Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

О.П. Єрменчук

ОСНОВНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КРАЇНАХ ЄВРОПИ: ДОСВІД ДЛЯ УКРАЇНИ

Монографія

Дніпро
2018

УДК 351.863 + 338.246.87
Є 72

Рекомендовано до друку Вченою радою Дніпропетровського державного університету внутрішніх справ (протокол № 1 від 20.09.2018)

РЕЦЕНЗЕНТИ: **Суходоля О. М.** – доктор наук з державного управління, професор; **Кириченко О. В.** – доктор юридичних наук, доцент; **Рижов І. М.** – доктор юридичних наук, професор, Заслужений юрист України.

Єрменчук О.П.

Є 72 Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : моногр. / О. П. Єрменчук. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

ISBN 978-617-7665-36-5

Здійснено комплексний аналіз теоретичних і практичних проблем пов'язаних з організацією захисту критичної інфраструктури в провідних країнах Європи. Досліджено понятійно-категорійний апарат у цій сфері. Розглянуто еволюційні процеси та апробований досвід спільної діяльності залучених державних органів та партнерів з приватного сектору різних держав і їх повноваження, основні складові елементи ієрархічної системи важливі для її побудови та функціонування.

За результатами вивчення запропоновано авторське бачення нової організаційно-правової національної моделі захисту критичної інфраструктури.

Матеріали монографії не містять відомості, що становлять державну таємницю та службову інформацію з грифом обмеження доступу «Для службового користування» (висновок від 04.10.2018 р.).

Для науковців та практиків, державних управлінців та представників приватного бізнесу, залучених державних органів та правоохоронців, що здійснюють побудову системи захисту критичної інфраструктури в Україні.

ISBN 978-617-7665-36-5 УДК 351.863 + 338.246.87

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДБ – державна безпека

ДПП – державно-приватне партнерство

ЗМІ – засоби масової інформації

ЗКІ – захист критичної інфраструктури

ЄС – Європейський Союз

КІ – критична інфраструктура

КМ – Кабінет міністрів

МВС – Міністерство внутрішніх справ

МЗС – Міністерство закордонних справ

МО – Міністерство оборони

НАТО – Північно-Атлантичний Альянс

РНБО – Рада національної безпеки і оборони

СБ України – Служба безпеки України

США – Сполучені Штати Америки

ВСТУП

Досвід провідних країн Європи свідчить, що захист критичної інфраструктури (далі – КІ) належить до основних напрямів державної політики з питань забезпечення державної безпеки.

Зазначене питання, безумовно, є актуальним і для нашої держави. Це пов'язано з тим, що сьогодні Україна протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки. Військовий конфлікт на сході країни, торгівельні війни, економічна експансія, різке посилення тероризму, небувалий ріст злочинності, руйнування та пошкодження численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, втрата новітніх технологій – все це та інші ризики вимагають від держави нових підходів до завчасного виявлення загроз та їх попередження і припинення.

Нові та небезпечні виклики регіональній і глобальній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури та наукової розробки зазначеної проблематики.

Окремі питання, пов’язані із захистом критичної інфраструктури, були порушені в наукових працях Д.С. Бірюкова, Є.В. Брежнєва, Д.Г. Бобро, О.Ф. Величка,

Д.В. Дубова, В.П. Горбуліна, С.П. Іванюти, В.В. Зубарєва, В.К. Конах, С.І. Кондратова, М.В. Мірошника, О.І. Насвіт, М.А. Ожевана, В.М. Панченко, В.В. Петрова, І.М. Рижова, П.П. Скурського, О.М. Суходолі, В.М. Щербини, О.М. Юрченка, однак основні підходи до організації захисту критичної інфраструктури в країнах Європи та, з їх урахуванням, створення організаційної та правової системи в Україні потребують комплексного наукового дослідження.

Водночас наявна вітчизняна правова база потребує удосконалення, у тому числі й уточнення понятійно-категорійного апарату.

Сьогодні у нашій державі розпочато створення нормативно-правової та організаційно-структурної системи захисту КІ. Одним з перших серед вагомих кроків стала підготовка в 2015 р. фахівцями Національного інституту стратегічних досліджень Зеленої книги з питань захисту критичної інфраструктури, де сформульовано стратегічні цілі державної політики у сфері захисту критичної інфраструктури в Україні, принципи побудови системи захисту критичної інфраструктури та основні завдання такої системи. Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», уведеним в дію Указом Президента України від 16 січня 2017 р. № 8/2017, визначено завдання щодо комплексного вдоско-

налення правової основи захисту КІ та системи державного управління її безпекою. Важливим етапом у розвитку цього напрямку стало схвалення Концепції створення державної системи захисту критичної інфраструктури розпорядженням Кабінету Міністрів України від 06 грудня 2017 р. № 1009-р. Її метою є необхідність визначення основних напрямів і механізмів комплексного правового врегулювання захисту критичної інфраструктури та створення системи державного управління у сфері її захисту, розробка сучасних підходів до управління безпековими ризиками, оптимізоване використання наявних ресурсів, гнучкість та швидкість реагування на інциденти та кризи.

У згаданих та деяких інших нормативно-правових актах закладено концептуально-стратегічні основи діяльності у досліджувані сфері. Наразі для захисту КІ та протидії загрозам у сфері державної безпеки досить необхідною є теоретична розробка цього питання для подальшого практичного впровадження організаційно-правової моделі функціонування об’єктів КІ. Особливо актуалізує тему дослідження те, що згідно з розпорядженням Кабінету Міністрів України від 06 грудня 2017 р. № 1009-р. наразі центральними органами виконавчої влади та іншими державними органами і установами здійснюється розробка для подання на розгляд Кабінету Міністрів України проекту Закону України «Про критичну інфраструктуру та її захист». Тому зростає необхідність наукового вивчення подібних систем

в зарубіжній практиці, детальний огляд яких міститься в даній роботі автора.

