [6] during the 2014 presidential election and the NotPetya virus. Malicious programs penetrate systems and block their operation.

The fourth reason is the theft of information and important data. Examples of such attacks are in the news every day, including the theft of personal data of famous customers of the jewelry brand Graff Diamonds in the UK, the theft of the data of more than 40 million users of the mobile operator T-Mobile in the US, and the theft of information about Glovo couriers in Spain [7]. There are other reasons, such as hacker training, destabilization of the situation in the regions, and interference with the transmission and reception of information.

Regardless of the reasons, attacks always have a negative impact on companies. They can lead to the shutdown of some or all departments, undermine trust in the company, and cause colossal losses, as well as create a direct threat to the life and health of many people, including employees, partners, and customers. Such attacks can lead to catastrophic consequences for critical infrastructure facilities, which include companies in the chemical sector, information technologies, energy, the transport system, water supply, and others. Sectors of the economy are interconnected, and the failure of one facility can affect others.

Therefore, the protection of critical infrastructure objects should always be at the center of attention, and it is important to pay special attention to the application of modern technologies, the exchange of experience, and the training of cyber defenders. The training of cyber defenders must be continuous, as they are on the front lines in the fight against technological threats. Anti-cyber activities are becoming increasingly important, and initiatives such as cyber hackathons and cyber defense tournaments are substantial to improve defenses.

Examples of events where the FBI is investigating cyberattacks on critical infrastructure facilities in the US, frequent attacks on Ukrainian government websites, and the Israeli military successfully stopping cyberattacks on valuable facilities show that the issue of cyber defense is as important as physical defense objects. By protecting passwords, servers, and controllers, we protect not only businesses but also the entire state's interests.

References:

1. Bill C-26: An Act respecting cyber security, amending the Telecommunications Act, and making consequential amendments to other Acts. URL: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html

2. Про внесення змін до Кримінального процесуальног окодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам. Закон України від 15 березня 2022 р. № 2137-IX. URL: https://ips.ligazakon.net/document/view/T222137?an=76

3. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану. Закон України від 24 березня 2022 р. № 2149-IX.URL: https://ips.ligazakon.net/document/view/T222149?an=19

4. The European Union Agency for Cyber Security (ENISA). URL: https://www.enisa.europa.eu/publications#c3=2013&c3=2023&c3=false&c5=publicationDate&reversed=on&b_start=0&c2=Critical+infrastructure

5. Did someone really hack into the Oldsmar, Florida, water treatment plant? New details suggest maybe not. CyberScoop. URL: https://cyberscoop.com/water-oldsmar-incident-cyberattack/

6. Cyberattack on Ukraine grid: here's how it worked and perhaps why it wasdone. THE CONVERSATION. Published: January 18, 2016. URL: https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802

7. Spain's delivery platform Glovo was fined again for breaching labor laws. January 24, 2023. URL: https://techcrunch.com/2023/01/24/glovo-madrid-labor-law-fine/

УДК 342

Олена САВЧУК

к.ю.н., доцентка, доцентка кафедри права Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна;
доцентка кафедри екологічного права
Національного Юридичного університету ім. Я. Мудрого, м. Харків, Україна
ORCID: 0000-0003-3299-7936

ІННОВАЦІЙНІСТЬ ЕКОЛОГО-ПРАВОВОЇ СКЛАДОВОЇ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ УКРАЇНИ

Анотація: У роботірозглядається сучасний стан та перспективи розвитку еколого-правової складової енергетичної галузі в Україні. Зокрема, досліджуються інноваційні підходи та технології, що застосовуються для забезпечення сталого розвитку та екологічної безпеки у сфері енергетики. Робиться акцент на важливості інноваційних підходів у підвищенні ефективності та зниженні негативного впливу енергетичного сектору на довкілля.

Ключові слова: інновації, еколого-правова складова, енергетична галузь, паливно-енергетичний комплекс.

INNOVATIVENESS OF THE ENVIRONMENTAL AND LEGAL ENERGY INDUSTRY OF UKRAINE

Abstract: The work examines the current state and prospects for the development of the environmental and legal component of the energy industry in Ukraine. In particular, innovative

approaches and technologies used to ensure sustainable development and environmental safety in the field of energy are investigated. Emphasis is placed on the importance of innovative approaches in increasing efficiency and reducing the negative impact of the energy sector on the environment.

Keywords: innovations, ecological and legal component, energy sector, fuel and energy complex.

Сучасний розвиток суспільства неможливий без надійного та ефективного енергетичного сектору. Проте, наростаюча потреба у енергії спричиняє виродження екологічних проблем, що вимагають комплексного правового врегулювання. Енергетичний сектор є основною ланкою економіки, проте його функціонування супроводжується викидами та іншими негативними впливами на навколишнє середовище. Вирішення цих проблем стає нагальним завданням для збереження природних ресурсів та запобігання змінам клімату.

Україною був ратифікований Договір до Енергетичної Хартії та Протокол до Енергетичної Хартії з питань енергетичної ефективності і суміжних екологічних аспектів, а також Кіотський протокол до Рамкової Конвенції Організації Об'єднаних Націй про зміну клімату. Проаналізувавши названі документи, стає очевидним, що охорона та використання природних ресурсів в енергетичній галузі є пріоритетним напрямом, а використання відновлюваних джерел енергії, у свою чергу, є одним із заходів, спрямованих на виконання договірними сторонами своїх зобов'язань. З огляду на вищевикладене, енергетичний сектор можна віднести до однією з найскладніших проблем сучасного світу, яка вимагає вирішення з акцентом на сталий розвиток.

Треба погодитися з М. В. Красновою, яка зазначала: «основна увага має бути приділена імплементації положень Енергетичної Хартії, інших нормативно-правових актів у сфері енергетики, оскільки для України відкривається унікальна можливість долучитися до вдосконалення правового регулювання енергетики у всіх її аспектах, починаючи з питань торгівлі енергоносіями, квотами на викиди парникових газів, енергетичними інвестиціями, закінчуючи питаннями енергозбереження і охорони довкілля від негативного впливу діяльності відтворювальної енергетики [2, с. 68].

Основною сучасною тенденцією енергетичної сфери є розвиток відновлювальної енергетики, формування екологічного мислення під загрозою кліматичних змін. Інноваційний розвиток відновлювальної енергетики знаходить свій прояв у розробці та поширенні новітніх технологічних процесів та технологій отримання енергії з відновлювальних джерел, а також її постачання. Освоєння нових технологій транспортування енергії, впровадження енергоефективних, ресурсозберігаючих технологій,

освоєння альтернативних джерел енергії визнається одним зі стратегічних напрямів діяльності нашої країни [3, с. 173].

Оскільки Україна – енергозалежна країна, то в умовах сталого розвитку її першочерговим завданням виступає подолання енергетичної кризи. Саме інновації, пов'язані з високотехнологічним виробництвом, екологозбалансованим використанням природно-ресурсного потенціалу, забезпеченням екологічної безпеки, вжиттям заходів із ресурсозаміщення (на відновлювальні джерела енергії), сприяють захисту публічних інтересів держави від зовнішніх і внутрішніх загроз. З огляду на це при розробці інноваційних засад реформування енергетичної галузі законодавці і науковці орієнтуються на: енергоефективність, формування конкурентних енергетичних ринків, диверсифікація енергопостачання, збільшення в енергетичному балансі частки альтернативних джерел енергії і видів палива [1, с. 159-167].

Стратегічні орієнтири розвитку паливно-енергетичного комплексу України на період до 2035 року визначено Розпорядженням Кабінету Міністрів України від 18 серпня 2017 р. № 605-р «Про схвалення Енергетичної стратегії України на період до 2035 року "Безпека, енергоефективність, конкурентоспроможність" У преамбулі документу зазначається, що Україна є і в перспективі прагне залишатися одним із найбільших в континентальній Європі виробником вуглеводнів та надійним транзитером енергоресурсів (в першу чергу природного газу і нафти), забезпечуючи безпечне і надійне постачання енергоресурсів власним споживачам та споживачам суміжних ринків, які мають бути видобуті та доставлені з високим рівнем екологічної та соціальної відповідальності, з докладанням зусиль для дотримання зобов'язань зі скорочення викидів парникових газів. Метою Стратегії є забезпечення потреб суспільства та економіки в паливно-енергетичних ресурсах у технічно надійний, безпечний, економічно ефективний та екологічно прийнятний спосіб для гарантування поліпшення умов життєдіяльності суспільства [4].

Еколого-правове регулювання є невід'ємною частиною правової системи, яка спрямована на забезпечення екологічної безпеки та відновлення природних ресурсів. У контексті енергетичної галузі, це означає встановлення норм, що обмежують вплив виробництва енергії на довкілля, а також сприяють використанню енергетичних джерел з найменшим негативним екологічним впливом.

Запровадження сучасних технологій та використання альтернативних джерел енергії стають стратегічними напрямками вирішення проблем, пов'язаних з негативним впливом енергетичного сектору на навколишнє середовище. Ефективне еколого-правове регулювання сприяє стимулюванню

інновацій у сфері енергетики та сприяє переходу до екологічно чистих технологій.

Отже, Еколого-правова складова є необхідним елементом в управлінні енергетичною галуззю для забезпечення сталого розвитку та екологічної безпеки. Інтеграція екологічних принципів у правовій системі сприяє досягненню гармонії між потребами суспільства та природним середовищем, забезпечуючи довгострокову стійкість енергетичної галузі та збереження природних ресурсів для майбутніх поколінь.

Список використаних джерел:

1. Гетьман А. П. Анісімова Г. В. Проблеми законодавчого забезпечення державної інноваційної й екологічної політики у сфері використання природно-ресурсного потенціалу України в енергетичній галузі. Економіко-правові проблеми розвитку та сприяння господарській діяльності в сучасних умовах : збірник матеріалів круглого столу (м. Харків, 25 травня 2018 р.) / редкол.: М. П. Кучерявенко, О. О. Дмитрик, С. В. Глібко. Харків : Право, 2018. С. 159-167/
2. Краснова М. В. Регулювання відновлювальної енергетики в системі законодавства і права України: науково-методологічні аспекти. П’яте зібрання фахівців споріднених кафедр з проблем аграрного, земельного, екологічного, природоресурсного права та альтернативної енергетики : матер. Всеукр. наук. конф. (м. Одеса, 10-13 червня 2021 року) / відп. Ред. Т. Є. Харитонова, Х. А. Григор’єва. Одеса: Видавництво дім «Гельветика», 2021. 332 с.
3. Правове забезпечення адаптації інвестиційної моделі розвитку економіки України та ринків фінансових послуг до права Європейського Союзу : монографія / [С. В. Глібко, Н. М. Внукова, О. О. Дмитрик та ін.] ; за ред. С. В. Глібка, Н. М. Внукової, О. О. Дмитрик. Харків: Право, 2017. 400 с.
4. Про схвалення Енергетичної стратегії України на період до 2035 року “Безпека, енергоефективність, конкурентоспроможність”. Розпорядження Кабінету Міністрів України від 18 серпня 2017 р. № 605-р. Урядовий кур’єр від 08.09.2017. № 167.

УДК 342.1

Карина САЛАЄВА
кандидатка юридичних наук, доцентка кафедри кримінального права та кримінології факультету №6 Харківського національного університету внутрішніх справ, м. Харків, Україна
e-mail: salaievaa@gmail.com, ORCID: 0000-0003-2991-946X

АНАЛІЗ ЗАСАД ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: Запропоноване дослідження спрямоване на вивчення стратегій, методів та інструментів, що застосовуються у державній політиці для захисту важливих об'єктів критичної інфраструктури від потенційних загроз, таких як кібератаки, терористичні акти, природні катастрофи та інші небезпечні події. Аналізується роль державних органів у

формуванні та впровадженні політики забезпечення безпеки критичної інфраструктури, включаючи розроблення стратегій превентивних заходів, планування реагування на кризові ситуації та відновлення після них. Робиться акцент на розробці комплексних планів заходів, які враховують специфіку різних видів критичної інфраструктури, таких як енергетика, транспорт, телекомунікації, фінансові та інші сектори, а також їх взаємодію.

Ключові слова: критична інфраструктура, засади забезпечення безпеки критичної інфраструктури, державна політика, захист критичної інфраструктури.

ANALYSIS OF THE PRINCIPLES OF STATE POLICY IN THE SPHERE OF CRITICAL INFRASTRUCTURE PROTECTION

Abstract: The proposed research is aimed at studying the strategies, methods and tools used in public policy to protect important critical infrastructure objects from potential threats such as cyber and terrorist acts, natural disasters and other dangerous events. The role of state bodies in the formation and implementation of critical infrastructure security policies is analyzed, including the development of strategies for preventive measures, planning for response to crisis situations and recovery after them. Emphasis is placed on the development of comprehensive action plans that take into account the specifics of various types of critical infrastructure, such as energy, transport, telecommunications, financial and other sectors, as well as their interaction.

Keywords: critical infrastructure, principles of critical infrastructure security, state policy, protection of critical infrastructure.

Сучасний світ стикається зі зростаючими викликами, пов'язаними зі збільшенням кількості кібератак, кліматичними катастрофами та іншими небезпеками, що загрожують стабільності і розвитку суспільства. Крім того, необхідно враховувати важливі аспекти щодо забезпечення надійності, цілісності та доступності критичної інфраструктури, зокрема в контексті цифрової безпеки та захисту від кіберзагроз. Важливо враховувати правовий контекст, що регулює ці питання, а також розглядати роль державних і недержавних суб’єктів у забезпеченні сталості і безпеки інфраструктури, вплив міжнародних стандартів на формування внутрішніх політик забезпечення безпеки критичної інфраструктури.

У світлі вищезазначеного, мета запропонованого дослідження полягає в аналізі публічно-правових засад безпеки та сталого розвитку критичної інфраструктури з урахуванням положень вітчизняного законодавства, а також визначення оптимальних стратегій та механізмів, які можуть забезпечити сталість, надійність та безпеку критичної інфраструктури в умовах сучасних викликів та загроз. Захист критичної інфраструктури – цілеспрямована взаємоузгоджена спільна діяльність державних інститутів, власників та операторів об’єктів критичної інфраструктури, спрямованих на профілактику, запобігання і своєчасне виявлення потенційних та припинення або нейтралізацію реальних загроз; мінімізацію та ліквідацію наслідків та швидке

відновлення функціонування критичної інфраструктури у разі її пошкодження, що реалізовуються з метою уникнення людських жертв, значних матеріальних та екологічних збитків, або інших драматичних наслідків, які можуть призвести до порушення національної безпеки й оборони [3]. Крім того, для України наразі важливо визначити ці засади, беручи до уваги постійні ракетні атаки та інші небезпеки, які загрожують нашій державі під час воєнного стану.

Критичною інфраструктурою є система важливих об'єктів національної інфраструктури, що забезпечують стале функціонування енергетики, ядерної та хімічної промисловості, транспорту та зв'язку, банків та фінансових установ, системи інформаційних технологій та телекомунікацій, продовольчої галузі, системи охорони здоров'я, а також галузей комунального господарства тощо. Вони є важливими для успішного функціонування та розвитку економіки, забезпечення безпеки суспільства та держави, можуть призвести до значних матеріальних збитків, незворотні людських жертв та витрат. Крім того, виведення їх з ладу, руйнування чи знищення негативно позначиться на національній безпеці або обороні України [1, с. 153].

Законодавчі засади державної політики у сфері захисту критичної інфраструктури закріплені у Законі України «Про критичну інфраструктуру» (далі – Закон) [2]. У статті 4 зазначеного Закону сформульовано 8 принципів, на яких базується державна політика у сфері її захисту. Першим складовим елементом засад, визначених у спеціальному законі є «визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури». Це означає, що суб'єкти, залучені до роботи з критичною інфраструктурою мають усвідомлювати важливість захисту та підтримки елементів і систем, які є життєво важливими для нормального функціонування суспільства, економіки та держави в цілому. Таке розуміння спонукає уряд та органи управління до розробки та впровадження стратегій, політик та практичних заходів, спрямованих на попередження та ліквідацію можливих загроз та забезпечення стійкості усіх важливих систем. Воно також включає в себе співпрацю з різними зацікавленими сторонами, в тому числі приватним сектором, міжнародними партнерами та громадськістю, з метою розробки комплексних стратегій та заходів, спрямованих на забезпечення надійності та безпеки критичної інфраструктури.

У п. 2 ч. 2 ст. 4 Закону, що аналізується, закріплена засада «визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури». Можемо говорити, що це механізм розробки і прийняття законодавчих актів, які конкретизують принципи та підходи, які повинні бути використані для забезпечення безпеки та стійкості

критичних систем. Це створює правову основу для удосконалення та впровадження стратегій, планів дій та практичних заходів у цій сфері. Крім того, це може включати в себе розробку технологічних рішень, поліпшення систем моніторингу та реагування, розвиток планів відновлення та інші практичні заходи. Стратегічні завдання визначають конкретні цілі та завдання, які мають бути досягнуті у процесі забезпечення безпеки критичної інфраструктури. Вони можуть охоплювати такі аспекти, як вдосконалення кібербезпеки, планування надзвичайних ситуацій, розвиток запобіжних заходів та інші, що спрямовані на мінімізацію ризиків та підвищення стійкості.

Досліджуючи третю засаду державної політики у сфері захисту критичної інфраструктури («визначення суб’єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії»), хочемо наголосити на тому, що це установлення структури та ролей різних суб'єктів, які беруть участь у захисті критичної інфраструктури в межах держави. Це включає розподіл відповідальності та повноважень між різними урядовими органами, державними установами, приватним сектором та іншими зацікавленими сторонами.

Наступним принципом безпеки і розвитку відповідно до Закону є «створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх виді». Така засада означає, що ліквідація та/або мінімізація наслідків реалізованих загроз, кризових ситуацій та інших їх видів включає в себе розробку та впровадження планів надзвичайних ситуацій, оперативних дій у разі виникнення кризових ситуацій, а також механізмів реагування на аварійні ситуації. Це передбачає планування та тренування персоналу, створення механізмів відновлення після кризових ситуацій та інші заходи, спрямовані на мінімізацію наслідків можливих загроз та забезпечення швидкого відновлення нормального функціонування системи, впровадження комплексних стратегій та заходів, спрямованих на попередження, зниження та управління ризиками, пов'язаними з можливими загрозами для критичної інфраструктури.