Зазначені обставини спонукають до змістовного аналізу понятійно-категорійного апарату, розгляду еволюційних процесів та апробованого досвіду з організації захисту критичної інфраструктури в провідних країнах Європи, основних складових елементів цього нового процесу для вітчизняних гравців, аналізу ієрархічної побудови системи залучених органів та повноважень і заходів, що ними вживаються. За результатами його вивчення необхідно запропонувати нову організаційно-правову модель захисту критичної інфраструктури в інтересах державної безпеки України.

Саме ці підстави і стали рушійним фактором та основою для наукових пошуків автора й підготовки цих матеріалів.

1. ПОНЯТТЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Історичний ретроспективний аналіз розвитку світових держав та цивілізацій свідчить, що небезпеки як зовнішнього, так і внутрішнього характеру періодично постають перед кожним суспільством. З часом, залежно від економічного, соціального та технологічного рівня розвитку, змінюються лише форми прояву таких загроз та об'єкти спрямувань, ураження чи виведення з ладу яких може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку держави, забезпечення її суверенітету, територіальної цілісності та національної безпеки.

Про існування певних об'єктів, що мають принципово важливе значення для забезпечення сталого функціонування суспільства, було відомо ще древнім китайцям та грекам.

На етапі зародження цивілізацій однією з основних загроз для соціального устрою вважалось вторгнення іноземних військ, тобто безпосередня військова загроза. Так, давньокитайський філософ Сунь Цзи ще в 7 ст. до н.е. у

своїй праці «Мистецтво війни» виділяв 5 найбільш уразливих об'єктів, які прагне знищити будь-який ворог: люди, запаси, обози, склади, загони[1].

В ті часи до важливих (критичних) об'єктів обов'язково включали транспортну мережу та водопроводи, які були надзвичайно необхідними для населення держав. Їх стабільна робота була запорукою забезпечення потреб громадян та необхідною умовою для управління народом. У зв'язку з цим під час нападу ворогів основною задачею оборонців було захистити саме ці об'єкти від зруйнування. Загалом у подальшому здобуття чи знищення таких об'єктів стало основою військового мистецтва та діяльності спецслужб.

Вважається, що першим, хто почав використовувати слово «інфраструктура», був Сократ (5 ст. до н.е.): «Для того щоб людина існувала, їй потрібні тили, які надає суспільство: безпека, соціальний порядок та господарські товари. Однак це вона може отримати в тому випадку, якщо буде поважати концепт суспільства та свої обов'язки. Основними з цих обов'язків є забезпечення інфраструктури та послуг, наданих суспільством»[2]. Згодом «інфраструктура» («infra-structure») використовується спочатку у військовій, а потім і в інших сферах у Фран-

[1] Трактаты о военном искусстве / Сунь-цзы, У-цзы / пер. с кит., предисл. и коммент. Н.И. Конрада. М., 2010. С. 70.

[2] Evolutions of Infrastructure: 15,000 Years of History by Demeter G. Fertis, Anna Fertis, Published by Vantage Press, 1998.

ції у значенні «те, що знаходиться під забудовами», а також в Англії. На думку деяких вчених, в т.ч. Стефена Левіса, саме використання зазначеного поняття французькими працівниками при будівництві залізничних доріг, тунелів та мостів у США сприяло його поширенню на американському континенті. Згодом його значення дещо змінюється[3].

Сьогодні, з розвитком людства, значного прогресу досягли і форми ведення війни. Результатом еволюційних змін у системі міжнародних відносин та відмінною рисою XX століття можна назвати неоголошені, так звані «гібридні», війни[4]. На думку Ф. Хофмана, військового консультанта та аналітика, у гібридних війнах агресор часто використовує унікальну комбінацію загроз, скерованих на найбільш вразливі місця жертви агресії. Хофман розглядає її у застосуванні стосовно тактично важливих об'єктів найрізноманітніших комбінацій дозволеної зброї, партизанської війни, тероризму тощо для досягнення політичних цілей. За його прогнозами, з цим видом війн доведеться мати справу все частіше[5]. Український політолог та історик Є. Магда серед засобів впливу, під якими розуміються загро-

[3] URL: http://hakpaksak.wordpress.com/2008/09/22/the-etymology-of-infrastr-and-the-infrastructure-of-the-internet.

[4] Магда Е. Гибридная агрессия России: уроки для Европы. К.: Каламар, 2017. С. 21.

[5] Hoffman F. Onnot-so-newwarfare: political war fare vs hybrid threats. URL: http://warontherocks.com.

зи у таких війнах, виділяє такі їх комбінації: політичні, воєнні, економічні, соціальні, інформаційні, терористичні, підривні тощо[6].

При зміні засобів мета зазначених дій залишається тією ж – отримання різного роду вигоди: матеріальної, фінансово-економічної чи політичної[7]. Їх метою стають ті ж найважливіші (критичні) об'єкти держави, котра є жертвою агресії.

Еволюція форм та засобів ведення війни прямо залежить від об'єктів спрямувань, що теж еволюціонують. Останніми десятиліттями бурхливий розвиток технологій, особливо в ІТ-сфері, призвів до значних, а іноді – і революційних, змін у підвищенні ступеня взаємозв'язку, взаємопроникнення і взаємозалежності різноманітних мереж і систем, виробничих, фінансових, торговельних та інших процесів у всіх сферах життя більшості країн світу. Лише в XX столітті, під час так званої карибської кризи, вперше почали інтенсивно вирішуватися питання, пов'язані з критичною інфраструктурою «невійськового» характеру – безпекою телекомунікаційних мереж. Серед найбільш резонансних фактів кібератак на об'єкти критичної інфраструктури варто згадати кібератаки на об'єкти ядерної галузі Ірану в 2010 р. за допомогою комп'ютерного вірусу

[6] Магда Е. Гибридная агрессия России: уроки для Европы. К.: Каламар, 2017. С. 30-31.

[7] Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К., 2017.

«Stuxnet»[8]. Українські оператори теж ставали об'єктами деструктивного впливу[9]. Зокрема, в 2015 р. троянською програмою «BlackEnergy» було виведено з ладу енергосистему «Прикарпаттяобленерго». Тоді було вимкнено близько 30 підстанцій, понад 230 тисяч мешканців залишились без світла. Загалом, згідно з даними з відкритих джерел, в грудні 2016 р. на засіданні РНБО України було зазначено, що лише за останні 2 місяці в Україні було зафіксовано 2,5 тис. кібератак[10].

Тому провідні світові держави, поряд з фізичною інфраструктурою, виділяють та здійснюють захист кіберкритичної інфраструктури. У Плані захисту критичної інфраструктури США від 2015 р. закріплено, що забезпечення безпеки та стійкості фізичної та кіберкритичної інфраструктури сприяє мінімізації наслідків від дії загроз та сприяє її швидкому відновленню[11]. У Німеччині, окрім загроз від терактів і злочинних дій та від стихійних явищ, виділяють третій вид – загрози від технічних збоїв та

[8] Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави // Захист інформації. НАУ, 2017. Т. 19.

[9] Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки): аналітична записка Національного ін-ту стратегічних досліджень. Березень 2017 р. http://www.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf.

[10] Світова гібридна війна: український фронт: монограф. / за заг. ред. В.П. Горбуліна. К., 2017; URL: https://uk.m.wikipedia.org/wiki/Кібервійна.

[11] National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication.

людських прорахунків, під якими розуміються в тому числі і кіберзагрози[12].

Доцільно також зазначити про існування небезпеки іншого, не соціального, а природного характеру. До неї слід віднести паводки, засухи, епідемії, епізоотії та епіфітотії, землетруси та бурі, і цей перелік можна продовжити. Майже усі країни загрози природного характеру виділяють окремою групою.

Загалом, проаналізувавши світовий досвід, пропонуємо вважати, що *захист критичної інфраструктури поєднує три основні напрями:*

1) захист від загроз у сфері державної безпеки; вони можуть включати внутрішні загрози та фізичне знищення КІ;

2) захист від кіберзагроз;

3) захист від надзвичайних ситуацій.

Таким чином, критична інфраструктура завжди була і залишається першочерговим об'єктом захисту та джерелом інтересу агресора чи важливим об'єктом, що може бути уражений різного роду факторами, в т.ч. не лише соціального, а і природного характеру. Залежно від розвитку суспільства зміст поняття «критична інфраструктура» постійно змінюється. Водночас спроби виділити її в окрему категорію та організовувати належний захист на рівні за-

[12] Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий // Bundesministerium des Innern, 2006. URL:https://www.bmi.bund.de.

гальнодержавного підходу в світі розпочали досить нещодавно.

Над проблематикою критичної інфраструктури з 1980-х років активно почали працювати США, зокрема Національний дослідний інститут (U.S. National Research Council)[13]. Досить популяризувала цю проблематику у 1980-х рр. книга «Америка в руїнах»[14]. Значно активізувалось дослідження проблеми після терористичних актів 11 вересня 2001 р. в США, 11 березня 2004 р. в Мадриді та 7 липня 2005 р. в Лондоні[15].

В Україні цю наукову проблему хоч і розпочали розглядати з початку 2000-х рр., однак можна стверджувати, що нового рівня вона досягла починаючи з 2015 р. Поштовхом цьому слугувало дослідження науковців НІСД «Зелена книга з питань захисту критичної інфраструктури в Україні». У зазначеній книзі під терміном *«критична інфраструктура України»* визначено 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

[13] Infrastructure for the 21st Century: Framework for a Research Age. Washington: National Academies Press, 1987. ISBN 978-030-9078-146.

[14] Choate, Pat a Susan Walter. America in ruins: the decaying infrastructure. Durham, N.C.: Duke Press Paperbacks, 1981. ISBN 08-223-0554-2.

[15] Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С. Обеспечение безопасности критических инфраструктур в США (аналитический обзор) // Труды ИСА РАН. 2006. Т. 27.

національної безпеки[16]. Загалом автори дослідження намагались сформулювати стратегічні цілі державної політики у сфері захисту критичної інфраструктури в Україні, принципи побудови системи захисту критичної інфраструктури та завдання такої системи. Наразі в продовження порушених питань фахівцями у зазначеній галузі в державі назріла актуальність здійснити подальші кроки стосовно аргументації вибору моделі функціонування при безпосередній побудові цієї системи, визначенні ролі та місця учасників процесу. Звісно, що для вирішення такого завдання вірним шляхом буде розгляд еволюційних процесів та апробованого досвіду у сфері захисту критичної інфраструктури провідних держав Європи.

Як уже зазначалось, зміст поняття «критична інфраструктура» постійно коригується та удосконалюється. Так, в 2002 р. в рамках роботи Євроатлантичної ради НАТО закріплено, що «критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих і необхідних видів діяльності економіки та державного управління». До таких галузей, в першу чергу, включені: телекомунікаційні, енергетичні, банківські, фінансові, водногосподарські системи та аварійні служби державної і недержавної власності.