П. 5 ч. 2 ст. 4 Закону закріпив ще один важливий принцип. «Створення системи раннього виявлення загроз критичній інфраструктурі» означає встановлення комплексу механізмів та процедур, спрямованих на вчасне виявлення потенційних загроз, що можуть виникнути для різних елементів критичної інфраструктури. Це включає в себе визначення певних сигналів, які можуть свідчити про можливі небезпечні ситуації, а також встановлення механізмів їх моніторингу та аналізу. Створення такої системи базується на

впровадженні спеціальних сенсорів, моніторів та інших технічних засобів, які дозволяють виявляти аномальні або підозрілі події в реальному часі. Ці системи можуть бути основані на використанні сучасних технологій моніторингу, супроводження та аналізу даних, таких як системи відеоспостереження, системи виявлення вторгнень, системи контролю якості повітря та води тощо. Основна мета створення системи раннього виявлення загроз полягає в тому, щоб мати можливість вчасно реагувати на потенційні небезпеки та уникнути серйозних наслідків для критичної інфраструктури та суспільства в цілому. Це передбачає визначення певних показників, які свідчать про можливі загрози, та встановлення механізмів автоматичного або частково автоматичного сповіщення відповідальних органів та служб для подальшої реакції.

Шостий принцип державної політики у сфері захисту критичної інфраструктури є «запровадження державно-приватного партнерства, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури», що є встановленням спільної співпраці між державними органами, приватним сектором та населенням з метою підвищення ефективності заходів з безпеки та стійкості критичних систем. Це включає спільні зусилля уряду та приватних компаній щодо розробки та впровадження стратегій, технологій та інновацій, спрямованих на забезпечення надійності та безпеки критичної інфраструктури. Державно-приватне партнерство дозволяє комбінувати ресурси та експертизу обох сторін для досягнення спільних цілей у сфері безпеки. Взаємодія з населенням також є важливою складовою державно-приватного партнерства у сфері безпеки критичної інфраструктури. Це включає в себе залучення громадськості до процесу планування, реалізації та оцінки заходів з безпеки, а також надання належної інформації та інструкцій щодо поведінки в надзвичайних ситуаціях. Широке залучення населення допомагає покращити свідомість про потенційні загрози та збільшити загальний рівень підготовки до можливих кризових ситуацій.

«Забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури» (сьома засада) означає встановлення та підтримку взаємодії між різними країнами, міжнародними організаціями та іншими зацікавленими сторонами з метою спільного вирішення проблем безпеки та стійкості критичних систем на глобальному рівні. Це включає обмін інформацією, досвідом та найкращими практиками. Крім того, забезпечення міжнародного співробітництва також охоплює спільне планування та проведення навчань, тренувань та симуляцій з метою підвищення готовності та реагування на кризові ситуації. Це допомагає підвищити координацію та ефективність

міжнародних зусиль у вирішенні загроз критичній інфраструктурі та зменшити вплив можливих кризових ситуацій на глобальному рівні.Міжнародне співробітництво у сфері захисту критичної інфраструктури є важливим елементом глобальної стратегії безпеки, оскільки воно дозволяє об'єднувати зусилля різних країн та міжнародних організацій для забезпечення безпеки та стійкості критичних систем у всьому світі.

І наостанок, варто проаналізувати принцип «створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури». Це розробка стратегій, планів та механізмів, спрямованих на мінімізацію перерв у наданні важливих послуг та функцій, необхідних для життєдіяльності суспільства. Це включає створення запасних механізмів, резервних систем та альтернативних шляхів постачання послуг, які можуть бути активовані у випадку непередбачуваних ситуацій або кризових подій. Такі механізми можуть включати резервування запасних джерел енергії, резервування даних, планування евакуації та резервних комунікаційних систем, а також інші запобіжні заходи.Додатково, це включає розробку та впровадження планів відновлення, які передбачають швидке відновлення функцій критичної інфраструктури після кризових ситуацій. Це може охоплювати у собі планування та тренування персоналу, використання автоматизованих систем відновлення, розробку планів постачання необхідних ресурсів та координацію з відповідними органами для швидкого реагування та відновлення нормального функціонування.Створення умов швидкого відновлення надання життєво важливих функцій та послуг в разі реалізації загроз і порушення функціонування критичної інфраструктури є важливою складовою стратегії забезпечення стійкості та безпеки суспільства в умовах можливих кризових ситуацій.

У результаті запропонованого дослідження можна зробити висновки про ефективність існуючих стратегій та виявити недоліки, що потребують подальшого вдосконалення, зокрема шляхом розробки нових політичних ініціатив, законодавчих актів та міжнародних угод для підвищення рівня захисту критичної інфраструктури у вимірі національної та міжнародної безпеки.

Список використаних джерел:

1. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпропетр. держ. ун-т внутр. справ, 2018. С. 153-154.

2. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX. Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 04.11.2023).

3. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток*. 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2610 (дата звернення: 04.11.2023). DOI: 10.32702/2307-2156-2022.1.38

УДК 351:346

Володимир СЕЛЕВКО
кандидат філософських наук, завідуючий відділом аспірантури та докторантури Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: v.selevko@khai.edu, ORCID: 0000-0002-9543-4981
Ірина ТУР
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права) Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: i.tur@khai.edu, ORCID: 0000-0003-1630-7878

ЩОДО ПИТАННЯ НЕ ЗАПРОВАДЖЕННЯ МАРАТОРІЮ НА ПРОЦЕДУРУ БАНКРУТСТВА ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Анотація: у доповіді розглянуті питання об'єктивних обставин не запровадження мораторію на банкрутство об'єктів критичної інфраструктури під час військового стану, що було обумовлено загрозою для економічних процесів в умовах ринкової економіки.

Ключові слова: об'єкти критичної інфраструктури, військовий стан, мораторій, банкрутство, зловживання становищем, ринкова економіка.

ON THE ISSUE OF NOT INTRODUCING A MORATORIUM ON THE BANKRUPTCY PROCEDURE FOR CRITICAL INFRASTRUCTURE OBJECTS DURING MARTIAL LAW

Abstract: the report examines the objective circumstances of not introducing a moratorium on the bankruptcy of critical infrastructure objects during martial law, which was caused by a threat to economic processes in the market economy.

Keywords: critical infrastructure facilities, martial law, moratorium, bankruptcy, abuse of position, market economy.

Для стабільного і безпечного існування сучасне суспільство та його члени мають надійно отримувати цілу низку самих різноманітних продуктів і послуг, мати доступ до ряду важливих ресурсів тощо. Для цього створюються і використовуються певні об'єкти, мережі та системи,фізичні або віртуальні.

Відповідно до Закону України «Про критичну інфраструктуру» до об’єктів критичної інфраструктури відносяться 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. Після початку повномасштабної військової агресії рф проти України та введення воєнного стану на всій території нашої держави, переважна більшість підприємств та сфер послуг, зупинили свою роботу. Незважаючи на намагання законодавця внести зміни до ст. 8 Закону України "Про критичну інфраструктуру" (щодо врегулювання спорів, предметом яких є право власності держави на об’єкти критичної інфраструктури, що перебувають у державній власності) під час воєнного стану. Законопроектом передбачалось запровадження мораторію на банкрутство об’єктів критичної інфраструктури, які перебувають у державній власності до завершення воєнного стану та протягом два років після його скасування. Тим не менш зміни у відповідний Закон не було внесено.

Кодекс України з процедур банкрутства також не зазнав суттєвих до відповідної проблем змін. Виходячи з того, що зруйновані логістичні ланцюжки, втрачені через окупацію або знищені виробничі активи,негативно вплинуло на можливість виконувати зобов’язання. В таких умовах на думку експертів саме банкрутство залишається потужним інструментом для відновлення платоспроможності або законного виходу з господарської діяльності для боржника та надає можливість кредиторам забезпечити повернення боргів.

Це, на думку експертів змушує учасниківукраїнської економіки домовлятись домовлятися між кредиторами і боржниками з розумінням ставляться до збереження бізнесу кожного з них. Кредитори, в т.ч. банки, за можливості, будуть намагатися врегулювати відносини з позичальниками шляхом реструктуризації кредитів, надання кредитних канікул та утримання від агресивних дій по примусовому стягненню заборгованості. Значно виріс попит на послуги з супроводу процедур реструктуризації. З такими запитами звертаються як кредитори, так і боржники.

Натомість законодавець своєю чергою запровадив мораторій на нарахування штрафних санкцій щодо прострочених кредитних зобов’язаннях, що має додатково підтримати бізнес на час дії воєнного стану.

Таким чином, не запровадження мораторію на банкрутства об’єктів критичної інфраструктури пояснюється виникнення більшої шкоди для економіки, коли б недобросовісні боржники використали б його для процедурних зловживань. А це викликало б масове невиконання зобов’язань у всіх секторах економіки. Тому у висновку законодавець сподіваючись на

можливості ринкової економіки до саморегулювання та до самовідновлення не реалізував наміри про обмеження прав кредиторів на стягнення боргових зобов'язань.

Список використаних джерел:

1. Закон України «Про критичну інфраструктуру» № 1882-IX ВР. Редакція від 05.12. 2022 URLhttps://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Зелена книга з питань захисту критичної інфраструктури в Україні. – Київ, 2015. - 305 С.
3. Проект Закону про внесення зміни до статті 8 Закону України "Про критичну інфраструктуру" (щодо врегулювання спорів, предметом яких є право власності держави на об'єкти критичної інфраструктури, що перебувають у державній власності) № 3369-IX від 05.09.2023https://itd.rada.gov.ua/billInfo/Bills/Card/41078

УДК 629.7.062

Олексій ТРЕТЯК
доктор технічних наук, доцент, завідувач кафедри аерогідродинаміки
Національного аерокосмічного університету ім. М. Є. Жуковського
"Харківський авіаційний інститут", м. Харків, Україна
e-mail: o.tretyak@khai.edu, ORCID: 0000-0002-7295-5784

СТВОРЕННЯ НОВИХ КОНСТРУКЦІЙ ГЕНЕРУЮЧОГО ОБЛАДНАННЯ

Анотація: У цій доповіді розглянуто тенденції до збільшення потужності електрогенеруючого обладнання при зменшенні масо-габаритних характеристик на одиницю потужності. Доведено необхідність розробки та використання ефективної методології, що буде враховувати весь цикл розрахунків для електричних генераторів у тривимірній постановці при створенні нових конструкцій генеруючого обладнання.

Ключові слова: електрогенеруюче обладнання, збільшення потужності, напружено-деформований стан, метод скінченних елементів.

DEVELOPMENT OF THE NEW DESIGNS OF GENERATING EQUIPMENT

Abstract: This report examines the trends in increasing of power of the power generating equipment while reducing the mass-dimensional characteristics per unit of power. The need to develop and use the effective methodology that will take into account the entire cycle of computations for electric generators in the three-dimensional setting when creating new designs of generating equipment is proven.

Keywords: electric generating equipment, power increase, stress-strain state, finite element method.

Сучасному електрогенераторобудуванню характерні тенденції до збільшення потужності електричних агрегатів, зменшення їх масо-габаритних характеристик на одиницю потужності, а також ускладнення умов роботи генераторів, що призводить до збільшення міжремонтних періодів і термінів експлуатації, зростання часу їх використання на надпроєктних режимах. У зв'язку з цим підвищуються загальні вимоги до надійності енергомашино-будівного обладнання в цілому і, зокрема, до міцності окремих конструкційних елементів генераторів. У зв’язку з цим, при розробці нових конструкцій електрогенеруючого обладнання, особливого значення набувають дослідження напружено-деформованого стану (НДС) елементів та вузлів генераторів в тривимірних постановках, які дозволяють оцінити реальний запас міцності конструкцій, що надзвичайно важливо як при проектуванні нових генераторів з покращеними техніко-економічним показниками, так і при модернізації існуючого обладнання.

Проектування та виготовлення нових машин, конкурентних на світовому ринку, а також ефективна модернізація існуючих агрегатів неможлива без удосконалення методів розрахунку міцності їх елементів та застосування новітніх комп’ютерних засобів для аналізу їх напружено-деформованого стану. В усьому світі спостерігається стала тенденція до збільшення потужності генераторів та зменшення їх ваги, що призводить до підвищення рівня напружень у елементах та їх перерозподілу, а це також вимагає більш удосконалених методів розрахунку їх міцності.

Складність аналізу НДС елементів конструкцій та вузлів електрогенераторів обумовлена, перш за все, необхідністю розв’язання цілого комплексу задач – газодинамічної, температурної та термопружної – для аналізу їх міцності при впливі температурних та силових навантажень. Елементи конструкцій генератора працюють в умовах складного навантаження, викликаного спільною дією інерційних сил від обертання ротора, сил тяжіння, навантажень, що виникають від посадок деталей з натягом, а також температурних навантажень, які виникають, перш за все, внаслідок виділення тепла в активному контурі і визначаються параметрами роботи системи їх примусового вентилювання. При комплексному проектуванні генератора це призводить до необхідності розгляду цілого комплексу задач, пов'язаного з визначенням термонапруженого стану конструкцій, ускладненого попередніми натягами, впливом температурних полів, що залежать від параметрів роботи систем вентилювання та багатьох інших факторів.

Більшість елементів конструкцій генераторів працюють в умовах помірного нагріву. Але, у випадку великих електричних машин, значні їх

геометричні розміри можуть приводити до появи істотних переміщень та додаткових зусиль на сусідні елементи та опори, що також необхідно враховувати для генераторів великої потужності. Крім того, для цього класу машин існують особливі обмеження щодо можливої маси, геометричних параметрів ротора та генератора, які викликані неможливістю забезпечити їх необхідну міцність та жорсткість, а також транспортування до місця встановлення.

Довгий час основні розрахунки міцності елементів конструкцій генераторів проводилися аналітично за інженерними методиками, заснованими на теорії опору матеріалів. В останні десятиліття спостерігається стрімкий розвиток чисельних методів для аналізу НДС елементів конструкцій генераторів. Зараз найчастіше для дослідження їх міцності застосовуються чисельні методи, засновані на методі скінченних елементів (МСЕ). Основна особливість сучасного етапу полягає в переході від більш простих моделей до складніших, які мають більш високу точність і універсальність.

Таким чином, розробка ефективної методології, що буде враховувати весь цикл теплових, вентиляційних та механічних розрахунків для електричних генераторів у тривимірній постановці для уточненої оцінки міцності елементів їх конструкцій при впливі номінальних і надномінальних (аварійних) навантажень дозволить здійснювати створення нових конструкцій електрогенеруючого обладнання збільшеної потужності зі зниженням їх масо-габаритних показників на одиницю потужності.

Список використаних джерел:

1. Valavi M., Nysveen A., Nilsen R., Le B. J., Devillers E. Analysis of magnetic forces and vibration in a converter-fed synchronous hydrogenator. 2017 IEEE Energy Conversion Congress and Exposition (ECCE), Cincinnati, OH, USA, 2017, P. 1838-1844. URL: https://doi.org/10.1109/ECCE.2017.8096018.
2. Tretiak O., Kritskiy D., Kobzar I., Sokolova V., Arefieva M., Tretiak I., Hromenko D., Nazarenko V. Modeling of the Stress–Strain of the Suspensions of the Stators of High-Power Turbogenerators. Computation. 2022; 10(11):191. URL: https://doi.org/10.3390/computation10110191.
3. Tretiak O.; Kritskiy D.; Kobzar I.; Arefieva M., Nazarenko V. The Methods of Three-Dimensional Modeling of the Hydrogenerator Thrust Bearing. Computation 2022, 10, 152. URL: https://doi.org/10.3390/computation10090152.
4. Tretiak, O.; Kritskiy, D.; Kobzar, I.; Arefieva, M.; Selevko, V.; Brega, D.; Maiorova, K.; Tretiak, I. Stress-Strained State of the Thrust Bearing Disc of Hydrogenerator-Motor. Computation 2023, 11, 60. URL: https://doi.org/10.3390/computation11030060.

JEL Classification: G28, K12
Yevgenia TUPITSKA
PhD in Law, Docent of the Department of Civil and Legal Policy,
Intellectual property Law and Innovations,
Yaroslav Mudryi National Law University, Kharkiv, Ukraine;
e-mail: evgeniya.ta@gmail.com, ORCID: 0000-0002-7484-9723

PRIVATE LEGAL MEANS OF PROTECTING THE RIGHTS OF PARTICIPANTS IN CREDIT AND FINANCIAL RELATIONS IN THE CONDITIONS OF WAR IN UKRAINE

Abstract: The thesis of the report is investigatedthe peculiarities of legislative changes that took place in the field of credit regulation and were implemented in Ukrainian legislation in connection with the introduction of martial law as a result of the armed aggression of the Russian Federation. The impact of crisis situations on the functioning of the country's financial sector is analyzed and a conclusion is made about the effectiveness of their legislative regulators.

Keywords: debt, debt liability, money, credit, bond, loan, credit relationship, safety measures.

Credit relations in Ukraine, as in any country with a market economy, form the foundations of economic processes. Today, the country is experiencing a deep crisis in the financial sector, which is due to the full-scale military invasion of Russia on the territory of Ukraine, and will lead to significant negative and long-term consequences in the future. In connection with the general tendency of individuals and business representatives not to return borrowed loan funds, the state faces serious challenges regarding the stabilization of the financial and credit system. The latter is possible through the implementation of the necessary legislative regulators, which will be able to ensure the support of the interests of both borrowers and lenders, as well as the spread of various guarantee programs of state support of financial institutions and consumers of their services in various areas of financial activity.

When considering the concept of credit legal relations, it should first of all be noted that they can be defined as relations of a contractual nature, which consist in the postponement of the fulfillment of an obligation under a retaliatory contract or the transfer by the creditor of money or other things, determined by generic features, for a fee on the condition of returning their equivalent in a certain term. Such a broad interpretation of this concept is not accidental. Credit obligations arise as a result of their parties committing various transactions, which, as a rule, are drawn up in the form of credit agreements between the bank and borrowers. Thus, the legislator provides various contractual constructions, which include credit obligations and to which the relevant legal provisions can be applied. Among them, we can name commercial lending (Article 1057 of the Civil Code of Ukraine), novation of debt

into a loan obligation (Article 1053 of the Civil Code of Ukraine), factoring agreements, financial leasing, insurance, investment legal relations, etc. [4, p. 152].