Досить активно дослідження з безпеки почали про-

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

водитись з 2003 р. в рамках програми ЄС «European industrial potential in the field of security research» та «European Security Research Programme (ESRP)». З 2007 р. в цілях підготовки заходів на випадок війни чи надзвичайних подій розпочалась робота над ініціативою «Research for Secure Europe» (дослідження для безпеки Європи). Поряд із зазначеним, починаючи з 2004 р., на рівні ЄС та Європейської комісії почалось створення проекту захисту критичної інфраструктури «European Programme for Critical Infrastructure Protection» (далі – «EPCIP»). У ньому важливу увагу було приділено захисту від терористичних загроз. В цей час під критичною інфраструктурою розуміється «обладнання, служби й інформаційні системи, життєво важливі для держави, знищення чи відмова від яких призведе до послаблення суспільства, національного господарства, системи охорони здоров'я, безпеки ефективного функціонування державного устрою».

17 листопада 2005 р. Комісія прийняла «Зелену книгу» із захисту критичної інфраструктури (EPCIP). Її основною задачею було сформувати на політичному та безпосередньо на рівні виконавців загальну позицію та заходи із захисту критичної інфраструктури в країнах-членах ЄС. Червоною ниткою проведено те, що захист критичної інфраструктури кожної країни потребує посилення взаємодії та обміну інформацією щодо загроз на загальноєвропейсь-

кому рівні та між окремими країнами-учасницями.

Дослідження підходів держав ЄС до розуміння критичної інфраструктури сьогодні засвідчує її сприйняття як комплексної системи, що має побудову мережі, яка включає окремі елементи цієї мережі та ланцюжок з'єднань (окремих пов'язаних елементів). Місця з'єднань елементів ланцюжків утворюють вузол. Пошкодження чи руйнування одного з вузлів впливає на діяльність інших та може призвести до повалення всієї критичної інфраструктури. Тому в інтересах захисту критичної інфраструктури потрібно захищати такі вузли.

Захист критичної інфраструктури будується на зменшенні вразливості системи чи збільшенні її стійкості до наслідків надзвичайних подій[17]. В США розрізняють два елементи, що стосуються критичної інфраструктури: це власне критична інфраструктура та основні елементи (активи чи джерела), яких у сукупності нараховують 16 секторів. В Європі застосовують «рівні областей» (секторів) та «рівні продуктів та послуг» (елементів), їх кількість складає від 8 до 10. Якщо раніше захист критичної інфраструктури в Європі в першу чергу був націлений на забезпечення стабільного функціонування національних крити-

[17] Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: ВШБ – Технич. ун-т Острава, 2014/2015. 60 с. (текст для курсов, подготавливаемых в рамках сотрудничества Чешская республика – Молдавия). С. 32.

чних інфраструктур, то зараз основною метою Європейської програми із захисту критичної інфраструктури є забезпечення рівномірного захисту критичної інфраструктури всього європейського простору. Згідно з положеннями програми основними її завданнями є протидія тероризму та кіберзагрозам.

Вочевидь, враховуючи вищевикладене, при формулюванні визначення вітчизняної критичної інфраструктури доцільно зважати на те, що світова практика визнала доцільність включення до складу інфраструктури матеріальних та нематеріальних об'єктів. Характеристику значення цих об'єктів для функціонування держави пропонується охопити словосполученням «надзвичайно важливі». Вони подібним чином визначаються у законодавстві США та Німеччини, де звучать як «системи та засоби, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів...» (Patriot Act, 2001) та «організаційні і фізичні структури й об'єкти, настільки життєво важливі для суспільства та економіки Німеччини...»[18].

Саме тому, на нашу думку, вітчизняне визначення критичної інфраструктури має включати «сукупність надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури». На законодавчому

[18] Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. наради / упоряд. Д.С. Бірюков, С.І Кондратов; за заг. ред. О.М. Суходолі. К., 2016.

рівні це забезпечить можливість здійснення заходів із протидії тероризму та кіберзагрозам критичній інфраструктурі на загальнодержавному рівні таким чином, як це здійснюється і в країнах ЄС.

Важливо зауважити, що останнім часом у визначенні критичної інфраструктури акцент зміщується з фізичного виміру об'єктів все більше до їх функцій та послуг. Саме вони забезпечують потреби суспільства, держави та її економіки, тому і лежать в основі визначення критичності. Це надає ефективні методологічні можливості для визначення критеріїв відбору елементів критичної інфраструктури та першочерговості їх захисту[19].

Іншою рисою об'єктів критичної інфраструктури є їх належність до національної інфраструктури. Як зазначалось у попередніх роботах автора, **«національна інфраструктура»** – це взаємопов'язана система державного управління та об'єктів інфраструктури, що є основою функціонування держави, її економіки та суспільства. **«Об'єкт національної інфраструктури»** може об'єднувати в собі державні та приватні підприємства, організації та установи, а також їх власність та результати діяльності, що є складовими єдиного механізму функціонування держави, її

[19] Там само.

економіки та суспільства[20]. Автором не випадково застосовується такі поняття, як власність та результати діяльності. Вони є досить широкими та зможуть поєднати в собі такі запропоновані вітчизняними науковцями та водночас не досить притаманні для українського законодавства терміни: системи та їх частини, мережі, ресурси, вузли тощо.

Лише надзвичайно важливі для забезпечення державної безпеки об'єкти національної інфраструктури можуть визначатися як критична інфраструктура[21].

У директиві Ради ЄС критична інфраструктура поділяється на національну критичну інфраструктуру та європейську. Національна критична інфраструктура включає «засоби, системи та їх частини держави – члена ЄС, що є принциповими для збереження найбільш важливих суспільних функцій, здоров'я, безпеки, забезпечення належних господарських чи соціальних умов для населення, порушення чи руйнування яких спричинило б державі – члену ЄС серйозні наслідки в результаті відмови таких функцій»[22]. Оскільки деякі елементи критичної інфраструктури

[20] Єрменчук О.П. Складові національної інфраструктури // Науковий вісник ДДУВС. 2017. № 4. С. 109-115; Єрменчук О.П. Поняття критична інфраструктура // Інформаційна безпека людини, суспільства, держави. 2018. № 1 (23). С. 20-27.

[21] Єрменчук О.П. Сутність та зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури // Бюлетень Міністерства юстиції України. 2017. № 11. С. 35-41.

[22] Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

мають вагоме значення не лише на національному, а й на міждержавному рівні, в ЄС визначили європейську критичну інфраструктуру, до якої віднесли «критичну інфраструктуру, що знаходиться в державах – членах ЄС, порушення чи руйнація якої могли б спричинити серйозні наслідки не менше, ніж у двох державах»[23].

Цікаву думку з приводу віднесення до критичної інфраструктури можна знайти в статті професора Йозефа Ржиги у журналі «Урбанізм і територіальний розвиток». Позиція автора характеризується тим, що критерії вибору мають бути основані на професійних знаннях з урахуванням обсягу, важливості та часового фактору[24].

Загалом, аналізуючи поняття «критична інфраструктура», зрозуміло, що воно повинно включати ті найважливіші об'єкти, без яких чи з порушенням діяльності яких у державі можуть настати навіть невідворотні негативні процеси, можуть бути завдані великі збитки громадянам, їх здоров'ю та життю, соціально-економічній ситуації. Саме від стабільної діяльності критичної інфраструктури залежить функціонування національної інфраструктури та економіки в цілому.

На нашу думку, вітчизняне визначення критичної інфраструктури має бути таким: **критична інфраструк-**

[23] Там само.

[24] Říha, Josef. Urbanismus a územní rozvoj. ročník X. číslo 4/2007. URL: http://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf.

тура – це система надзвичайно важливих матеріальних та нематеріальних об’єктів національної інфраструктури, що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки.

2. ОРГАНІЗАЦІЙНА МОДЕЛЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ПРОВІДНИХ КРАЇНАХ ЄВРОПИ

2.1. Велика Британія розпочала визначати і захищати свою критичну інфраструктуру однією з перших у Європі. У 1999 р. у Великобританії був створений Координаційний центр з безпеки національної інфраструктури, який входив до складу Міністерства внутрішніх справ, що згодом припинив діяльність. На даний час при MI-5 функціонує Центр із захисту національної критичної інфраструктури. В 2016 році з нього виділився Національний центр кібербезпеки.

Національна інфраструктура Великої Британії – це засоби, системи, сайти, інформація, люди, мережі та процеси, необхідні для функціонування країни, від яких залежить повсякденне життя. Вона також включає в себе деякі функції, сайти та організації, які, хоча і не є критичними для забезпечення основних послуг, але потребують захисту через потенційну небезпеку для громадськості (наприклад, для цивільних ядерних та хімічних об'єктів)[25].

Виділяють 13 національних секторів (в попередньому

[25] URL: https://www.cpni.gov.uk/about-cpni.

переліку їх було 9) інфраструктури: хімічна галузь, промисловість, цивільні ядерні комунікації, оборона, надзвичайні служби, енергетика, фінанси, продовольство, уряд, охорона здоров'я, космос, транспорт та вода.

Не все в секторі національної інфраструктури вважається «критичним» (CNI). Під CNI розуміють об'єкти, системи, сайти, майно, інформацію, людей, мережі та процеси, втрата чи збій у функціонуванні яких призведе до серйозного шкідливого впливу на наявність, доставку чи цілісність основних послуг, що спричинить серйозні економічні або соціальні наслідки або втрату життя.

Організаційна модель. Модель захисту КІ можна назвати централізованою правоохоронною. Основні органи, які забезпечують захист критичної інфраструктури, відносяться до органів державної безпеки, мають відношення чи входять до Об'єднаного розвідувального комітету. Деякі питання політики у сфері ЗКІ здійснюють підрозділи Кабінету Міністрів.

Нормативні акти. Великобританія, за зразком США, у захисті критичної інфраструктури орієнтується, перш за все, на протидію тероризму і порушенню кіберпростору. Свою політику держава узагальнює в Стратегії національної безпеки, а також у таких нормативних актах: «Антитерористична стратегія» (CONTEST – Counter terrorism strategy), «Програма стійкості критичної інфраструктури» (CIRP – Critical Infrastructure Resilience Programme) і

«Стратегія щодо захисту кіберпростору» (Cyber Security Strategy). Кожних чотири роки, з 2010 р., Урядом розробляється «План національної інфраструктури» (National Infrastructure Plan). Основними законами, які регулюють діяльність органів, що захищають КІ, є закони: «Про службу безпеки» 1989 р., «Про розвідувальні служби» 1994 р., «Про свободу інформації», «Про правосуддя та безпеку» 2013 р. Також діє національний реєстр ризиків.