Elements of a credit contractual obligation are subjects, objects, and content (subject) [1, p. 37]. It is worth noting that one of the subjects of the credit agreement is always a legal entity that can participate in the indicated transaction both on the side of the creditor and the borrower of funds.

Attention should be paid to legislative changes regulating the activities of financial institutions during the period of martial law in Ukraine [3, p. 48]. Thus, on February 11, 2022, the Law of Ukraine "On Financial Services and Financial Companies" entered into force, according to which non-banking financial institutions located in the temporarily occupied territories and the territories of the Joint Forces Operation as of the date should be excluded from the relevant state registers entry into force of the specified law. In addition, institutions that do not have valid licenses on the date of entry into force of the law must leave the market. In addition, on August 16, 2022, the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding the Features of the Financial Sector in Connection with the Introduction of Martial Law in Ukraine" dated July 27, 2022 No. 2463-IX was published. This normative act provides that: during the period of martial law in Ukraine, introduced by the Decree of the President of Ukraine "On the introduction of martial law in Ukraine" dated February 24, 2022 No. 64/2022, approved by the Law of Ukraine "On the approval of the Decree of the President of Ukraine "On the introduction of martial law of the State of Ukraine" dated February 24, 2022 No. 2102-IX, the supervisory board of the credit union has the right to make a decision on the temporary suspension of the credit union's activities [3].

Also, considering the activities of legal entities acting as creditors under credit agreements, one cannot ignore the problematic issues that arise in connection with the nationalization or liquidation of legal entities whose activities were associated with the aggressor state. In particular, it is worth referring to the judicial practice and indicating the Resolution of the KGS of the Supreme Court of July 20, 2022 in case No. 910/4210/20. In this case, the Supreme Court had to resolve the issue of whether the collection of the debts of the Russian Federation against a block of shares of a Ukrainian bank owned by a resident of the Russian Federation was legally enforced. The purpose of removing the corporate veil is to settle the imbalance of interests that arises between the participants of the legal relationship as a result of the abuse of the limited liability or autonomy of the corporation. The Supreme Court has already applied the doctrine of the lifting of the corporate veil (non-recognition of the independent legal personality of a legal entity, the separation of its property from the property of the participants), in particular, solving the issue of responsibility for the damage caused. At the same time, the application of this rule to legal entities

created by a foreign state has considerable specificity. It is generally accepted that the state is responsible for the actions of state bodies and its bodies, even if they are formally separate legal entities, are responsible for the actions and debts of the state. Whereas state-owned companies, which are separate legal entities, are not responsible for the state's debts. At the same time, state authorities can recognize not only those organizations that have the appropriate status in the national law of the debtor state, but also, under certain conditions, state companies.Examining the materials of the case, the court concluded that the government of the Russian Federation actually considered the relevant financial institution not as an independent legal entity that engages in entrepreneurial activity at its own discretion and risk, but as a financial body of the state, since it fulfills the goals, functions and tasks inherent in the state bodies, is under close control of the Russian Federation. Accordingly, the Court ruled that the property of such a legal entity, which is located on the territory of Ukraine, may be levied on the debts of the Russian Federation [5].

When considering the specifics of the participation of an individual on the side of the borrower in the credit agreement, attention should be paid to certain legislative changes regarding the establishment of certain categories of so-called "protected persons", which, in particular, include military personnel and internally displaced persons, who may be provided with additional state guarantees in the field lending Such persons are recognized as a) military personnel, including those who became disabled as a result of hostilities; b) representatives of military formations and special law enforcement agencies, the State Special Transport Service, the State Service for Special Communication and Information Protection of Ukraine, who are doing military service on the territory of Ukraine, members of the families of servicemen who were killed, died or went missing; persons in captivity; persons with whom contact has been lost, persons who are missing. Also, socially protected persons include persons deprived of liberty [6]. Thus, the Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding the Settlement of Overdue Debts During the Period of Martial Law in Ukraine" dated July 27, 2022 No. 2459-IX [7] provides that during the settlement of overdue debts during the period of martial law and within 90 days from the date of its termination or cancellation, the creditor and legal entities involved on a contractual basis by the creditor, the collection company in direct interaction with the consumer, are obliged to comply with the requirements for ethical behavior.In particular, it is forbidden to interact on one's own initiative with a consumer who, in the manner provided for in this clause, has informed about his/her belonging to a protected category. Thus, the Law of Ukraine "On Social and Legal Protection of Persons Deprived of Personal Liberty as a Result of Armed Aggression Against Ukraine and Members of Their Families" dated January 26, 2022 No. 2010-IX provides that persons deprived of personal

liberty freedom as a result of armed aggression against Ukraine, for the period of deprivation of personal freedom and within six months after release, are released from the obligation to fulfill obligations, as well as from accrual and payment (transfer) of penalty (fine, penalty) for violation of obligations. After the dismissal, such persons have the right to carry out the restructuring of their debt; the wife (husband) of a person who has been deprived of personal liberty as a result of armed aggression against Ukraine also has the right to restructure their debts for loans to banks and other financial institutions [6].

In addition, it should be noted that in order to protect and harmonize the credit and financial system of Ukraine, as well as to increase the demand for attracting credit funds on the domestic credit market, a number of legislative changes were adopted during the martial law in Ukraine. Thus, the legislator introduced the relevant changes through the adoption of the Law of Ukraine "On Amending the Tax Code of Ukraine and other legislative acts of Ukraine regarding the effect of norms during the period of martial law" dated March 15, 2022 No. 2120-IX [7]. This law amended the Civil Code of Ukraine and the Law "On Consumer Credit". The National Bank of Ukraine adopted the "Rules of operation of banks in connection with the introduction of martial law in Ukraine", approved by the resolution of the board of the National Bank of Ukraine No. 23 dated 03.25.2022 "On some issues of the activities of banks of Ukraine and banking groups" [2, p. 9].

As a conclusion, I would like to note that in addition to the fact that our state defends the freedom of every Ukrainian and sovereignty on its own territory, it also does not stop work in law-making activities with the aim of adapting the norms of law to the economic and social realities that arose due to the military invasion of the Russian Federation to Ukraine. Of course, rule-making is a multi-stage and collegial process that requires constant work, a systematic approach and constant updating. In our opinion, the provisions of normative legal acts and legislative projects in the field of execution of credit agreements need significant revision.This is especially acutely related to the provision of stable guarantees in the activity and functioning of a business that has a loan and the performance of which is secured by a mortgage, as well as the final resolution of the issue regarding the destroyed or damaged mortgaged property of the debtor.

References:

1. Bernaz-Lukavetska O. Vyznachennia poniattia finansovoho kredytu za zakonodavstvom Ukrainy (Definition of a financial loan under Ukrainian law) Rol prava ta zakonu v hromadskomu suspilstvi: Materialy mizhnarodnoi naukovo-praktychnoi konferentsii (Proceedings of the international scientific and practical conference) Kyiv, 10.02.2017) – K.: Tsentr pravovykh doslidzhen, 2017, p. 37-39.

2. Bilenko M. Novely zakonodavstva v bankivskii sferi v umovakh voiennoho stanu (New legislation in the banking sector under martial law). Nove ukrainske pravo, No 2, 2022, p. 9-14

3. Lepekh S. Poniattia dohovoriv pozyky, kredytu ta pozychky za zakonodavstvom Ukraïny (The concept of loan, credit and borrowing agreements under Ukrainian law). Aktualni problemy derzhavy i prava, 2002, No 13, p. 48.

4. Pohrebniak V. Rozvytok vidnosyn spozhyvchoho kredytuvannia v pravovykh systemakh inozemnykh derzhav. (Development of consumer lending relations in the legal systems of foreign countries), Nashe pravo, 2015, № 6, p. 152.

5. Postanova VPVS vid 13.07.2022 v spravi № 363/1834/17 https://reyestr.court.gov.ua/Review/105852863

6. Pro sotsialnyi i pravovyi zakhyst osib, stosovno yakykh vstanovleno fakt pozbavlennia osobystoi svobody vnaslidok zbroinoi ahresii proty Ukrainy, ta chleniv yikhnikh simei (On the social and legal protection of persons in respect of whom the deprivation of personal liberty as a result of armed aggression against Ukraine has been established, and members of their families): Zakon Ukrainy 26.01.2022, № 2010-IX URL: http://www.golos.com.ua/documents/z-2010-ix.pdf).

7. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo vrehuliuvannia prostrochenoi zaborhovanosti u period dii voiennoho stanu v Ukraini (On Amendments to Certain Laws of Ukraine Concerning the Settlement of Overdue Debts During the Period of Martial Law in Ukraine): Zakon Ukrainy vid 27.07.2022, № 2459-IX URL: http://www.golos.com.ua/documents/z-2459-ix.pdf.

УДК 347.4

Артем УШАКОВ
студент 726 ю., гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник
Алла ГОРДЕЮК
доцентка, канд. юрид. наук, доцентка кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: a.hordeiuk@khai.edu, ORCID: 0000-0001-7423-3673

ПРОБЛЕМИ ВИКОНАННЯ ЦИВІЛЬНО-ПРАВОВИХ ЗОБОВ'ЯЗАНЬ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

Анотація: У роботі досліджено зміни у законодавстві, які регламентують питання виконання цивільно – правових зобов'язань у період воєнного стану в Україні. Заначено на норми чинного законодавства, спрямовані на захист прав учасників зобов'язальних відносин через оптимізацію процесу виконання зобов'язання в умовах військової агресії РФ проти України.

Ключові слова: зобов'язання, зобов'язальні відносини, воєнний стан, боржник, кредитор.

PROBLEMS OF FULFILLING CIVIL AND LEGAL OBLIGATIONS DURING MARITAL LAW IN UKRAINE

Abstract:. The work examines changes in the legislation that regulate the issue of fulfilling civil and legal obligations during the period of martial law in Ukraine. It is indicated on the norms

of the current legislation, aimed at protecting the rights of participants in contractual relations through the optimization of the process of fulfilling obligations in the conditions of military aggression of the Russian Federation against Ukraine.

Keywords: Obligation, institution, Martial Law, legislation, contract, property, responsibility.

Зобов'язання є одним із фундаментальних інститутів цивільного права. Правовий концепт зобов’язання у площині цивільного правапередбачає, що одна сторона, яку називають кредитором, має повний законний вплив на іншу сторону, яка є боржником, і може вимагати від неї виконання конкретних дій або утримання від певних дій. Існування зобов'язань базується на таких правових засадах як свобода волі сторін, добросовісність, рівність прав та обов'язків, які визначаються цивільним законодавством [1]. Історія і сучасний стан зобов'язань свідчать про їх важливість і роль у суспільних відносинах.

Зобов'язання мають важливе значення в цивільному обороті, тому що віддзеркалюють принципи справедливості, добросовісності та взаємодії, на яких ґрунтується добросовісний цивільний (господарський оборот). Розуміння особливостей правової регламентації зобов'язань сприяє забезпеченню захиста суб’єктивних прав та інтересів учасників цивільних відносин як в мирний час, так і в умовах сучасних реалій.

Військовий стан, що був уведений Указом Президента «Про введення воєнного стану в Україні» від 24.02.22 р. № 64/2022 зумовив встановлення нових правил у сфері зобов’язальних відносин у зв’язку з тим, що у наслідок військової агресії РФ відбулося наступне: 1) порушення контрактів і договорів; 2) заборгованість перед кредиторами; 3) правовий вакуум; 4) обмеження особистих прав та свобод, що вплинуло на спосіб, яким громадяни можуть виконувати свої цивільні зобов'язання.

Отже, які саме зміни відбулися в українському законодавстві, що регулює зобов’язальні відносини? Так, Законом України від 15 березня 2022 р. № 2120-IX «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо дії норм на період дії воєнного стану» (далі – Закон) доповнено, серед іншого, розділ "Прикінцеві та перехідні положення" Цивільного кодексу України пунктом 18 [1, 2].

Доповнені положення передбачають, що під час тривання воєнного або надзвичайного стану в Україні і впродовж 30 днів після їх закінчення або скасування, якщо позичальник не виконав свої фінансові зобов'язання за договором, відповідно до якого було надано кредит або позику банком або іншим кредитодавцем, позичальник звільняється від відповідальності, передбаченої статтею 625 Цивільного Кодексу, і від обов'язку сплати кредитодавцю неустойки (штрафу, пені) за таке прострочення. Крім того, цей

пункт передбачає, що неустойка (штраф, пеня) та інші платежі, що повинні були б бути сплачені згідно відповідних угод, нараховані з 24 лютого 2022 року за прострочення виконання (невиконання, часткове виконання) таких угод, підлягають списанню кредитодавцем Також, відповідно зазначеного Закону доповнено розділ IV "Прикінцеві та перехідні положення" Закону України "Про споживче кредитування" пунктом 61, де встановлено, що під час дії в Україні воєнного або надзвичайного стану, а також протягом 30 днів після закінчення або скасування цих станів, якщо споживач не виконав свої зобов'язання за договором про споживчий кредит, споживач звільняється від відповідальності перед кредитодавцем за це прострочення. У випадку такого прострочення споживач також звільняється від обов'язку сплатити кредитодавцю неустойку (штраф, пеню) та інші платежі, передбачені договором про споживчий кредит у разі прострочення виконання або невиконання своїх зобов'язань за цим договором. Заборонено збільшення процентної ставки за використання кредиту з інших причин, ніж ті, які передбачені в частині четвертій статті 1056-1 Цивільного кодексу України, у випадку невиконання зобов'язань за договором про споживчий кредит протягом періоду, вказаного у цьому пункті.Крім того, встановлено, що неустойка (штраф, пеня) та інші платежі, визначені договором про споживчий кредит і нараховані починаючи з 24 лютого 2022 року за прострочення виконання або невиконання зобов'язань за таким договором, повинні бути списані кредитодавцем [2, 3].

Таким чином, після аналізу, зазначених вище положень законодавства можна стверджувати, що інститут зобов’язання є гнучким та чутливим до змін під час впровадженого воєнного стану у державі. Зокрема змінилися умови та вимоги до боржника залежно від обставин, що полегшують процедуру виконання його зобов’язання, але не припиняючи його. Тобто відповідні норми спрямовані на захист прав учасників зобов’язальних відносин через оптимізацію процесу виконання зобов’язання в умовах військової агресії проти України.

Список використаних джерел:

1. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо дії норм на період дії воєнного стану: Закон України від 15 березня 2022 р. № 2120-IX. URL.https//zacon.rada.gov.ua/laws/show2120-20#Text (дата звернення 03.11.23).
2. Цивільний кодекс України від 15.01.200р. 435-IV. Редакція від 05.10.2023.URL.https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення 03.11.23).
3. Про споживче кредитування: Закон України від 15.11.2016 р. № 1734-VIII. URL: https://zacon.rada.gov.ua/laws/show/1734-19#Text.Редакція від 10.06.23 (дата звернення 04.11.23).

УДК 343.3
Віталій ФЕДЮК
аспірант Науково-дослідного інституту вивчення проблем злочинності імені акад. В. В. Сташиса НАПрН України, м. Харків, Україна
e-mail: vitalii.fiediuk@ukr.net, ORCID: 0000-0002-6674-2969

ЕТАПИ РОЗБУДОВИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Анотація: У тезах проаналізовано хронологію розвитку нормативно-правової бази України у сфері захисту критичної інфраструктури. Виокремлено п'ять основних етапів розбудови нормативно-правового забезпечення в цій сфері, яке є системною складовою державної політики у сфері національної безпеки. Констатовано, що співпраця з інституціями НАТО та ЄС, а також виклики гібридної війни та воєнного стану стали важливими чинниками побудови та подальшого вдосконалення системи нормативно-правового захисту об'єктів критичної інфраструктури України.

Ключові слова: критична інфраструктура, захист критичної інфраструктури, нормативно-правове забезпечення, національна безпека.

THE STAGES OF DEVELOPMENT OF THE LEGAL PROVISION OF CRITICAL INFRASTRUCTURE PROTECTION OF UKRAINE

Abstract: The thesis analyzes the chronology of the development of the regulatory and legal framework of Ukraine in the field of critical infrastructure protection. Five main stages of the development of regulatory and legal provision in this area, which is a systemic component of state policy in the field of national security, have been singled out. It was established that cooperation with NATO and EU institutions, as well as the challenges of hybrid war and martial law became important factors in the construction and further improvement of the system of regulatory and legal protection of critical infrastructure objects of Ukraine.

Keywords: critical infrastructure, critical infrastructure protection,regulatory and legal provision, national security.

Складна безпекова ситуація в світовому масштабі, існування постійних викликів та загроз щодо економічної, політичної, воєнної, екологічної, інформаційної сфер життя суспільства обумовлюють необхідність створення правового механізму реагування на такі деструктивні явища з метою мінімізації їх небезпечного прояву, а також посилення стійкості до них. Стрижнем такого механізму слугує нормативно-правове забезпечення захисту критичної інфраструктури (далі – КІ), як системної складової державної політики у сфері національної безпеки.

Основні підходи до побудови системи нормативно-правового захисту КІ, пов'язаних із визначенням її концептуальних основ, завдань та вибору моделі функціонування (передусім, враховуючи досвід європейських держав та США з цього питання) поступово знаходять своє закріплення в законодавстві України.

Перший етап розбудови та період нормативно-правового забезпечення захисту КІ України припадає на 2005-2011 рр. Так, в абз. 6 пп. 4 п. 6 Постанови Верховної Ради України «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства» № 3175-IV від 01.12.2005 р. йдеться про доручення Службі безпеки України підготувати пропозиції щодо визначення та захисту критичних інформаційних інфраструктур. Слід констатувати, що наведене положення є першою згадкою про КІ в законодавстві України. Надалі, у п. 4.3.4 та п. 4.3.8 Стратегії національної безпеки, затвердженої Указом Президента України № 105 від 12.02.2007 р., про КІ йдеться у контексті ключових завдань політики національної безпеки у внутрішній сфері, а саме забезпечення енергетичної безпеки (завдання – дієвий захист об'єктів КІ паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій) та убезпечення систем управління об'єктами КІ в аспекті інформаційної безпеки. В межах цього етапу варто відмітити продовження тенденції формалізації ключових засад співпраці України з Організацією Північноатлантичного договору, які стосуються також й окреслення спільних завдань України та Альянсу із захисту життєво важливої інфраструктури, серед якої чільне місце посідають фізичні та кібернетичні системи забезпечення важливих і необхідних видів діяльності економіки та державного управління. Наприклад, згідно з пп. 2 п. 1.2.7 та пп. 1 п. 1.3.1 Положення Цільового плану Україна – НАТО на 2009 рік у рамках Плану дій Україна – НАТО, затвердженим Указом Президента України № 116/2009 від 02.03.2009 р., йдеться про такі завдання, як забезпечення функціонування Єдиної державної інформаційної системи у сфері протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, а також фінансування тероризму з використанням інфраструктури транспортної мережі Національної системи конфіденційного зв'язку (відповідальний орган – Адміністрація Держспецзв'язку), а також проведення засідання Спільної робочої групи Україна – НАТО з питань безпеки енергетичної інфраструктури та питань економічної безпеки.