Основні учасники / обов'язки. Секретаріат Кабінету Міністрів (англ. Cabinet Office, CO) входить до складу Уряду Сполученого Королівства, відповідає за забезпечення діяльності прем'єр-міністра та Кабінету Міністрів Сполученого Королівства[26]. Його основними задачами є: сприяння прем'єр-міністру у реалізації його повноважень та повноважень Кабінету Міністрів, здійснення політичних та конституційних реформ, пришвидшення обміну інформацією з пріоритетних державних питань та покращення взаємодії між державними органами[27].

Управління з безпеки кіберпростору та уряду (англ. Cyber and Government Security Directorate, CGSD) – урядовий підрозділ, що координує Національну програму кібербезпеки та відповідає за політику державної безпеки й інформаційної безпеки. CGSD створило Національний центр кібербезпеки (NCSC). Сприяє уряду у визначенні основних

[26] URL: https://www.gov.uk/government/organisations/cabinet-office.
[27] Там само.

напрямів захисту кіберпростору, оскільки відповідає за реалізацію ряду програм, зокрема: за підготовку Національної стратегії кібербезпеки (NCSS) 2016-2021 рр.; контроль за п'ятирічною національною програмою кібербезпеки 2016-2021 рр.; бере участь у формуванні політики державної безпеки.

Секретаріат з питань надзвичайних ситуацій (англ. Civil Contingencies Secretariat, CCS), створений у липні 2001 року, є підрозділом Секретаріату Кабінету Міністрів Великобританії, відповідальним за розробку планів та заходів, в тому числі і щодо критичної інфраструктури, на випадок надзвичайних ситуацій у Великобританії. Його задача полягає у забезпеченні стійкості та підвищенні захищеності Великої Британії у боротьбі з надзвичайними ситуаціями. Для цього необхідно постійно проводити заходи з їх прогнозування, оцінки, реагування, відновлення та запобігання[28]. CCS також відповідає за функціонування сайту UK Resilience website, де міститься корисна інформація для громадськості щодо захисту від надзвичайних ситуацій. До створення CCS в 2001 р. вказані повноваження належали Міністерству внутрішніх справ. У випадку національної кризи CCS сприяє діяльності Центру управління кризовими ситуаціями (англ. Cabinet Office Briefing Rooms, COBR). Центр представляє собою групу нарадчих кімнат у приміщенні Кабінету Міністрів, які використову-

[28] http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.

ють для засідань координаційного характеру у випадку кризових ситуацій, що мають важливе значення для Великої Британії. Метою його діяльності є швидке вироблення єдиної позиції та вжиття скоординованих заходів протидії наявним загрозам. Склад засідателів в COBR залежить від характеру інциденту та є змінним. Як правило, його очолює прем'єр-Міністр чи інший головний за профілем міністр, участь можуть брати в тому числі мери міст, представники органів самоврядування чи організацій.

Міністерство внутрішніх справ (англ. Home Office, HO) є державним органом у складі уряду Великої Британії, що відповідає за безпеку та правопорядок. До сфери управління входить поліція, служба безпеки (MI-5), пожежна й рятувальна служба, інші органи.

Міністерство внутрішніх справ реалізує та формує політику уряду з питань, пов'язаних з безпекою, боротьбою з тероризмом, протидією обігу наркотичних засобів, міграційну політику і ряд інших. Однією з основних функцій міністерства є забезпечення стабільності в суспільстві у випадку кризових явищ. Важливе місце належить питанню захисту критичної інфраструктури Великобританії та підвищенню її стійкості, розробці механізмів швидкого відновлення без значних економічних затрат та загроз життю людей[29].

Центр захисту національної критичної інфраструктури

[29] http://www.homeoffice.gov.uk.

(CPNI – англ. Centre for the Protection of National Infrastructure) є основним державним органом, який надає консультації з питань безпеки національної інфраструктури підприємствам, установам та організаціям. CPNI функціонує при Службі безпеки MI-5, підзвітний його директору та підконтрольний МВС. Слугує міжвідомчим центром для участі різних учасників у захисті КІ, адже для виконання своїх задач залучає різних суб'єктів та використовує ресурси ряду державних установ, Служби безпеки (MI-5), CESG (Національний технічний орган у справах інформації уряду Великої Британії) та інших організацій.

Центр із захисту національної інфраструктури був створений в 2007 р. на базі Національного координаційного центру з безпеки інфраструктури (NISCC) та Центру консультацій з національної безпеки (NSAC, був підрозділом MI-5). Надає комплексні консультації з питань безпеки підприємствам і організаціям, які є операторами критичної інфраструктури, включаючи інформаційні, кадрові та технічні аспекти безпеки, допомагаючи знизити вразливість національної критичної інфраструктури від тероризму та інших загроз. Рекомендації із захисту критичної інфраструктури надаються у вигляді індивідуальних консультацій, тренінгів, онлайн-інформації та опублікування консультаційних матеріалів. Діяльність CPNI спрямована на забезпечення збереження основних послуг економіки Великобританії (зв'язок, медична допомога, енергетика,

фінанси, харчові продукти, транспорт тощо). Без них держава може зазнати серйозних економічних збитків, соціальних загострень, навіть значних людських втрат[30].

Згодом функції із забезпечення кіберзахисту були передані Національному центру кібербезпеки.

Національний центр кібербезпеки Великобританії (англ. National Cybersecurity Center, NCSC) – організація Великобританії, яка надає консультативну допомогу і підтримку державному і приватному секторам з питань протидії загрозам комп'ютерної безпеки. NCSC було створено в 2016 році з метою захисту критично важливих об'єктів в Інтернет-сфері і здійснення протидії кіберзагрозам.

Центр створений на базі Центру урядового зв’язку (GCHQ), що займається радіоелектронною розвідкою та захистом інформації державних органів. Його можна порівняти з Агентством національної безпеки США. В центр включені експерти в галузі безпеки команди з реагування на комп'ютерні надзвичайні ситуації CERT-UK та MI-5.