Другим етапом розбудови нормативно-правових засад захисту КІ України слід вважати період 2011-2015 рр. В межах етапу відбулась активізація експертно-аналітичної діяльності з питань напрацювання концепції вітчизняної моделі захисту КІ. Так, команда фахівців (передусім, Національного інституту стратегічних досліджень (далі – НІСД), м. Київ) при підготовці концептуальних основ захисту КІ зіткнулась з низкою проблем, серед яких неоднозначне розуміння самої ідеї КІ; сумніви, чи потрібна Україні реалізація такої концепції, зважаючи на скрутні матеріальні спроможності держави; спроби включити потенційну систему захисту КІ до інших існуючих

державних систем (цивільного захисту, боротьби з тероризмом тощо) [1, с. 71-72]. Однак, у березні 2011 р. в НІСД було створено Міжвідомчу експертну робочу групу з питань нерозповсюдження зброї масового знищення, боротьби з тероризмом та захисту критичної інфраструктури, в ході діяльності якої захист КІ став однією з основних її предметних сфер. Так, понад третину всіх заходів, організованих робочою групою, були безпосередньо присвячені захисту КІ, включаючи міжнародну конференцію із захисту КІ у вересні 2013 р., проведену за спонсорського сприяння Програми професійного розвитку Офісу зв'язку НАТО в Україні та ПАТ «Укргідроенерго». Крім того, низка проблем, які обговорювалися на засіданнях робочої групи (наприклад, боротьба з ядерним та радіологічним тероризмом, загрози та оцінка ризиків у сфері ядерної безпеки), побічно стосувалися питань забезпечення нормативно-правового захисту КІ. Найбільш помітним результатом даного етапу є підготовка та оприлюднення Зеленої книги з питань захисту КІ (2015), як стратегічного орієнтиру для подальшої розробки нормативно-правової бази. Зокрема, нею констатовано необхідність введення до законодавства терміну «КІ»; визначення мети системи захисту КІ (забезпечення надійності її функціонування та здатності протистояти загрозам); захист КІ полягає не лише в фізичному розумінні, а спрямований на забезпечення стійкості КІ; визначення широкого переліку загроз за принципом «всі небезпеки» (надзвичайні ситуації, протиправна діяльність); встановлення критеріїв віднесення певного об'єкту до КІ тощо.

В межах третього етапу, який тривав з 2015 по 2018 рр., значущим є формування концептуальних основ нормативно-правового забезпечення захисту КІ. Слід відмітити, що значним чинником активізації зусиль в бік подальшої роботи над розвитком поняття «КІ», системи її захисту, складових тощо виступала необхідність протидії викликам гібридної війни рф проти України, яка почалася в 2014 р. Так, у п. 11 та п. 33 Воєнної доктрини України, затвердженої Указом Президента № 555/2015 від 24.09.2015 р. посилення охорони і захисту об'єктів КІ є основними цілями застосування воєнної сили в межах збройного конфлікту, а терористичні акти, диверсії на об'єктах КІ – це один із сценаріїв реалізації воєнних загроз безпеці України. Крім цього, найбільш вагомим доробком даного етапу слід визнати формалізацію поняття «КІ» та «об'єкт КІ» на рівні законодавства (абз. 6, 7 п. 2 Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затвердженого постановою КМУ № 563 від 23.08.2016 р.). Важливим кроком у розвитку нормативно-правового забезпечення захисту КІ стала також Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням КМУ № 1009-р

від 06.12.2017 р., в якій знайшли відображення основні проблеми та шляхи їх вирішення, серед яких найбільше наголошується на необхідності прийняття профільного закону.

Підготовка та прийняття Закону України «Про критичну інфраструктуру» стала основною, проте не єдиною формою роботи, що здійснювалася з метою розбудови нормативно-правового забезпечення захисту об'єктів КІ у 2018-2021 рр. Зазначений період такої діяльності слід виокремити, як четвертий етап, в межах якого, передусім, підготовлено та внесено до Верховної Ради України два альтернативні законопроєкти. Перший мав назву «Про критичну інфраструктуру» (реєстраційний № 5219) і був внесений народними депутатами, як суб'єктом законодавчої ініціативи. Другий – «Про критичну інфраструктуру та її захист» (реєстраційний № 5219-1) є законопроєктом, що підготовлений Кабінетом Міністрів України. Відмітимо, що урядовий законопроєкт є хронологічно першим, його розробка здійснювалась, починаючи з 2018 р. Серед найбільш помітних їх відмінностей варто зазначити, що законопроект № 5219 унормовує діяльність у сфері захисту КІ виключно в мирний час (ст. 3), а альтернативний урядовий законопроект – як в мирний час, так і в період надзвичайного стану (ст. 3). У законопроєкті № 5219 передбачено значно ширший перелік сфер КІ (наприклад, дослідницька діяльність, хімічна промисловість тощо) та суб'єктів національної системи захисту КІ (Національний банк України, Кабінет Міністрів України), ніж в альтернативному № 5219-1. У підсумку, чинний Закон України «Про критичну інфраструктуру» № 1882-IX від 16.11.2021 р., який визначив правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки, було прийнято на основі законопроєкту № 5219.

Протягом 2018-2022 рр. (до моменту прийняття та набрання чинності профільним законом) спостерігалось активне поглиблення нормативно-правового регулювання різних аспектів захисту об'єктів КІ. По-перше, заслуговує на увагу введення терміну «критично важливі об'єкти інфраструктури» в норми ч. 2 ст. 259, п. 2 примітки до ст. 360 Кримінального кодексу України. По-друге, постановою КМУ «Деякі питання об'єктів критичної інфраструктури» №1109 від 09.10.2020 р. затверджено Порядок віднесення об'єктів до критичної інфраструктури, Перелік секторів критичної інфраструктури та Методику категоризації об'єктів критичної інфраструктури. По-третє, відбувається розширення системи КІ (наприклад, Положення про визначення об'єктів критичної інфраструктури в банківській системі України, затверджене постановою Правління НБУ №151 від

30.11.2020 р.) По четверте, здійснено формалізацію вимог по кіберзахисту об’єктів КІ (Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою КМУ №518 від 19.06.2019 р.). По-п’яте, об’єкти КІ продовжують розглядатися як частина інших об’єктів забезпечення державної безпеки в цілому (п. 3 Стратегії забезпечення державної безпеки, затвердженої Указом Президента України №56/2022 від 16.02.2022 р.), про що свідчить, в тому числі, й створення в апараті РНБО України відповідної служби з питань захисту КІ.

І, нарешті, п’ятим етапом розбудови нормативно-правового забезпечення захисту КІ в Україні є період, що почався 16 червня 2022 р. із введенням в дію профільного закону, і триває до сьогодні. Зазначений етап характеризується поєднанням з дією правового режиму воєнного стану, що, безумовно, вимагає посилення захисту об’єктів КІ від загроз військового характеру (наприклад, рішення РНБО України «Про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», введене в дію Указом Президента України № 695/2023 від 17.10.2023 р.). Серед позитивних зрушень в бік повноцінного функціонування усієї системи захисту КІ, варто відмітити такі акти законодавства, як Порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього, затверджене постановою КМУ № 415 від 28.04.2023 р. та Порядок розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, затверджене постановою КМУ № 818 від 04.08.2023 р.

Отже, процес розбудови нормативно-правових засад забезпечення захисту об’єктів КІ умовно вже перебуває на п’ятому етапі свого розвитку. Його перспективними напрямами в подальшому, як видається, повинні стати більш продуктивна робота з адаптації вітчизняного законодавства до законодавства в сфері КІ, що діє в ЄС, продовження співпраці (підґрунтя якої вже було закладене на перших двох етапах) з безпековим сектором НАТО, нормотворчість, що спрямована як на деталізацію основних положень профільного закону про КІ, так і на поступове розширення захисту всіх об’єктів КІ (або їх окремих видів з певних секторів КІ) шляхом закріплення та уточнення ознак останніх в нормах законодавства про кримінальну відповідальність.

Список використаних джерел:

1. Developing the Critical Infrastructure Protection Systemin Ukraine: monography / S. Kondratov, D. Bobro, V. Horbulin et al.; general editor O. Sukhodolia. Kyiv: NISS, 2017. 184 p.

УДК 378:356:355
Єгор ХАЛЮЗОВ
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: y.s.khaliuzov@khai.edu, ORCID: 0009-0006-3912-5398
Науковий керівник
Василь ОСТРОПІЛЕЦЬ
кандидат юридичних наук, старший дослідник, доцент кафедри права
гуманітарно-правового факультету Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: ovr1967@gmail.com, ORCID: 0000-0003-0378-4253

СЕКТОР ПРАВОСУДДЯ ЯК СКЛАДОВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: у доповіді розглянуті проблемні аспекти доповнення об'єктів критичної інфраструктури судами та установами правосуддя для подальшого захисту їх безперешкодного функціонування, визначені обов'язки Державної судової адміністрації України як секторального органу сфери правосуддя щодо формування конкретного переліку об'єктів критичної інфраструктури, пов'язаних зі здійсненням правосуддя та критерії визначення підприємств, які є критично важливими для функціонування системи правосуддя.

Ключові слова: критична інфраструктура, правосуддя, Державна судова адміністрація України, судовий захист.

JUCTICE SECTOR AS A COMPONENT OF CRITICAL INFRASTRUCTURE

Abstract: This report discusses the problematic aspects of complementing critical infrastructure facilities with courts and justice institutions to further protect their unimpeded functioning, defines the responsibilities of the State Judicial Administration of Ukraine as a sectoral body of the justice sector to form a specific list of critical infrastructure facilities related to the administration of justice and the criteria for determining enterprises that are critical to the functioning of the justice system.

Keywords: critical infrastructure,justice**,** the State Judicial Administration of Ukraine, judicial protection.

Здійснення правосуддя є необхідною складовою для функціонування і розвитку правової та демократичної держави. Незважаючи на складні умови воєнного стану, право на судовий захист порушених прав і свобод повинно бути забезпечено та гарантовано державою.

Нормами Закону України «Про правовий режим воєнного стану» передбачено, що в умовах правового режиму воєнного стану суди, органи та установи системи правосуддя діють виключно на підставі, в межах

повноважень та в спосіб, визначені Конституцією України та законами України. Повноваження судів, органів та установ системи правосуддя, передбачені Конституцією України, в умовах правового режиму воєнного стану не можуть бути обмежені [6].

Внаслідок пошкодження та зруйнування об'єктів інфраструктури і будівель судів, відключень електроенергії, теплопостачання, відсутності генераторів та інших систем накопичення електроенергії дуже складно забезпечити безперервне функціонування судів та своєчасний розгляд справ. Вказані обставини можуть призводити до порушення права на судовий захист, неможливості в повній мірі судами здійснювати правосуддя та як наслідок виникає порушення встановлених процесуальних строків розгляду справ тощо.

З прийняттям Закону України «Про критичну інфраструктуру» було визначено правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури, що є складовою законодавства у сфері національної безпеки, положеннями зазначеного Закону України встановлено життєво важливі функції та/або послуги, порушення яких призводить до негативних наслідків для національної безпеки України, до яких належать, серед іншого, і правопорядок, здійснення правосуддя, тримання під вартою [4].

Водночас, сектор правосуддя був відсутній у перших редакціях Переліку секторів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 [1].

Питання доповнення зазначеної постанови сектором правосуддя неодноразово підіймалось суддівською спільнотою, але лише 16 грудня 2022 року Кабінетом Міністрів України було доповнено перелік секторів критичної інфраструктури сектором «Правосуддя», секторальним органом визначено Державну судову адміністрацію України [2].

Порядком віднесення об'єктів до критичної інфраструктури передбачено, що секторальні органи у сфері захисту критичної інфраструктури, використовуючи перелік секторів критичної інфраструктури, ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури. Відомості про об'єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться секторальними органами у сфері захисту критичної інфраструктури до секторальних переліків об'єктів критичної інфраструктури, які ними складаються та ведуться. Секторальні органи у сфері захисту критичної інфраструктури складають переліки всіх об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності.

Секторальні органи подають уповноваженому органу з питань захисту критичної інфраструктури переліки об’єктів критичної інфраструктури для формування зведеного переліку об’єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України [2].

Таким чином, на Державну судову адміністрацію України як секторальний орган сектору «Правосуддя» покладений обов’язок скласти перелік конкретних об’єктів – судів та установ системи правосуддя, що підпадають під критичну інфраструктуру та подати зазначений перелік до Державної служби спеціального зв'язку та захисту інформації України як уповноваженому органу з питань захисту критичної інфраструктури.

16 березня 2023 року Державна судова адміністрація України своїм наказом затвердила критерії визначення підприємств, які є критично важливими для функціонування системи правосуддя в особливий період, підприємства, що мають важливе значення для функціонування системи правосуддя в особливий період, якщо вони відповідають хоча б двом або більше з таких критеріїв:

1) мають важливе значення для здійснення правосуддя та надання доступу до нього, перебувають у сфері управління Державної судової адміністрації України;

2) здійснення забезпечення функціонування та кіберзахисту інформаційних, автоматизованих систем, реєстрів, баз даних, обов’язковість впровадження і використання яких передбачена процесуальним законодавством, іншими законами та нормативно-правовими актами, реалізацію яких забезпечує ДСА України;

3) залучені до реалізації проектів міжнародної технічної допомоги, які впроваджуються в установах органів правосуддя;

4) розмір середньої заробітної плати застрахованих осіб-працівників підприємств, установ, організацій, що здійснює діяльність у сфері правосуддя, за останній календарний квартал повинен становити не менше розміру середньої заробітної плати по країні за IV квартал 2021 р. (відповідно до даних Держстату, що підтверджується довідкою);

5) виконання робіт та надання послуг для органів в системі правосуддя на підставі договорів (угод, меморандумів, контрактів), укладених на строк не менше шести місяців;

6) надання послуг, що забезпечує потреби судів, органів та установ у системі правосуддя, відсутність яких може призвести повну зупинки доступу до електронного правосуддя [3].

Разом з цим, у рішенні Ради суддів України № 36 від 30.08.2023 року (далі – Рішення) констатовано, що: «…ДСА України провалено роботу з

віднесення судів України, органів та установ до об’єктів критичної інфраструктури, адже станом на даний час Державна служба спеціального зв'язку та захисту інформації України не отримувала від ДСА України секторальний перелік об’єктів критичної інфраструктури, тобто, перелік судів та установ системи правосуддя, які мають бути віднесені до таких об’єктів.ДСА України не провела жодних консультацій з Радою суддів України з приводу відмови від виконання чинного законодавства України з віднесення судів України до об’єктів критичної інфраструктури. Жодних інших ефективних рішень (можливо і альтернативних), яким чином забезпечити належні умови праці судів України в умовах тривалих відключень приміщень від електроенергії ДСА Україні досі не запропоновано…» [5].

Слід звернути увагу, що у зазначеному Рішенні наголошується на тому, що Раді суддів України невідомо, щоб ДСА України розроблялись якісь заходи задля запобігання можливим негативним наслідкам можливого блекауту, в тому числі шляхом закупівлі генераторів та/чи систем зберігання енергії. Також ДСА України не опрацьовано питання, чи сам факт віднесення певного суду/установи системи правосуддя до об'єкту критичної інфраструктури, з огляду на додаткові завдання та обов'язки, які виникнуть у операторів об'єктів критичної інфраструктури, міг би бути додатковим аргументом для виділення додаткових коштів від Уряду для забезпечення роботи таких об'єктів в умовах воєнного стану [5].

Підсумовуючи, зазначаємо про те, що на теперішній час досі залишається невирішеним питання практичної реалізації вимог законодавства щодо включення об’єктів сектору правосуддя до критичної інфраструктури, оскільки не був поданий чіткий перелік судів та установ системи правосуддя з метою подальшого їх внесення до реєстру критичної інфраструктури. Таким чином, уповноваженим органам слід у пріоритетному порядку розробити та подати перелік судів та установ системи правосуддя, що відповідають критеріям, які слід віднести до критичної інфраструктури з метою подальшого їх захисту та забезпечення усіма необхідними засобами безперешкодного функціонування та як наслідок можливості забезпечення державою дотримання прав на справедливий та своєчасний судовий захист.

Список використаних джерел:

1. Деякі питання об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 06.11.2023).

2. Про внесення змін до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 : Постанова Кабінету Міністрів України від 16.12.2022 р. № 1384. URL: https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#Text (дата звернення: 06.11.2023).

3. Про затвердження критеріїв визначення підприємств, які є критично важливими для функціонування системи правосуддя в особливий період : Наказ Державної судової адміністрації України від 16.03.2023 р. № 133. URL: https://dsa.court.gov.ua/userfiles/media/new_folder_for_uploads/dsa/N_133_23.pdf (дата звернення: 06.11.2023).

4. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882- IX. URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text (дата звернення: 06.11.2023).

5. Про організаційне та фінансове забезпечення діяльності органів судової влади : Рішення Ради суддів України від 30.08.2023 р. № 36. URL: https://rsu.gov.ua/uploads/article/risenna-rsu-no-36-vid-30082023-p-af1d78172b.pdf (дата звернення: 06.11.2023).

6. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 06.11.2023).

УДК 342

Юлія ХЛИСТУН
здобувач освіти першого року навчання, спеціальність 081 - Право, третій науковий рівень доктор PhD кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна,
e-mail: hlystunjulia@gmail.com, ORCID: 0009-0000-5016-8694

ПРАВОСУДДЯ ЯК СЕКТОР БЕЗПЕЧНОЇ ІНФРАСТРУКТУРИ ТА ЙОГО БЕЗПЕКА

Анотація: У вказаній темі викладено бачення щодо поняття критичної інфрастуктури, та його об`єктів. Зазначено, що правосуддя відносено до сектору критичної інфрастуктури, та зазначені повноваження ДСА як органу у сфері його захисту, та висловлена позиція, що ящо конкретний суд увійшов до об`єкту критичної інфрастуктури, то обов`язки щодо забезпечення його захисту покладаються фактично на операторів критичної інфрастури, тобто в тому числі і на сам суд та на територіальні управління ДСА, що тягне за собою створення спеціального апарату, фахівці якого повинні проводити аналіз існуючих загроз та ризиків, та розробляти відповідні рекомендації щодо захисту об`єкту інфраструктури.

Ключові слова: критична інфрастуктура, об`єкти критичної інфраструктури, сектор критичної інфрастуктури, правосуддя, оператор критичної інфрастуктури.

JUSTICE AS A SECURE INFRASTRUCTURE SECTOR AND ITS SECURITY

Abstract: The specified topic outlines the vision of the concept of critical infrastructure and its objects. It is noted that justice belongs to the sector of critical infrastructure, and the powers

of the State Judicial Administration as a body in the field of its protection are indicated, and the position is expressed that if a specific court is included in the object of critical infrastructure, then the duties to ensure its protection actually rest on operators of critical infrastructure, that is, including the court itself and the territorial administration of the State Judicial Administration, which entails the creation of a special apparatus whose specialists must conduct an analysis of existing threats and risks and develop appropriate recommendations for the protection of the infrastructure object.

Keywords: critical infrastructure, critical infrastructure objects, critical infrastructure sector, justice, critical infrastructure operator.

Враховуючи події, які відбуваються на даний час, а саме збільшення негативних процесів природного та техногенного характеру, зростання терористичних актів, події на Сході та Півдні України починаючи з 2014 року, повномаштабне вторгнення держави-агресора РФ, що актуалізувало для нашої держави питання захисту інфраструктури, життєво важливої для безпеки людини, суспільства і держави – інфраструктури, яка в світовій практиці визначається як критична.

Поняття «критична інфраструктура» вперше з'явилась у директиві PDD-63 (PresidentialDecisionDirective), яка була підписана президентом Сполучених Штатів Америки Б. Клінтоном у 1996 році. Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі. І найголовніше, закладено вимогу щодо забезпечення безпеки критичних елементів інфраструктури. Згодом питанням критичної інфраструктури та її безпеки почали приділяти увагу в інших країнах, зокрема: Німеччині, Великій Британії, Нідерландах, Чеській Республіці, Словаччині, Польщі, Угорщині та ін. Важливим у цьому процесі є те, що у деяких національних законодавствах при визначенні терміна «критична інфраструктура» акцентовано на функціях та послугах. Саме функції та послуги об'єктів критичної інфраструктури, якими забезпечують суспільство, бізнес та державу, є в основі визначення їх критичності, що дає методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту [1, с. 6].

В різних країнах світу під поняттям «критична інфаструктура» розуміють об'єкти і системи, настільки важливі для забезпечення життєдіяльності людей і держави, дестабілізація роботи яких, не говорячи вже про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків. При цьому, особливу небезпеку несуть каскадні ефекти, коли порушення в роботі одного об'єкту КІ приводять до порушень в роботі інших об'єктів і систем унаслідок їх взаємозалежності («ефект доміно») [2].

В Україні термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах, проте його визначення було відсутнє в чинному законодавстві. Вперше в офіційних документах України термін «критична інфраструктура» вжито у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства. В Стратегії національної безпеки «Україна у світі, що змінюється» (2012 р.) цей термін згадувався при визначенні шляхів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки. В новій Стратегії національної безпеки України (2015 р.) термін «критична інфраструктура» використовується деталізованіше [1, с. 7].

На думку авторів зазначеної книги, «критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [1, с. 7].

В подальшому бачення змісту поняття «критична інфраструктура» законодавець виклав у тексті Закону України «Про критичну інфраструктуру», де остання визначається як сукупність об’єктів критичної інфраструкури [3].

Законодавець розкриває зміст поняття об’єктів критичної інфраструктури як 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. Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що 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. Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури.Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури. Секторальні органи у сфері захисту критичної

інфраструктури складають та ведуть секторальні переліки об’єктів критичної інфраструктури.

Перелік секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури (далі - Перелік), визначається Кабінетом Міністрів України. У разі необхідності внесення змін до Переліку Кабінет Міністрів України переглядає та змінює його виходячи з критеріїв критичності, визначених цим Законом. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема: здійснення правосуддя [3].

Правосуддя як сектор критичної інфраструктури з типом основної функції: здійснення правосуддя також знайшов своє відображення в Постанові КМУ, де органом у сфері його захисту було визначено ДСА [4].

Від так, на вказаному секторі зупинемось більш детально, оскільки всі суди в нашій країні не можуть припинити здійснювати правосуддя в умовах введеного воєнного стану, а його здійснення в умовах відсутності електропостачання, інтернет-зв`язку, безпечних місць для укриття під час здійснення обстрілів є майже неможливим, та призводить до його призупинення, що є недопустимим, та призведе до порушення прав та свобод людини і громадянина.

Також на вказане звернула увагу Рада суддів України усіх судів України, та зазначила, що навіть в умовах воєнного або надзвичайного стану робота судів не може бути припинена, тобто не може бути обмежено конституційне право людини на судовий захист [5].

Тому, на ДСА покладено обов`язок визначити окремі об`єкти – суди, які повинні підпадати під критичну інфраструктури, та їх перелік, та разом із оператором критичної інфраструктури має здійснити категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) за Методикою категоризації об’єктів критичної інфраструктури, затвердженою постановою Кабінету Міністрів від 9 жовтня 2020 р. №1109 «Деякі питання об’єктів критичної інфраструктури» і подати інформацію до Реєстру об’єктів критичної інфраструктури.

Встановлені I, II, III, IV категорії критичності судів, ДСА подає їх до Держспецзв`язку для формування зведеного переліку об`єктів критичної інфрастуруктури, що затверджуються Кабінетом Міністрів України, та щомісяця подає оновлені відомості щодо них. Держспецзв`язку має право витребувати документи, на підставі яких було прийнято рішення щодо категоризації об’єктів критичної інфраструктури. У разі невідповідності

наданих документів законодавству у сфері захисту критичної інфраструктури Держспецзв`язку здійснює формування зведеного переліку об’єктів критичної інфраструктури без урахування таких об’єктів.

Відомості про об’єкти критичної інфраструктури, що містяться у зведеному переліку об’єктів критичної інфраструктури та секторальних переліках об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства [4].

Разом з цим, в подальшому оператори критичної інфраструктури, що в даному випадку є балансоутримувачами приміщень, у яких розміщуються суди, органи та установи системи правосуддя, протягом трьох місяців з дня внесення про об`єкт критичної інфраструктури забезпечують подання на погодження паспорта безпеки на об`єкт критичної інфраструктури до ДСА.

Паспорт безпеки на об’єкт критичної інфраструктури повинен в собі містити інформацію про ідентифікацію об’єкта та заходи щодо його захисту і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв’язок та обмін інформацією з суб’єктами національної системи захисту критичної інфраструктури.

При цьому законодавець покладає саме на операторів критичної інфраструктури наступні обов`язки: 1) забезпечити захист об’єктів критичної інфраструктури; 2) невідкладно поінформувати відповідальних суб’єктів національної системи захисту критичної інфраструктури (секторальні та функціональні органи) про інциденти, що сталися на об’єктах критичної інфраструктури, які належать їм на праві власності або на іншій законній підставі; 3) завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об’єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об’єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації; 4) щороку надавати інформацію про виконання повноважень відповідно до цього Закону за формою, визначеною Кабінетом Міністрів України [3].

Реєстр об`єктів критичної інфраструктури на даний час лише формується, та до нього будуть вноситись в першу чергу відомості про об`єкти критичної інфрастуктури І та ІІ категорії критичності, до якої суди не входять.

Підсумовуючи, зазначимо, що в даному випадку, віднесення сектору Правосуддя до об`єктів критичної інфрастури є вкрай важливим та необхідним, оскільки правосуддя в Україні не може призупинятись, що може призвести до свавілля в суспільстві. Однак, ящо конкретний суд увійшов до об`єкту критичної інфрастуктури, то обов`язки щодо забезпечення його

захисту покладаються фактично на операторів критичної інфрастури, тобто в тому числі і на сам суд та на територіальні управління ДСА, що тягне за собою створення спеціального апарату, фахівці якого повинні проводити аналіз існуючих загроз та ризиків, та розробляти відповідні рекомендації щодо захисту об`єкту інфраструктури. Також, при організації безпеки конкретного суду необхідно враховувати його призначення та відповідно до цього створювати безпечні умови забезпечення важливих функцій держави в умовах воєнного стану.

Список використаних джерел:

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов. К. : НІСД. 2016. 176 с.
2. Про доцільність та особливості визначення критичної інфраструктури в Україні». Аналітична записка/Д.С. Бірюков. URL: http://www.niss.gov.ua/articles/1026/.
3. Про критичну інфраструктуру: Закон від 16 листопада 2021 р., №1882-IX. Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (01.11.2023).
4. Деякі питання об'єктів критичної інфраструктури: Постанова КМУ від 9 жовтня 2020 р. № 1109. Редакція від 11.05.2023. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (01.11.2023).
5. Рішення № 9 від 24 лютого 2022 р.: Рада Суддів України. URL: https://rsu.gov.ua/uploads/news/risenna-rsu-no9-vid-240222-2de02988e4.pdf (01.11.2023).

УДК 342

Богдан ЧАЛИЙ
здобувач третього (наукового) рівня освіти доктор PhD кафедри права гуманітарно-правового факультету, Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна
e-mail: b.y.chalyi@khai.edu, chaliybohdan@ukr.net, ORCID: 0000-0001-5086-8228

НОРМАТИВНО-ПРАВОВА РЕГЛАМЕНТАЦІЯ ВИКОРИСТАННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Перехід суспільства від аналогових технологій до *цифрових* пов'язано з виникненням актуальних питань, що потребує дослідження та подальшого їх практичного втілення. Проблема захисту інформації з обмеженим доступом в сучасних умовах посідає провідне місце в повсякденній діяльності фізичних осіб та у господарській діяльності суб'єктів господарювання. Особливий попит отримання інформації з обмеженим доступом зумовлено отримання перевагам у конкурентній боротьбі юридичних осіб, що здійснюють господарську діяльність, фізичні особи володіючи певною інформацією є більш конкурентоспроможними. Особливості діяльності кожного підприємства і є пришвидшуючими факторами, що зумовлюють більш вигідні умови випуску та реалізації товарів чи послуг.

Питання комерційної таємниці було актуальним завжди, оскільки кожне підприємство намагалось зберегти свої індустріалізаційні секрети та технології. Законодавче відображення вищезазначена правова категорія знайшла закріплення у Кримінальному уложенні 1903 року [1], у положеннях якого виокремлювалися декілька видів таємниць, зокрема, комерційна. Не дивлячись на різні стадії розвитку суспільства, питання захисту комерційної таємниці залишалось, і особливу актуальність придбало зі здобуттям Україною незалежності, а саме з моменту прийняття Акту незалежності України 1991 року, а також у зв'язку з подальшими кроками до вступу України до Європейського Союзу, оскільки виникає необхідність виконання вимог Угоди про комерційне використання інтелектуальної власності TRIPS [2].

На законодавчому рівні закріплено положення щодо збору та розповсюдження інформації, що віднайшло своє відображення у статті 34 Конституції України: «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.».[3] Але законодавець передбачив і іншу сторону, попередивши зловживання своїми правами, - було встановлено обмеження, а саме забороняється розголошувати інформацію, одержаної конфіденційно.

Згідно статті 420 Цивільного кодексу України до об'єктів права інтелектуальної власності, зокрема, але не виключно, належить комерційна таємниця [4].

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (стаття 505 Цивільного кодексу України) [4].

У подальшому законодавче регулювання комерційної таємниці знайшло своє відображення у Законі України "Про інформацію" [5], Постанові КМУ «Про перелік відомостей, що не становлять комерційної таємниці» [6], Закон України "Про доступ до публічної інформації [7] та ін.

Зазначаємо, що в Угоді про торговельні аспекти прав інтелектуальної власності (статтею 39 розділу 7 встановлено, що фізичні та юридичні особи повинні мати можливість захисту інформації, яка законно знаходиться під їх контролем, від розкриття, придбання або використання іншими без їхньої

згоди у такий спосіб, який суперечить чесній комерційній практиці, якщо така інформація:

а) є секретною у тому розумінні, що вона як єдине ціле або у точній конфігурації та поєднанні разом її компонентів, загально відомих або доступних для осіб у колах, що звичайно мають справу з інформацією, про яку йдеться;

б) має комерційну цінність через те, що вона є секретною;

в) зберігається в секреті внаслідок вжиття за відповідних обставин певних заходів особою, яка законно здійснює контроль за цією інформацією) [8].

Господарський кодекс України також містить відповідні положення (статтею 36 встановлено, що під комерційною таємницею слід розуміти відомості (інформацію), пов’язані з виробництвом, управлінням, технологією, фінансовою та іншою діяльністю суб’єкта господарювання, що не є державною таємницею, та розголошення якої може завдати шкоди інтересам суб’єкта господарювання. За неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею, винні особи несуть відповідальність, встановлену законом; частиною 1 статті 162 передбачається, що суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності) [9].

Отже, зазначимо, що у чинному законодавстві України відсутній перелік конкретних відомостей, які можуть визнаватися комерційною таємницею. Чинне законодавство не дає чіткого визначення понять, термінів та не забезпечує правову основу регулювання суспільних відносин у цій сфері, а встановлює тільки загальні правила у сфері виявлення, збору, аналізу та передачі інформації, яка зазначена як комерційна. Відтак, через неоднозначне розуміння та тлумачення інститут комерційної таємниці працює не ефективно. Як наслідок, з боку держави немає гарантій захисту інформації фізичних та юридичних осіб. Погіршується становище суб’єктів інтелектуальної власності тим, що представники органів державної влади та органів місцевого самоврядування, які мають доступ до комерційної таємниці суб’єктів господарювання, не несуть жодної відповідальності за розголошення таких відомостей, що іноді призводить до зловживання своїм становищем для отримання певної вигоди.

В умовах воєнного стану будь-яка інформація, зокрема, але не виключно, комерційна, потребує особливого та ретельного дослідження та регулювання. І хоча деякі механізми протидії існують, вони потребують глибокого аналізу та доопрацювання.

Таким чином, для посилення розвинення економіки, інноваційного розвитку та стимулювання інвестицій в Україні, потрібно посилити регулювання вищезазначених суспільних відносин шляхом внесення змін до законодавчої бази та її розширення, а саме створення профільного спеціального акту, оскільки такі законодавчі зміни необхідні в умовах сьогодення.

Список використаних джерел:

1. Кримінальне уложення 1903 року (Уголовное уложение 1903 года // Приложеніе к Собр. Узак. и Расп. Правительства за 1903 год. - № 38. - Отд. 1. - 144 с.).
2. Угода про комерційне використання інтелектуальної власності: від 15.04.1994. Редакція від 6.12.2005. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text. –10.02.2023.
3. Конституція України: від 28.06.1996 № 254к/96-ВР. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. – 10.02.2023.
4. Цивільний кодекс України: від 16.01.2003 № 435-IV. Редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text. – 10.02.2023.
5. Закон України "Про інформацію": від 02.10.1992 № 2657-XII. Редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text. – 10.02.2023.
6. Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці»: від 09.08.1993 № 611. URL: https://zakon.rada.gov.ua/laws/show/611-93-п#Text. – 10.02.2023.
7. Закон України "Про доступ до публічної інформації: від 13.01.2011 № 2939-VI. Редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text. – 10.02.2023.
8. Угода про торговельні аспекти прав інтелектуальної власності: від 15.04.1994. Редакція від 06.12.2005. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text. – 10.02.2023.
9. Господарський кодекс України: від 16.01.2003 № 436-IV. Редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text. – 10.02.2023.

УДК347.822.4
Аделіна ЧУМАКОВА
студентка 756юм., гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник
Алла ГОРДЕЮК
доцентка, канд. юрид. наук,доцентка кафедри права
гуманітарно-правового факультету
Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: a.hordeiuk@khai.edu, ORCID: 0000-0001-7423-3673

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

Анотація: у роботі досліджено сучасний стан убезпечення цивільної авіації в Україні, проаналізовано правове забезпечення, окреслені напрями державної політики в цій сфері, зокрема в умовах воєнного стану, визначені перспективи розвитку цивільної авіації в нашій країні.

Ключові слова: цивільна авіація, авіаційна безпека, безпека польотів, державна політика.

LEGAL BASIS FOR ENSURING CIVIL AVIATION SECURITY

Abstract: this paper examines the current state of civil aviation security in Ukraine, analyzes the legal framework, outlines the directions of state policy in this area, in particular under martial law, and identifies the prospects for the development of civil aviation in our country.

Keywords: civil aviation, aviation safety, flight safety, state policy.

Визначення авіаційної безпеки та безпеки польотів міститься в п. 2 ч. 1 ст. 1 Повітряного кодексу України (далі – ПКУ), а саме, авіаційна безпека – захист цивільної авіації від актів незаконного втручання, який забезпечується комплексом заходів із залученням людських і матеріальних ресурсів [1].

Забезпечення безпеки цивільної авіації у мирний час – це комплексний процес, який передбачає забезпечення безпеки польотів, захист цивільної авіації від актів незаконного втручання [2]. Підвищення рівня безпеки цивільної авіації досягається шляхом впровадження всіма суб'єктами авіаційної діяльності системи управління безпекою польотів та поетапної модернізації інфраструктури авіаційної галузі, пріоритетним при цьому є ефективна державна політика щодо забезпечення високого рівня безпеки польотів.

Головним завданням державної політики забезпечення якості та безпеки польотів суден цивільної авіації є підвищення рівня безпеки польотів за

рахунок впровадження системи управління якістю польотів всіма суб'єктами авіаційної діяльності. Впровадження системи управління якістю польотів повинно забезпечити стале скорочення кількості авіаційних подій та людських жертв з одночасною модернізацією авіаційної галузі за всіма напрямками її діяльності.