Діяльність NCSC, враховуючи американську Директиву № 41 (PPD-41), зосереджена на кіберінцидентах, а не на зборі розвідувальної інформації.

Метою діяльності є покращення кіберзахисту об'єктів критичної інфраструктури, мереж державного та приватного секторів, надання консультацій операторам та громадянам для функціонування та ведення бізнесу з використ-

[30] http://www.cpni.gov.uk/default.aspx.

танням інформаційних мереж та Інтернету[31], своєчасне виявлення кібератак і їх швидка нейтралізація, виявлення загроз функціонуванню сайтів державних відомств та блокування поширення вірусних програм; участь у розробці «Стратегії щодо захисту кіберпростору» та у формуванні переліку загроз у даній сфері.

NCSC у разі появи загроз з боку іноземних держав, злочинних організацій, окремих груп чи осіб забезпечує якісну протидію їм для мінімізації ризиків і шкоди та здійснює їх вивчення, розробляє методичні та практичні заходи із недопущення в подальшому. Центр також співпрацює з іншими правоохоронними органами, організаціями у сфері оборони, службами розвідки та безпеки Великобританії та приватним сектором.

Отже, CPNI пропонує заходи для захисту КІ, а NCSC визначає ризики для вжиття відповідних контрзаходів. З метою посилення кіберзахисту з 2015 р. реалізує програму «10 кроків до кібербезпеки», де пропонується алгоритм дій для захисту операторів від кібератак.

Служба безпеки (Військова розвідка, англ. Military Intelligence 5, MI-5) є основним контррозвідувальним органом та органом безпеки Сполученого Королівства і керує Об'єднаним розвідувальним комітетом (JIC). Відповідно до Закону «Про службу безпеки» 1989 р. Служба безпеки у Кабінеті Міністрів підпорядкована Міністерству внутріш-

[31] https://www.ncsc.gov.uk/information/about-ncsc.

ніх справ, однак входить до структури Об'єднаного розвідувального комітету[32].

Діяльність органу спрямована на захист британської парламентської демократії та економічних інтересів, боротьбу з тероризмом, шпигунством та поширенням зброї масового знищення у Великій Британії[33].

Одним з основних завдань MI-5 є діяльність щодо захисту критичних елементів національної інфраструктури, ключових (фізичних та електронних) компонентів. Ці компоненти є життєво важливими для надання основних послуг, таких як енергетика, зв'язок, транспорт та вода. Більшість роботи у цій сфері здійснює Центр з охорони національної інфраструктури (CPNI), що підзвітний Генеральному директору MI-5[34]. Він відповідає за формування критичних об'єктів.

Щоб протидіяти міжнародному та внутрішньому тероризму, шпигунству та іншій ворожій іноземній діяльності, CPNI надає експертні рекомендації операторам КІ, наявну розвідувальну інформацію, а також дані стосовно загроз та питань безпеки персоналу.

Управління з питань безпеки та боротьби з тероризмом (англ. Office for Security and Counter-Terrorism, OSCT) є виконавчим органом у складі МВС, що створений у 2007 р. для боротьби з тероризмом у Великобританії. Досить ті-

[32] http://www.mi5.gov.uk/output/uk-home-page.html.
[33] Там само.
[34] Там само.

сно співпрацює з поліцією та службами безпеки[35]. Управління підзвітне міністру внутрішніх справ та міністру з питань безпеки. Формує політику та заходи безпеки для боротьби з тероризмом. До повноважень входить: розробка заходів з протидії терактам, забезпечення захисту критичної інфраструктури від терактів (в тому числі з використанням електронно-обчислювальної техніки), розробка законодавства у сфері протидії тероризму, захист громадських діячів, взаємодія з урядовими структурами та службою екстреної допомоги під час терактів або контртерористичних операцій[36].

Національне бюро з питань боротьби з тероризмом (англ. National Counter Terrorism Security Office, NaCTSO) є поліцейським підрозділом, підзвітним МВС, що досить тісно взаємодіє з Центром захисту національної критичної інфраструктури (CPNI). Бере участь у розробці стратегії боротьби з тероризмом.

NaCTSO забезпечує захист важливих, небезпечних та потенційно уразливих об'єктів, а також надає консультації щодо загроз та сприяє функціонуванню мережі консультаційних центрів по боротьбі з тероризмом (CTSA). Консультанти по боротьбі з тероризмом входять до складу поліції у Великобританії та забезпечують підвищення стійкості до терористичних нападів.

[35] http://security.homeoffice.gov.uk.
[36] Там само.

Центр урядового зв'язку (англ. Government Communications Headquarters, GCHQ). Спецслужба GCHQ, разом із MI-5 та MI-6, входить до складу Об'єднаного розвідувального комітету. Створена як шрифтова школа в часи Першої Світової війні, зараз згідно з офіційними загальнодоступними джерелами відповідає за проведення радіоелектронної розвідки та забезпечення захисту інформації державних органів.

У сфері захисту критичної інфраструктури GCHQ надає відповідні рекомендації технічного характеру в інтересах Центру захисту національної критичної інфраструктури (CPNI), консультації та практичну допомогу державному і приватному сектору для захисту критичної інфраструктури, відому як Information Assurance.

З метою розробки програми «10 кроків до кібербезпеки», що містить керівництво для операторів критичної інфраструктури щодо забезпечення належної кібербезпеки своїх установ та організацій, проводить спільну діяльність з департаментом бізнесу, інновацій та навичок (BIS), Кабінетом Міністрів та CPNI.