Важливою складовою вітчизняної державної політики щодо забезпечення безпеки цивільної авіації є її нормативно-правове забезпечення. Так, правові засади щодо правового регулювання даної сфери державного управління зокрема становлять:ПКУ від 19.05.2011, Кримінальний кодекс України від 05.04.2001, Кодекс України про адміністративні правопорушення від 07.12.1984, Закон України «Про державну програму авіаційної безпеки цивільної авіації» від 21.03.2017, Укази Президента України, наприклад, Указ «Про невідкладні заходи щодо забезпечення безпеки цивільної авіації в Україні» від 15.01.1998 № 17, Постанови та розпорядження Кабінету Міністрів України, а саме про «Деякі питання Міжвідомчої комісії з авіаційної безпеки цивільної авіації» 09.06.2021 № 594, «Про затвердження Положення про Державну авіаційну службу України» від 08.10.2014 № 520 та інші.

Окрему увагу в даному контексті доцільно звернути на Закон України «Про Державну програму авіаційної безпеки цивільної авіації» (далі – Програма), який є спеціальним нормативним актом в сфері забезпечення безпеки цивільної авіації. Згідно з Програмою підтримання відповідного рівня авіаційної безпеки має здійснюватися за такими основними напрямами: жодне повітряне судно, внесене до Державного реєстру цивільних повітряних суден України, або іноземне повітряне судно не може вилітати з або прилітати до аеропортів України за відсутності документів, що необхідні згідно з Правилами надання експлуатантам дозволів на виліт з аеропортів України та приліт до аеропортів України; жодна особа або транспортний засіб не може увійти або заїхати до контрольованої зони без перепустки, а до стерильних зон та зон обмеженого доступу, що охороняються, без перепустки та проходження контролю на безпеку, який повинен здійснюватися належним чином на постійній основі; жодна особа не може бути допущена на борт повітряного судна без відповідного дозволу уповноваженої посадової особи суб'єкта авіаційної діяльності; під час виконання авіаційних робіт та базування на злітно-посадкових майданчиках або майданчиках для виконання авіаційних хімічних робіт організація забезпечення авіаційної безпеки покладається на керівника суб'єкта авіаційної діяльності та командира повітряного судна; суб'єкт авіаційної діяльності авіації загального призначення та фізична особа - експлуатант повітряного судна повинні забезпечувати авіаційну безпеку в місцях базування, стоянок повітряних суден та під час виконання

польотів; авіаційний персонал та персонал, задіяний в авіаційній діяльності, робота якого пов'язана із забезпеченням авіаційної безпеки, можуть бути допущені до провадження такої діяльності лише за наявності відповідних документів з авіаційної безпеки, виданих центральним органом виконавчої влади, що реалізує державну політику в галузі цивільної авіації, або навчальними закладами, сертифікованими таким органом; міжнародні договори України про повітряне сполучення, укладені Україною з іншими державами, повинні містити вимоги з авіаційної безпеки відповідно до стандартів і рекомендацій Міжнародної організації цивільної авіації [3].

Крім того, можна виділити надзвичайно актуальні проблеми в галузі забезпечення безпеки польотів у цивільній авіації, зокрема, недокомплектованість кадрами державних інспекторів, що здійснюють державний контроль за діяльністю авіаційних підприємств в галузі безпеки польотів і авіаційної безпеки; недосконалість наявних тренажерів, що призводить до подорожчання підготовки, а також зниження навиків членів екіпажу в керуванні повітряними судами, особливо в екстремальних ситуаціях; недостатня оснащеність цивільної авіації технічними засобами забезпечення авіаційної безпеки; невідповідність інформаційного забезпечення безпеки польотів потребам системи державного регулювання, що ускладнює своєчасне прийняття рішень для запобігання надзвичайних ситуацій; застаріла лабораторна база й устаткування науково-дослідних і проектних організацій цивільної авіації та промисловості. Також до проблем щодо безпеки польотів повітряних суден, які потребують вирішення можна віднести відсутність порядку фінансування витрат на утримання і розвиток служби пошукового й аварійно-рятувального забезпечення польотів цивільної авіації.

Після введення воєнного станувідповідно до Указу Президента України «Про введення воєнного стану» від 24.02.2022 №64/2022, в нашій державі у зв’язку з військовою агресією РФ загроза безпеці польотів у небі України призвела до закриття повітряного простору та масового блокування авіаційної діяльності [4].

Звісно ж, чим довше триватиме війна, тим важчою буде ситуація для української цивільної авіації, і тим довше їй потім доведеться відновлюватись. Оптимальним варіантом був би запуск перельотів навіть в умовах війни. Але сьогодні Україна перебуває в групі з семи країн з найвищим першим рівнем ризику з погляду безпеки польотів. Експлуатантам цивільних літаків рекомендовано повністю уникати таких зон, адже літаки можуть бути неправильно ідентифіковані системами протиповітряної оборони й на них помилково націляться, або потрапити під перехресний вогонь під час

повітряних атак тощо. Так, Державна авіаційна служба України зазначає, що з метою забезпечення захисту цивільної авіації наразі, відповідно до Загальної оцінки рівня загрози та ризиків авіаційній безпеці цивільної авіації у межах території України та повітряного простору над нею, територію України та повітряний простір над нею віднесено до конфліктних зон з високим ступенем ризику авіаційній безпеці. Це пов'язано з наявністю на території України реальних загроз для повітряних суден цивільної авіації та персоналу цивільних аеропортів/аеродромів, спричинених повномасштабним військовим вторгненням збройних сил РФ на територію України – обстріли населених пунктів, знищення цивільних об'єктів та об'єктів критичної інфраструктури тощо**.**

Однак існує думка фахівців, що зумовлена аналізом випадків збиття цивільних літаків над зонами конфліктів у минулому про те, що практики обов'язкового повного закриття повітряного простору немає. Навіть сьогодні з аеропортів, зарахованих до найвищого першого рівня ризику, виконують польоти. Саме тому пропонують запуск польотів із двох українських аеропортів: «Міжнародного аеропорту Львів» ім. Д. Галицького та «Міжнародного аеропорту Ужгород». Через територіальну близькість до кордону цих аеропортів літаки змогли б швидко потрапити в повітряний простір Європейського Союзу і безпечно здійснювати польоти. Однак для цього все одно потрібні гарантії безпеки від Збройних Сил України, яких на сьогодні на жаль немає. Більш того, окреслені вище проблеми забезпечення безпеки цивільної авіації, що мали місце у мирний час, у період воєнного стану у державі ще більше загострюються. Тому поновлення польотів літаків цивільної авіаціє залишається на сьогодні край спірними питанням.

Слід зазначити, що у перспективі свого розвитку авіаційна галузь в Україні стоїть перед завданням глибокої зміни підходів, інтеграції в європейську авіаційну спільноту, впровадження законодавчих нововведень, оптимізації наглядових функцій та переходу до цифрових дозвільних процедур. Чинна система авіаційного нагляду в ЄС виступає визнаним міжнародним стандартом, до якого Україна прагне приєднатися у майбутньому і вже зробила перші кроки у цьому напрямку. Зокрема було підписано Угоду між Україною, з одної сторони, та Європейським Союзом, з іншої сторони, про спільний авіаційний простір від 12.10.2021 (далі – Угода), а потім був прийнятий Закон України «Про ратифікацію Угоди між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони, про спільний авіаційний простір», який ухвалено 17.02.2022. Також відсутність проміжних національних структур робить логічним етапом нашого

наближення до ЄС перехід до Європейського агентства з безпеки польотів (EASA) відповідно до наших зобов'язань у рамках Угоди [5, 6].

Таким чином, в законодавстві України містяться нормативно-правові акти, покликані забезпечувати безпеку використання повітряних суден в Україні. Проте, попри нормативно-правове регулювання даного питання, існує чимало проблем щодо забезпечення безпеки використання повітряних суден, які потребували негайного розгляду і вирішення в мирний час, а під час воєнного стану, враховуючи пріоритетні завдання щодо подолання військової агресії РФ, рішення зазначених вище проблем, на наш погляд, унеможливлюється в сучасних українських реаліях.

Список використаних джерел:

1. Повітряний кодекс України від 19.05.2011 №3393-V. Редакція від 21.10.2023. URL: https://zakon.rada.gov.ua/laws/show/3393-17 – 15.10.2023.
2. Конвенція про міжнародну цивільну авіацію (ІКАО) від 07.12.1944. URL: https://zakon.rada.gov.ua/laws/show/995_038 – 15.10.2023.
3. Про Державну програму авіаційної безпеки цивільної авіації: Закон України від 21.03.2017 № 1965-VIII ВР. Редакція від 28.04.2023. URL: https://zakon.rada.gov.ua/laws/show/1965-19#Text – 15.10.2023.
4. Указ Президента України «Про введення воєнного стану» від 24.02.2022 №64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text – 15.10.2023.
5. Угода між Україною, з одної сторони, та Європейським Союзом, з іншої сторони, про спільний авіаційний простір від 12.10.2021. URL: https://zakon.rada.gov.ua/laws/show/984_004-21#n2 – 15.10.2023.
6. Закон України «Про ратифікацію Угоди між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони, про спільний авіаційний простір» від 17.02.2022 № 2067-IX. URL: https://zakon.rada.gov.ua/laws/show/2067-20#Text – 15.10.23

УДК 343.9

Натела ШЕВЧЕНКО
аспірантка кафедри кримінального права
Національного юридичного університету імені Ярослава Мудрого,
м. Харків, Україна
e-mail: n.s.shevchenko@nlu.edu.ua, ORCID: 0000-0003-2647-8160

ЗАБРУДНЕННЯ ДОВКІЛЛЯ ВНАСЛІДОК УДАРІВ ПО ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: В тезах надано загальну характеристику наслідків для довкілля в результаті збройної агресії російської федерації проти України. Наголошено, що обстріли призводять до серйозних екологічних наслідків, відбуваються глобальні зміни у довкіллі. Здійснено аналіз шкідливого впливу ударів по об'єктам критичної інфраструктури для

основних складових довкілля: атмосферне повітря, ґрунти, води, флора та фауна. Проаналізовано наслідки, що були спричинені в результаті атак по паливо-мастильним базам, гідротехнічним спорудам. На основі розглянутого матеріалу зроблено висновок, що удари по об'єктам критичної інфраструктури завдають значної шкоди довкіллю, перш за все забруднюють його.

Ключові слова: довкілля, забруднення довкілля, об'єкти критичної інфраструктури.

ENVIRONMENTAL POLLUTION AS A RESULT OF STRIKES ON CRITICAL INFRASTRUCTURE FACILITIES

Abstract: The theses provide a general description of the environmental consequences of the armed aggression of the russian federation against Ukraine. It is emphasized that shelling leads to serious environmental consequences and global environmental changes. The author analyzes the harmful effects of strikes on critical infrastructure on the main components of the environment: air, soil, water, flora and fauna. The author analyzes the consequences caused by attacks on fuel and lubrication facilities and hydraulic structures. Based on the material reviewed, it is concluded that attacks on critical infrastructure facilities cause significant damage to the environment, primarily pollution.

Keywords: environment, environmental pollution, critical infrastructure facilities.

В умовах повномасштабної збройної агресії російської федерації (далі – рф) проти України та активного ведення бойових дій на території України, із застосуванням різного роду озброєння та військової техніки, виникає загроза здійснення ударів по об'єктам критичної інфраструктури. В результаті цього завдається шкода не лише життю та здоров'ю людей, власності, іншим суспільним благам, а й довкіллю, зокрема атмосферному повітрю, ґрунтам, водам, флорі та фауні. Вже зараз зрозуміло, що збитки, спричинені військовими діями будуть відчутними ще протягом багатьох десятиліть.

Так, починаючи з лютого 2022 року рф постійно здійснює масовані артилерійські обстріли та ракетні удари по території України. Зокрема, станом на вересень 2023 року по Україні було випущено близько 7 тис. ракет. Лише протягом вересня 2023 р. країна-агресор застосувала проти України 246 ракет різних типів, 746 ударних дронів та 1159 керованих авіабомб. Абсолютна більшість цих ударів – проти цивільних об'єктів [7]. На жаль, часто ціллю стають саме об'єкти критичної інфраструктури, зокрема, аеропорти, мости, електричні підстанції, гідротехнічні споруди, газосховища, нафтобази тощо.

Такі обстріли призводять до серйозних екологічних наслідків, відбуваються глобальні зміни у довкіллі, в тому числі значно забруднюється атмосферне повітря. Варто наголосити, що під час детонації ракет та артилерійських снарядів утворюється низка хімічних сполук: чадний газ (CO), вуглекислий газ (CO2), водяна пара (H2O), бурий газ (NO), закис азоту (N2O), діоксид азоту (NO2), формальдегід (CH2O), пари ціанистої кислоти (HCN),

азот (N2), а також велика кількість токсичної органіки, окислюються навколишні ґрунти, деревина, дернина, конструкції. Під час вибуху всі речовини проходять повне окиснення, а продукти хімічної реакції вивільняються в атмосферу. Основні з них – вуглекислий газ і водяна пара – не є токсичними, а шкідливі в контексті зміни клімату, оскільки обидва є парниковими газами. В атмосфері оксиди сірки та азоту можуть спричинити кислотні дощі, які змінюють pH ґрунту та викликають опіки рослин, до яких особливо чутливі хвойні. Кислотні дощі мають негативний вплив і на організм людини, інших ссавців та птахів, впливаючи на стан слизових тканин та органів дихання. Металеві уламки снарядів, що потрапляють у довкілля, також не є безпечними та цілковито інертними. Чавун із домішками сталі є найбільш поширеним матеріалом для виробництва оболонки боєприпасів та містить у своєму складі не тільки стандартні залізо та вуглець, а й сірку та мідь. Ці речовини потрапляють до ґрунту і можуть мігрувати до ґрунтових вод і в результаті потрапляти до харчових ланцюгів, впливаючи і на тварин, і на людей [5].

Удари, що час від часу відбуваються по базам зберігання паливо-мастильних матеріалів, які є об’єктами критичної інфраструктури, становлять серйозну екологічну загрозу та спричиняють значне забруднення атмосферного повітря, вод, ґрунтів. Починаючи з лютого 2022 року в результаті таких атак було пошкоджено або повністю зруйновано низку таких об’єктів. Наприклад, внаслідок ракетної атаки по нафтобазі у Кривому Розі згоріло понад 5 тис. кубометрів дизельного палива. За даними Державної екологічної інспекції України (далі – Держекоінспекція) було нараховано 117 млн грн збитків. Внаслідок витоку і забруднення землі, ґрунтів, засмічення було нараховано 7 млн грн [2]. В результаті обстрілу по нафтобазі у селі Крячки Київської області було знищено 10 резервуарів із нафтопродуктами та більшу частину трубопроводів. У результаті горіння в атмосферне повітря потрапило 41 830 тон забруднюючих речовин, в тому числі 41,694 тис. тон діоксиду вуглецю, 76 тон оксиду вуглецю, 17 тон діоксиду азоту, 6 тон оксиду цинку. За підрахунками Держекоінспекції забруднення нафтопродуктами у 17 разів перевищує гранично-допустимі концентрації. Загальна сума збитків, завданих в результаті потрапляння небезпечних речовин в атмосферне повітря, складає 888,383 млн грн [3].

Руйнація такої важливої гідротехнічної споруди, як гребля Каховської гідроелектростанції (далі – Каховська ГЕС) у червні 2023 року спричинила екологічну катастрофу. В результаті відбулося часткове або повне затоплення низки населених пунктів, що призвело до загибелі людей та тварин, значне забруднення вод, в тому числі нафтопродуктами, хімікатами,

вибухонебезпечними предметами, відходами зі звалищ, недоступність води для зрошення полів, знищення червонокнижних видів тварин, птахів, риб, руйнація культурних пам'яток тощо. За даними фахівців збитки довкіллю сягають близько 1,5 млрд доларів [4]

Підрив цього об'єкта є порушенням статті 55 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I) від 8 червня 1977 р. Регламентовано, що при веденні воєнних дій має бути виявлена турбота про захист природного середовища від широкої, довгочасної і серйозної шкоди. Такий захист включає заборону використання методів або засобів ведення війни, що мають на меті завдати або, як можна очікувати, завдадуть такої шкоди природному середовищу й тим самим завдадуть шкоди здоров'ю або виживанню населення [1]. Знищення греблі Каховської ГЕС визнано екоцидом за українським законодавством – стаття 441 Кримінального кодексу України. Однак, на жаль, наразі екоцид не є окремим міжнародним злочином, а тому він не потрапляє під юрисдикцію Міжнародного Кримінального Суду (МКС). Таке діяння може бути кваліфіковано як воєнний злочин за статтею 8 Римського Статуту МКС, адже воєнним злочином є умисне вчинення нападу з усвідомленням того, що такий напад призведе до випадкової загибелі чи поранення цивільних осіб або заподіє шкоди цивільним об'єктам чи масштабної, довготривалої та серйозної шкоди навколишньому природному середовищу, яка буде явно надмірною в порівнянні з конкретною та безпосередньо очікуваною загальною військовою перевагою [6].

Таким чином, країна-агресор, здійснюючи обстріли по об'єктам критичної інфраструктури завдає значної шкоди довкіллю. Більшість таких діянь спричинюють екологічні катастрофи, а їх наслідки населення України та, мабуть, і всього світу, відчуватиме ще протягом тривалого часу. Внаслідок цих дій відбувається погіршення стану атмосфери, гідросфери, літосфери та біосфери, що призводить до руйнування екосистем, забруднення повітря, вод та ґрунтів, зменшення біорізноманіття не лише на території нашої держави, а й може мати довгострокові негативні наслідки для зарубіжних країн.

Варто наголосити, що відповідні дії з боку рф прямо порушують норми Женевських конвенцій, зокрема I Додаткового протоколу, в частині заборони застосування методів або засобів ведення воєнних дій, які мають на меті завдати або, як можна очікувати, завдадуть широкої, довгочасної і серйозної шкоди природному середовищу. Відповідні діяння мають бути зафіксовані з метою притягнення рф до відповідальності на міжнародному рівні та здійснення відповідних репарацій.

Список використаних джерел:

1. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I) від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#top (дата звернення 05.10.2023)
2. Екологічні збитки від удару армії РФ по нафтобазі у Кривому Розі оцінили в понад 100 млн грн. URL: https://suspilne.media/303468-ekologicni-zbitki-vid-udaru-armii-rf-po-naftobazi-u-krivomu-rozi-ocinili-v-ponad-100-mln-grn/ (дата звернення 05.10.2023)
3. Знищення нафтобази на Київщині: фахівці підрахували збитки довкіллю. URL: https://bigkyiv.com.ua/znyshhennya-naftobazy-na-kyyivshhyni-fahivczi-pidrahuvaly-zbytky-dovkillyu/(дата звернення 05.10.2023)
4. Підрив Каховської ГЕС: екологічні збитки становлять $1,5 млрд URL: https://censor.net/ua/news/3441674/pidryv_kahovskoyi_ges_ekologichni_zbytky_stanovlyat_15_mlrd (дата звернення 06.10.2023)
5. Природа та війна: як військове вторгнення Росії впливає на довкілля України. URL: https://ecoaction.org.ua/pryroda-ta-vijna.html (дата звернення 05.10.2022)
6. Римський Статут Міжнародного Кримінального Суду. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text (дата звернення 06.10.2023)
7. РФ у вересні випустила по Україні 246 ракет, 746 дронів та 1159 керованих авіабомб – Зеленський. URL: https://www.ukrinform.ua/rubric-ato/3768870-rf-u-veresni-vipustila-po-ukraini-246-raket-746-droniv-ta-1159-kerovanih-aviabomb-zelenskij.html (дата звернення 04.10.2023).

УДК 342

Ігор ШИНКАРЕНКО
PhD (канд. юрид. наук), професор, Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна
e-mail: sir2009@ukr.net, ORCID: 0000-0001-5524-2259

АКТУАЛЬНІ ПРОБЛЕМИ ФОРМУВАННЯ МОДЕЛІ СТІЙКОСТІ ОБ'ЄКТІВ АЕРОКОСМІЧНОГО КОМПЛЕКСУ УКРАЇНИ

Відповідно Рішення Ради національної безпеки і оборони України, Указом Президента України від 27 вересня 2021 року № 479/2021 була прийнята Концепція забезпечення національної системи стійкості [1], яка поставила перед науковим суспільством низку теоретико прикладних завдань:

- формування механізмів організації і координації дій щодо формування інноваційних підходів до технічніко інженерного;
- інституційного рівня безпека та захищеності об'єктів критичної інфраструктури
- формування методичного рівня оцінювання ризиків національній безпеці, стану відповідних спроможностей з метою підготовки, прийняття і впровадження стратегічних рішень спрямованих на побудову стійкості об'єктів аерокосмічного комплексу України;

- на координаційному рівні діяльності суб'єктів системи національної стійкості, формування ефективної системи комунікації між органами державної влади, органами місцевого самоврядування та населенням.

Означене стало важелем формування теоретико-правової бази системи національної стійкості у період, що залишився до нападу збройних сил РФ.

Аналіз наукових здобутків отриманих за період бойових дій свідчить, що проблеми побудови моделей та формування систем забезпечення національної стійкості розроблена тільки на загально-фрагментальному рівні.

Розглядаючи проблеми стійкості окремої галузі, вважаємо необхідно виходити зі змісту поняття національної стійкості. Так у своїй доповіді віце президент НАНУ академік С.І. Пирожков вказав, що під цим терміном розуміють здатність держави у взаємодії із суспільством зберігати стійкість до зовнішніх і внутрішніх агресивних впливів, оперативно реагувати на асиметричні загрози, а також відновлюватися після руйнівних наслідків агресивних дій будь-якої природи. Далі він вказує, що «національна стійкість» воно охоплює протидію в усіх сферах: політичній, економічній, військово-політичній, соціальній, екологічній тощо, тому головне – не тільки вміти протистояти, а й працювати на випередження [2].

Загально теоретичні підходи до стійкості як складової системи безпеки відображені в низці нормативно - правових актів програмного характеру - стратегії, концепції, доктрини: Концепція забезпечення національної системи стійкості [1]; Стратегія забезпечення державної безпеки [3]; Концепція боротьби з тероризмом в Україні [4]; Стратегія воєнної безпеки України [5], Стратегія інформаційної безпеки [6], Стратегія кібербезпеки України [7] та ін.

Дослідження означених програмних документів, чинних законодавчих актів, сучасної нормативної бази щодо завдань формування стратегії у сфері національної системи стійкості дозволяє констатувати наявність прогалин щодо:

- належного наукового обґрунтування формування концептуальних теоретико-правових засад цього процесу;
- вибору певної моделі забезпечення національної стійкості;
- ключових завдань, які необхідно вирішити, особливо стосовно об'єктів аерокосмічного комплексу.

Період озброєної агресії Росії показав, що аерокосмічна галузь формує національну стійкість України та є важелем формування нашої перемоги на ґрунті існуючих космічних технологій. На сьогодні сформувалася думка, що не вважаючи на певні вразливості космічної діяльності здійснюються:

- розробка оновленої її стратегії у межах розвитку національних космічних спроможностей;

-забезпечується підвищення стійкості критичної інфраструктури для безпеки й оборони України, Європи і всього світу.

Незважаючи на кібератаки проти космічної та авіаційній інфраструктурі України та інших країн до та після початку повномасштабної агресії 24 лютого 2022 року, лише у 2022 році світовий космічний бюджет зріс на 9% до абсолютного показника у 103 мільярди євро. Серед цих витрат фінансування «військового» космосу збільшилося на 16% та склало 48 мільярдів євро, така пропорція у показниках зростання є свідченням того, які пріоритети зараз людство надає у розвитку космічних технологій. Наразі навколо Землі обертаються близько 5500 супутників, і майже 10% (близько 500 одиниць) належать або керуються військовими організаціями [8].

Значний вплив аерокосмічного комплексу на національну безпеку формує виклики щодо побудови сучасної організаційно-правової моделі безпеки авіакосмічної галузі України, як складової критичної інфраструктури.

Окрім того суб'єкти господарювання аерокосмічного комплексу здійснюють:

- наукові космічні дослідження спрямовані на використання космічного простору;
- науково-дослідні та конструкторські роботи що розробки об'єктів космічної діяльності;
- виробничу діяльність у сфері будування об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- експлуатацію, технічне обслуговування та ремонт об'єктів космічної діяльності (в тому числі їх агрегатів та складових частин);
- забезпечення запуску апаратів, їх складових частин [9].

Всі виробничі цикли на об'єктах аерокосмічного комплексу та випробувань ракетно-космічної техніки, агрегатів та складових частин створюють низку ризиків та безпекових загроз локального, регіонального та глобального характеру [10, с. 24-31].

На наш погляд однією з прогалин щодо побудови системи національної стійкості взагалі та стійкості об'єктів аерокосмічного комплексу зокрема є системні помилки щодо здійснення реактивних організаційних, адміністративних та оперативно-розшукових заходів правоохоронними органами з метою мінімізації ризиків та загроз об'єктам аерокосмічного комплексу.

Слід підтримати думку науковців, які вважають, що напрям діяльності Національної поліції України як базовий елемент національної стійкості має бути врахований під час розробки та впровадження Концепції забезпечення національної стійкості [11, с. 198]. Враховуючі цілі сталого розвитку України

на період до 2030 року щодо створення стійкої інфраструктури, сприяння всеохоплюючій і сталій індустріалізації та інноваціям першочерговими [12] стають завдання забезпечення стійкості об'єктів аерокосмічного комплексу силами НПУ, СБУ, ДПСУ, Державної митної служби під час протидії злочинності та нейтралізації загроз безпеки.

Фактично реалізація означеної цілі загострює протиріччя між цільовими показниками, визначеними завданнями ЦСР та іншими програмними документами України [13, с. 36] в умовах воєнного часу та необхідно формування моделей адекватної реакції на загрози у сфері дестабілізуючій ролі загроз з боку злочинних спільнот.

При чому слід враховувати, що ознаками стійкості об'єктів господарювання є:

– здатність пристосовуватися до роботи в складних дестабілізуючих умовах;

– здатність адекватно реагувати всім складовим елементам на ризики та загрози [14].

Формуючі проекти законодавчих актів щодо побудови правових засад стійкості об'єктів аерокосмічного комплексу слід враховувати, що вони повинні створити нормативне підгрунтя їхньої здатності функціонувати і розвиватись в умовах мінливого внутрішнього і зовнішнього середовища, збалансовано та невизначеної кількості внутрішніх та зовнішніх загроз.

Проблеми. *Підґрунтям стійкості аерокосмічного комплексу на думку науковців та фахівців-практиків є прийняття законів:*

1. «Про державне регулювання у сфері супутникової навігації».

2. «Про державне регулювання у сфері дистанційного зондування Землі». (Останні проекти були узгоджені перед початком агресії РФ у 2021 році.)

3. Впровадження у національне космічне право сучасних космічних понять і термінів: аерокосмічний об'єкт дистанційного зондування Землі, дистанційне зондування Землі, діяльність з дистанційного зондування Землі, оператор аерокосмічних об'єктів дистанційного зондування Землі, космічні системи дистанційного зондування Землі, користувач даних дистанційного зондування Землі, національний ринок космічних інформаційних технологій, супутникова навігація, супутниковий зв'язок, глобальні навігаційні супутникові системи, національний супутниковий зв'язок [15, с. 9-16] тощо.

4. Закон України «Про космічну діяльність» не враховує сучасні виклики і загрози у сфері національної стійкості космічної діяльності, переважну більшість складають норми, які не мають належного правового

механізму їхньої реалізації особливо щодо існуючих ризиків та безпекових загроз.

Пропозиції. *У сфері правового забезпечення національної стійкості України стосовно об'єктів аерокосмічного комплексу необхідно:*

1. Здійснити теоретичні дослідження з метою розробки правової концепції стійкості об'єктів аерокосмічного комплексу з врахуванням його місця у системі національної стійкості та розробка на її підгрунті моделі кодифікації космічного законодавства.

2. Здійснити модернізацію національного космічного законодавство з урахуванням завдань формування стійкості об'єктів космічної інфраструктури України та положень оновлених міжнародних договорів і законодавства інших країн партнерів України.

3. З метою формування ефективної організаційної моделі інституційного забезпечення системи стійкості об'єктів аерокосмічного комплексу додати зміни до законодавства у сфері повітряного транспорту космічної діяльності з метою узгодження функцій – задач як наслідок координації діяльності суб'єктів протидії злочинності у цій сфері.

4. Розробити організаційну модель системи державного моніторингу та прогнозування напрямків розвитку національної космічної діяльності з врахуванням оборонних векторів, ризиків та безпекових загроз.

5. З метою забезпечення єдиних методологічних підходів формування правової, організаційної складової стійкості об'єктів аерокосмічного комплексу України розробити і впровадити єдину методику оцінювання ризиків безпеці й стану відповідних спроможностей.

6. Враховуючі досвід протидії гібрідним загрозам у період надання відсічі агресії РФ розробити моделі взаємодії на міжвідомчому та міждержавному рівні у сфері забезпечення стійкості з урахуванням глобальних та регіональних безпекових процесів.

Список використаних джерел:

1. Концепція забезпечення національної системи стійкості: Указ Президента України «Про запровадження національної системи стійкості» від 27 вересня 2021 року № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021#Text

2. Пирожков С. І. Про національну доповідь НАН України «Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз» За матеріалами доповіді на засіданні Президії НАН України 6 квітня 2022 року. URL: http://dspace.nbuv.gov.ua/bitstream/ handle/123456789/185177/10-Pyrozhkov.pdf?sequence=1

3. «Про Стратегію забезпечення державної безпеки»: Указ президента україни №56/2022 від 16.02. 22. URL: https://www.president.gov.ua/ documents/562022-41377

4. Концепція боротьби з тероризмом в Україні: Указ Президента України «Про Концепцію боротьби з тероризмом в Україні» від 5 березня 2019 року № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

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

6. Стратегія інформаційної безпеки: Указ президента «Про Стратегію інформаційної безпеки» № 685/2021від 28 грудня 2021р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

7. Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 року № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013

8. Борель Ж. Війна Рф проти України підкреслила значення космосу у сучасних бойових діях. URL: https://www.ukrinform.ua/rubric-polytics/3659739-borrel-vijna-rf-proti-ukraini-pidkreslila-znacenna-kosmosu-u-sucasnih-bojovih-diah.html(дата звертання 01.06.23).

9. Державне космічне агентство України (2021). URL: https://www.nkau.gov.ua/ (дата звернення: 18.05.2023).

10. Мілімко Л.В. Правове регулювання здійснення державного нагляду (контролю) за господарською діяльністю авіаційних підприємств. Наукові праці Національного авіаційнго університету. Серія: Юридичний вісник «Повітряне і космічне право». Київ: НАУ, 2020. № 3 (56). С. 24-31. DOI: https://doi.org/10.18372/2307-9061.56.14887

11. Кліман М.Р. Деякі питання вдосконалення процесу забезпечення національної стійкості в Україні. Юридичний науковий електронний журнал. №3. 2021. С.196-198. URL: http://www.lsej.org.ua/3_2021/51.pdfDOI https://doi.org/10.32782/2524-0374/2021-3/49

12. Про Цілі сталого розвитку України на період до 2030 року: Указ Президента України від 30 вересня 2019 року№ 722/2019. URL:https://zakon.rada.gov.ua/laws/show/722/2019#Text

13. Резнікова О.О. Формування національної стійкості у контексті імплементації Україною цілей сталого розвитку. Стратегічні пріоритети. №2(50). 2019. с. 27-37. URL:https://niss.gov.ua/publikacii/zhurnal-strategichni-prioriteti/strategichni-prioriteti

14. Резницька Т.О. Сутність стійкості господарської діяльності сільськогосподарських підприємств. Збірник наукових праць Вінницького державного аграрного університету. Випуск 36. 2008. URL: http://repository.vsau.org/card.php?lang=en&id=1703

15. Шемшученко Ю.С., Семеняка В.В. Сучасний стан та необхідність реформування космічного законодавства України. Часопис Київського університету права. 2019. №2. с. 9-16. DOI: 10.36695/2219-5521.2.2019.01; Про погодження проєкту Закону України «Про державне регулювання у сфері супутникової навігації»URL: https://www.drs.gov.ua/wp-content/uploads/2022/07/3517.pdf(звернення 30.06.23 21:55)

УДК 342
Олег ШИНКАРЕНКО
здобувач вищої освіти ступеня доктора філософії (PhD),
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харьків, Україна
ORCID: 0000-0002-6913-4667
Науковий керівник
Віта КОВАЛЬСЬКА
докторка юрид. наук, професорка
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харьків, Україна

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОГО УБЕЗПЕЧЕННЯ КОСМІЧНОЇ ДІЯЛЬНОСТІ

(*морально-правові засади використання штучного інтелекту***)**

У попередніх наших публікаціях наголошено, що інформаційна безпека як складова безпеки космічної діяльності складається з тріади:

«- діяльність із забезпечення – надання допомоги суб'єктам для досягнення поставлених цілей:

1) охорони прав інтелектуальної власності, державної, військової та комерційної таємниці;

2) забезпечення отримання повної, своєчасної, достовірної, цілісної доступної інформації;

3) дотримання законодавчого режиму обігу інформації з обмеженим доступом: конфіденційної; державної таємниці; службової інформації.

- **засоби забезпечення** – сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів здійснення діяльності щодо забезпечення;

- **суб'єкти забезпечення** – індивіди, організації, органи держави, які здійснюють діяльність щодо забезпечення космічної діяльності [1, с. 194]».

В той же час до засобів забезпечення інформаційної безпеки космічної діяльності на сучасному етапі розвитку науки й техніки, а в майбутньому до суб'єктів можливо віднести штучний інтелект. Означені перспективи визначають низку викликів, філософського, етично-морального та правового змісту. З одного боку враховуючі думки трансгуманістів, що вступ суспільства у інформаційну форму існування на тлі використання комп'ютерів та всесвітнього павутиння створило передумови управління людиною за допомогою алгоритмів, за якими працює штучний інтелект.

Ми згодні з думками науковців, що виникає низка безпекових морально-етичних та правових проблем використання андроїдів у різних сферах

діяльності у тому числі космічній, починаючи з наукових, дослідницьких, виробничих, обслуговуючих робіт закінчуючи забезпеченням різних рівнів інформаційної безпеки [2, с. 61-74; 3, с. 116-120].

Аналіз наукових публікацій останніх років свідчить, що окрім визначеного необхідно додати наступні умови побудови штучного інтелекту:

«як сконструювати цей інтелект таким чином, щоб жодна група людей не зуміла отримати з його допомогою переваги над іншими людьми, і щоб штучний інтелект не спрямував свою силу проти людства, а навпаки – використовувався на його благо» [4].

Дослідження складових космічної діяльності та законодавства у сфері її регулювання. Дозволяє констатувати, що на даному етапі розвитку людства постає питання як реалізувати потенціал штучного інтелекту у технологічному ланцюжки об'єкт-ЕОМ-ШІ-людина з забезпеченням обробки багатьох даних пов'язаних з космічною діяльністю:

- у виробництві об'єктів космічного та наземного базування устаткування з підтримкою ШІ використовується для оптимізації виробничого процесу та підтримки виконання завдань, які виконують люди;
- управління об'єктами космічного та наземного базування;
- підтримки зв'язку за допомогою супутників;
- вирішення комунікаційних, моніторингових задач пов'язаних з отримання та обробки значних обсягів інформації.

Окрім означеного ШІ повинен вирішити завдання стійкості на рівні конкретних суб'єктів-об'єктів космічної діяльності:

- спроможність надійно функціонувати у штатному режимі;
- адаптуватися до умов, що постійно змінюються**;**
- протистояти та швидко відновлюватися після реалізації загроз будь-якого виду: природного і техногенного характеру, загроз, що спричинені протиправними діями, та інших загроз [5, с. 17-18].

Реалізація означених задач визначається діяльністю суб'єктів забезпечення стійкості з використанням засобів та робототехніки зі штучним інтелектом в межах системи моніторингу ризиків та загроз безпеки, побудови організаційно-тактичної моделі запобігання, стримування, нейтралізації або пом'якшення наслідків терористичних дій спрямованих на знищення, виведення з ладу або зловмисне використання критичної інфраструктури в цілому та об'єктів космічної діяльності України, взагалі [6, с. 166-174.].

В той же час науковці дотримуються думки, що існує низка ризиків для людства пов'язаних з безконтрольним, або з порушення принципів моральності та етичності застосування технологій штучного інтелекту:

– втрата робочих місць людьми на ґрунті автоматизацію рутинних повторюваних операцій;

– порушення приватності, ледь не до повної її руйнації;

– Deepfakes («синтез слів «глибинне навчання» та «підробка» – методика синтезу зображення чи аудіо ряду мовлення людини, яка базується на штучному інтелекті; вона використовується для поєднання і накладення наявних зображень та відео на вихідні зображення або відеоролики»);

– автоматизована зброя, що поцілуватиме живі об'єкти без втручання людей-операторів;

– помилково-упереджені рішення систем через викривленість початкових навчальних даних (algorithmic bias) [7].

Останні два ризики найбільш небезпечні в умовах російської навали. Всі означені ризики безпосередньо пов’язані з поглядами представника трансгуманістів професора Ніка Бострома, голови Оксфордського інституту майбутнього людства щодо завантаження людського розуму до комп’ютера та створення та створення «швидкого надрозуму». Він зазначає, що швидкість надрозуму в десять тисяч разів перевищує швидкість біологічного мозку [8].

Як вбачається всі означені ризики можуть бути інтерпретовані як загрози національній безпеці та її підсистемі інформаційній безпеці космічної діяльності. Щоб уникнути цих проблемних питань слід погодитися з європейським законодавцем, яким було розроблено та опубліковано Рекомендації з етики для надійного штучного інтелекту (далі – Рекомендації) (European Commission, 2019).

Рекомендаціями визначена система принципів формування штучного ентилекту: поваги до автономії людини, запобігання шкоді, справедливість і пояснення. Фактично означені Рекомендації створюють умови реалізації системи методів контролю штучного інтелекту запропонованих Ніком Бостромом:

– ізоляційні методи - помістити ШІ в середовище, де він не зможе завдати шкоди людству;

– стимулюючі методи контролю полягають у створенні умов, за яких ШІ буде вигідно діяти на користь людей;

– методи затримки розвитку - свідомо обмежуємо інтелектуальні можливості системи або її доступ до інформації;

– методи розтяжок – це специфічне обладнання, яке дає можливість проводити діагностику ШІ, у тому числі без його відома [8].

Означені методи відповідно до Рекомендацій формують надійний штучний інтелект, який має три компоненти, що повинні бути протягом усього життєвого циклу системи:

1) Законність;

2) Етичність;

3) Надійність.

Ми згодні з думкою, що мета у вигляді надійного штучного інтелекту може бути досягнута лише тоді, коли людина візьме на себе відповідальність щодо формування такої надійності на різних етапах розробки, обігу та використання технологій ШІ. [9, 95-96].

Таким чином виникає низка викликів щодо використання ШІ взагалі та у космічній діяльності зокрема:

- загроза персональним даним;
- захисті прав і свобод осіб, які підлягають впливу штучного інтелекту;
- недостатній рівень регулювання використання та контролю за штучним інтелектом взагалі та забезпечення інформаційної безпеки космічної діяльності, зокрема.

Дослідження сучасних наукових публікацій свідчить, що підгрунтям таких ризиків є:

- відсутність досліджень щодо правового феномену штучного інтелекту та його статусу при реалізації завдань різного рівня;
- відсутній єдиний категорійний апарат;
- не сформовані загально-правові та наукові підходи до визначення поняття штучного інтелекту та його місця в сучасній системі суспільних відносин [10, с. 310-313].

Напрямками вирішення означених проблем є:

- прийняття закону про штучний інтерес з метою закріплення принципу збалансованого використання систем ШІ, захист прав громадян і підтримку інноваційного розвитку країни;
- здійснення досліджень на фундаментально-прикладному рівні щодо нейтралізації загроз збоку використання ШІ у оборонний сфері та космічній діяльності на грунті використання різних методів контролю штучного інтелекту;
- визначити теоретико-правові засади концепції, доктрини, стратегії та політики щодо використання штучного інтелекту з визначенням його правосуб'єктності та ймовірність відповідальності то що.

Список використаних джерел:

1. Шинкаренко І.О. Актуальні питання правового забезпечення інформаційної безпеки космічної діяльності. *Актуальні проблеми та перспективи розвитку юридичної науки, освіти та технологій у XXI столітті в дослідженнях молодих учених:* збірник матеріалів доповідей учасників всеукраїнської науково-практичної конференції. (Харків, 3

березня 2023 р.). Харків, 2023. с. 192-195. URL: https://dspace.univd.edu.ua/ server/api/ core/bitstreams /5527496e-3372-40b5-b2dc-650e973e3df4/content.

2. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. *Інформація і право*. № 1 (28). 2019. с. 61-67. URL: https://ippi.org.ua/bezhevets-am-pravovii-status-robotiv-problemi-ta-perspektivi-viznachennya-st-61-67. https://doi.org/10.37750/2616-6798.2019.1(28).273347

3. Позова Д. Д. Перспективи правового регулювання штучного інтелекту за законодавством ЄС. *Часопис цивілістики*. 2017. No 27. 116-120. URL: http://nbuv.gov.ua/UJRN/Chac_2017_27_24

4. Онищук І. Правове регулювання технологій штучного інтелекту: теоретико-прикладні та етичні засади. *Наукові записки Інституту законодавства Верховної Ради України.* № 3. 2020. URL*:* https://risu.ua/tehnologiyi-shtuchnogo-intelektu-spivvidnoshennya-prava-i-morali _n116164

5. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г.,Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. К. : НІСД, 2019. 224 с. ISBN 978-966-554-258-2. URL*:* https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

6. Шинкаренко О.І. Шинкаренко І.Р., Шинкаренко І.І. Теоретико - правові проблеми аналізу та оцінки загрози безпеці об'єктам аерокосмічного комплексу України. *Забезпечення стійкості у складних умовах: збірник матеріалів доповідей учасників міжнародної міждисциплінарної науково-практичної конференції*. (Харків – Брістоль, 8 червня 2023 р.). Харків- Брістоль, 2023. с. 166-174.

7. Вишня Г. Штучний інтелект і людина: загрози і можливості. 2 березня 2021, 17:50. URL: https://www.radiosvoboda.org/a/shtuchnyi-intelekt-zagrozy-i-mozhlyvisti/ 31145992.html (дата звернення 06.11/23, 13:38).

8. Superintelligence: Paths, Dangers, Strategies Джерело: https://hub.kyivstar.ua/reviews/shtuchnyy-intelekt.

9. Головко О., Боднар Є. Етико-правові проблеми використання роботів зі штучним інтелектом. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право. випуск* 3(55). 2022. с. 95-96. DOI: https://doi.org/10.20535/2308-5053.2022.3(55).269563

10. Теличко О.А., Рекун В.А., Чабаненко Ю.С. проблеми визначення та нормативного закріплення поняття «штучний інтелект» у законодавстві зарубіжних країн та України. *Юридичний науковий електронний журнал.* № 2. 2021. С. 310-313. URL: sej.org.ua/2_2021/77.pdf

УДК 378:356:355
Наталія ЯЗАН
здобувачка вищої освіти третього освітньо-наукового рівня (доктор філософії з Права)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна;
начальник сектору превентивної комунікації відділу превенції Ужгородського
районного управління поліції Головного управління Національної поліції
в Закарпатській області, майор поліції
e-mail: yazannatasha@ukr.net, ORCID: 0000-00021-7621-9506
Науковий керівник
Наталія ФІЛІПЕНКО
докторка юридичних наук, професорка,
професорка закладу вищої освіти кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: n.filipenko@khai.edu, ORCID: 0000-0001-9469-3650

ЗАСАДИ БЕЗПЕКИ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ ЯК ЕЛЕМЕНТУ СЕКТОРУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: в доповіді розглянуті питання створення належних умов безпеки для учасників освітнього процесу шляхом побудови/відбудови безпечної інфраструктури закладів освіти за допомогою не лише стандартних заходів, але й експериментальних проєктів за участю та взаємодією всіх служб і відомств, причетних до забезпечення сталого й безпекового освітнього процесу.
Ключові слова: діти, війна, безпека, військова агресія.

На території України внаслідок військової агресії Росії з 24 лютого 2022 року до теперішнього часу 3428 закладів освіти постраждали від бомбардувань та обстрілів, 365 з них зруйновано повністю [1]. А це означає, що діти нашої країни знаходяться під щільним прицілом та мають бути захищені. Для максимального захисту дітей під час освітнього процесу найбезпечніший варіант, щоб укриття знаходилось безпосередньо в закладі освіти, а не поза ним.

Адже якщо укриття розташоване поза школою, є ризики, що не всі діти зможуть встигнути вчасно евакуюватися, бо ми розуміємо, що під час повітряної тривоги кожна секунда переміщення до укриття може коштувати життя. Також, багато що залежить від кількості учнів та працівників у закладі освіти, від того, з якої відстані запущена ракета і якого вона типу ракета. Діти можуть реагувати непередбачувано, що значно ускладнить евакуацію. Тому чим швидше діти та працівники зможуть діставатися до укриття, тим краще.

Кабінет міністрів України затвердив План пріоритетних дій Уряду на 2023 рік розпорядженням від 14 березня 2023 р. № 221-р (у подальшому – План), згідно якому проводиться моніторинг кількості зруйнованих / пошкоджених громадських будівель, зокрема закладів освіти та охорони здоров'я, а також залучення коштів для їх відновлення (кошти резервного фонду державного бюджету, кошти міжнародних фінансових організацій тощо) [2].

На підставі Плану розроблена Концепція безпеки закладів освіти Розпорядженням Кабінету Міністрів України від 07 квітня 2023 року № 301-р (у подальшому – Концепція), основними завданнями якої є: створення безпечної інфраструктури закладів освіти; ефективне попередження та протидія негативним безпековим явищам в освітньому середовищі; формування компетентностей безпеки в учасників освітнього процесу; організація безпечного підвезення учнів та вчителів до/із закладів загальної середньої освіти.

Створення безпечної інфраструктури закладів освіти можливо забезпечити шляхом: облаштування існуючих та будівництва нових захисних споруд цивільного захисту закладів освіти із застосуванням проектів повторного використання або за індивідуальними проектними рішеннями з урахуванням вимог законодавства з питань пожежної безпеки, вимог щодо необхідної кількості евакуаційних виходів, наявності водопостачання, водовідведення, вентиляції, обігріву, освітлення, Інтернету, засобів надання медичної допомоги, доступності для маломобільних груп населення, зокрема осіб з інвалідністю; забезпечення мінімальних вимог для належної організації освітнього процесу в захисних спорудах цивільного захисту закладів освіти; забезпечення пожежної та техногенної безпеки закладів освіти; забезпечення в установленому порядку охорони закладів освіти із залученням поліції охорони, встановлення у закладах освіти комплексу тривожної сигналізації з підключенням до пунктів централізованого спостереження та реагування, встановлення стаціонарних металодетекторів, облаштування необхідних огорож та здійснення інших інфраструктурних заходів щодо організації безпеки закладів освіти; удосконалення нормативно-правової бази у сфері цивільного захисту з метою створення безпечних умов перебування у закладах освіти учасників освітнього процесу.

Ефективне попередження та протидію негативним безпековим явищам в освітньому середовищі можливо забезпечити шляхом: посилення поліцейської присутності у закладах освіти з наданням ефективних поліцейських послуг щодо недопущення вчинення правопорушень учасниками освітнього процесу та стосовно них; запровадження системи раннього попередження та евакуації

учасників освітнього процесу в разі нападу, ризику нападу на заклад освіти або іншої небезпеки; впровадження алгоритму дій у разі виникнення небезпечних ситуацій, виявлення вибухонебезпечних та інших підозрілих предметів у закладі освіти; трансформації психологічної служби системи освіти та психологічного супроводу з урахуванням впливу військової агресії на учасників освітнього процесу; удосконалення нормативно-правової бази у сфері громадської безпеки в частині підвищення ефективності попередження та недопущення вчинення правопорушень в закладах освіти.

Реалізація Концепції сприятиме створенню безпечного освітнього середовища в закладах освіти, поліпшенню стану їх пожежної та техногенної безпеки, можливості для кожного закладу освіти організовувати освітній процес в очному режимі, забезпеченню комфортного перебування в об’єктах фонду захисних споруд закладів освіти, а також підвезенню учнів та вчителів до/із закладів освіти.

Крім того, реалізація Концепції підвищить ефективність превентивних заходів щодо запобігання та попередження вчиненню правопорушень в освітньому середовищі та створить безпечні умови навчання та викладання, комфортну міжособистісну взаємодію, що сприятиме емоційному благополуччю учасників освітнього процесу, відсутності будь-яких проявів насильства, забезпечивши при цьому достатньо можливостей для їх запобігання, а також дотримання прав і норм фізичної, психологічної, інформаційної та соціальної безпеки кожного учасника освітнього процесу.

Забезпечення виконання завдань та заходів, передбачених Концепцією, допоможе убезпечити учасників освітнього процесу від непередбачуваних подій, спричинених військовою агресією Російської Федерації проти України, а також надасть можливість безперешкодної реалізації права на освіту та належні, безпечні і здорові умови навчання та викладання [3].

Говорячи про безпеку слід проговорити про алгоритм дій у разі нападу або ризику нападу на заклад освіти:

1. Керівник закладу освіти координує та контролює дії членів команди реагування закладу освіти та працівників закладу освіти.

2. Команда реагування закладу освіти та/або працівник закладу освіти:

1) негайно викликають поліцію та (за необхідності) інші екстрені служби, вмикає систему оповіщення за першим сигналом та повідомляє керівнику закладу освіти про напад або ризик нападу на заклад освіти;

2) з'ясовує обставини нападу або виникнення ризику нападу (сутність загрози, кількість постраждалих від нападу, їх фізичний стан та місце перебування);

3) у разі неможливості евакуації, зокрема якщо проведення евакуації може бути небезпечним, уживає заходів щодо залишення учасників освітнього процесу в місці їх перебування в закладі освіти та блокування будь-яким способом дверей та вікон;

4) у разі проведення евакуації вмикає систему оповіщення за другим сигналом;

5) уживає заходів щодо проведення безпечної евакуації учасників освітнього процесу в безпечне місце;

6) організовує безпечне пересування учасників освітнього процесу до укриття або іншого безпечного місця;

7) перевіряє приміщення, будівлю закладу освіти на відсутність у них учасників освітнього процесу;

8) виконує вимоги поліцейських та/або працівників ДСНС, які прибули в заклад освіти для реагування на напад або ризик нападу, та сприяє в межах компетенції їх діяльності та за можливості інформує про перебіг евакуації, місця перебування учасників освітнього процесу;

9) у разі наявності постраждалих від нападу організовує надання їм домедичної допомоги, у тому числі із залученням екстрених служб;

10) за можливості оповіщає батьків, інших законних представників про переміщення здобувачів освіти в укриття;

11) погоджує повернення учасників освітнього процесу до навчання після завершення заходів, вжитих у разі нападу або ризику нападу на заклад освіти, а також перевіряє кількість здобувачів освіти [4].

Поряд з тим, постановою Кабінету Міністрів України від 15 серпня 2023 р. № 867 затверджений Порядок реалізації експериментального проєкту «Спеціаліст із безпеки в освітньому середовищі», метою якого є забезпечення безпеки в освітньому середовищі, у тому числі запобігання, раннє виявлення, припинення та усунення можливих негативних явищ, шляхом запровадження та організації діяльності спеціаліста із безпеки в освітньому середовищі. Учасниками цього проекту є МОН, Мінінфраструктури, Мінсоцполітики, Національна поліція, ДСНС, а також органи місцевого самоврядування Вінницької, Волинської, Дніпропетровської, Закарпатської, Запорізької, Житомирської, Івано-Франківської, Київської, Кіровоградської, Львівської, Миколаївської, Одеської, Полтавської, Рівненської, Сумської, Тернопільської, Харківської, Хмельницької, Черкаської, Чернівецької та Чернігівської областей. Координатором експериментального проекту є МВС [5].

Підводячи підсумки розгляду питання засад безпеки навчальних закладів України, як елементу сектору критичної інфраструктури в умовах правового режиму воєнного стану можна стверджувати наступне – зазначене

питання є настільки актуальним, що не лише Міністерство внутрішніх справ, але й Міністерство освіти та науки, Мінінфраструктури, Мінсоцполітики, а також органи місцевого самоврядування роблять значні кроки для визнання навчальних закладів України елементом сектору критичної інфраструктури в рамках діючого законодавства.

Список використаних джерел:

1. URL: https://saveschools.in.ua/
2. Розпорядження Кабінету Міністрів України від 14 березня 2023 р. № 221-р Про затвердження плану пріоритетних дій Уряду на 2023 рік URL: https://ips.ligazakon.net/document/kr230221?an=1
3. Розпорядження Кабінету Міністрів України від 07 квітня 2023 року № 301-р Про схвалення Концепції безпеки закладів освіти URL: https://zakon.rada.gov.ua/laws/show/301-2023-%D1%80#Text
4. Спільний Наказ Міністерства внутрішніх справ України та Міністерства освіти та науки України від 18.08.2023 № 685/1013 «Про затвердження Порядку раннього попередження та евакуації учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти» URL: https://ips.ligazakon.net/document/RE40639?an=1
5. Постанова кабінету Міністрів України від 15 серпня 2023 р. № 867 «Про реалізацію експериментального проєкту “Спеціаліст із безпеки в освітньому середовищі» URL: https://www.kmu.gov.ua/npas/pro-realizatsiiu-eksperymentalnoho-proektu-spetsialist-iz-bezpeky-v-osvitnomu-t150823

УЧАСНИКИ КОНФЕРЕНЦІЇ

НАУКОВЕ ВИДАННЯ

БЕЗПЕКА ТА СТАЛИЙ РОЗВИТОК КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Тези доповідей науково-практичної конференції
(м. Харків, 8 листопада 2023 року) Електронне видання.

SECURITY AND SUSTAINABLE DEVELOPMENT OF CRITICAL INFRASTRUCTURE IN THE CONDITIONS OF MARTIAL LAW

Abstracts
of the Scientific and Practical Conference

Відповідальна за випуск С. Ю. Лукашевич
Технічний редактор Т. М. Лазарева
Коректор І. Ю. Тур
Комп’ютерне складання та верстання Т. М. Лазарева

Адреса редакційної колегії:
61070, м. Харків, вул. Чкалова, 17
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
тел. +38 (067) 575 83 94

Підписано до видання 23.10.2023
Ум. друк. арк. 21,39. Обл.-вид. арк. 20,54. Електронний ресурс