Діяльність здійснюється в інтересах національної безпеки, економічного добробуту Великобританії та з метою попередження, виявлення або припинення тяжких злочинів.

До основних задач входить протидія: кіберзагрозам (для цього співпрацює з операторами критичної інфра-

структури, для забезпечення безперервності основних послуг, які вчиняються з використанням цифрових мереж; з урядом та промисловістю, яким надає інформацію про загрози та експертні поради щодо захисту інформації; з правоохоронними органами для розслідування злочинів в Інтернет-сфері); тероризму – в частині недопущення поширення через Інтернет, набору нових бранців та координації вчинення терактів тощо; вчиненню тяжких злочинів; шпигунству, оскільки, розвиток технологічного світу означає, що кіберзлочинці можуть вчиняти збір даних від представників державних організацій та приватних компаній в інформаційній, комунікаційній та промисловій сфері, генетиці та обороні[37].

Діє відповідно до положень Закону «Про розвідувальні служби», 1994 р.

Агентство з протидії організованій злочинності (англ. Serious Organized Crime Agency, SOCA) є цивільним органом, який фінансується Міністерством внутрішніх справ, але є функціонально незалежним. Діяльність спрямована на протидію організованій злочинності та тяжким злочинам[38]. Міністр внутрішніх справ може визначати основні напрями роботи SOCA та оцінювати результат.

[37] https://www.gchq.gov.uk/topics/our-history.
[38] http://www.soca.gov.uk/index.html.

2.2. Франція виокремила критичну інфраструктуру та заклала правові основи для її захисту ще в 1997 р. Спочатку керівництво держави розпочало захищати критичну інфраструктуру в інформаційно-комунікаційній сфері. На даний час загальне керівництво захистом КІ в Франції здійснює прем'єр-міністр та, в основному, урядова вертикаль. Міністри зобов'язані контролювати практичне впровадження рішень щодо захисту КІ у сфері свого впливу. Основну відповідальність за організацію захисту КІ несе Генеральний секретаріат з питань оборони та національної безпеки (SGDSN), який аналізує відкриту інформацію та розвіддані спецслужб у сфері захисту КІ, слідкує за недопущенням загроз, координує міжвідомчу політику безпеки та оборони, забезпечує підготовку та дотримання рішень президента і прем'єр-міністра у цій сфері. Підхід базується на управлінні ризиками, попередженні, розробці планів реагування та обміну інформації між учасниками. Підрозділ з державного захисту та безпеки (PSE) займається питаннями планування заходів безпеки КІ.

Політику щодо безпеки інформаційних систем на національному рівні проводить Національне агентство з безпеки інформаційних систем (ANSSI).

Організаційна модель. Модель захисту КІ є децентралізованою, в ній важливу роль надано спецорганам у сфері національної безпеки. SGDSN підпорядкована прем'єру.

Включає підрозділ з Державного захисту та безпеки – PSE, який займається питаннями планування заходів з безпеки КІ та забезпечує відповідною інформацією секретаріат Ради з питань оборони та національної безпеки (CDSN). Паралельно в МВС (MI), яке виконує функції захисту ДБ, функціонує Міжвідомчий кризовий центр (CIC). До захисту КІ також залучені міністерства (Міністерство оборони, Міністерство юстиції, Міністерство економіки та фінансів, Генеральний секретаріат міністерств освіти і науки, Міністерство сільського господарства та продовольства, Міністерство екології) та громадські організації.

Одним з основних документів щодо захисту КІ є Закон № 6600 / SGDSN / PSE / PSN від 2014 р. «Про захист основних секторів економіки» (Secteurs d'Activités d'Importance Vitale). Тут термін «критичні» дослівно вживається у значенні *«життєво важливі»* (фр., importance vitale). *Об'єкти критичної інфраструктури* – установи, виробництво та споруди, які надають товари та послуги, незамінні для функціонування суспільства. До критичних відносять 12 секторів: громадське управління; судочинство; збройні сили; сільське господарство; електронні комунікаційні системи, аудіо- та відеоінформаційні технології; енергетика; космос і дослідницька діяльність; фінансовий сектор; вода; промисловість; громадське здоров'я; транспорт[39].

[39] http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf.

Нормативні акти. Стратегія оборони та національної безпеки, Стратегія з безпеки та оборони інформаційних систем, Біла книга з питань оборони та національної безпеки, Закон № 6600 / SGDSN / PSE / PSN від 2014 р. «Про захист основних секторів економіки», згідно з яким органи державної влади зобов'язані створити загальний План безпеки КІ, оператори КІ повинні розробити План забезпечення безпеки оператором.

Основні учасники / обов'язки. Рада з питань оборони та національної безпеки (фр., Conseil de Défense et de Sécurité nationale, CDSN) є французьким міжвідомчим органом, який збирається під головуванням Президента Республіки Франція під час кризових ситуацій та приймає рішення у сфері військового управління, оборони та національної безпеки, щодо реагування на масштабні кризи у сфері КІ та забезпечення економічної і енергетичної безпеки, проведення військових операцій внутрішнього характеру та зовнішніх важливих питань боротьби з тероризмом. Рада, як ключова установа в галузі безпеки, має координувати та сприяти боротьбі зі злочинністю.

Указом від 24 грудня 2009 р. передбачено дві спеціалізовані ради оборони: Національну раду з розвідки, яка визначає стратегічні напрями, сили, засоби та пріоритети діяльності розвідки (розвідувальне співтовариство теж бере участь у захисті КІ та діє під загальним керівництвом Національної ради з розвідки); Раду з ядерної зброї, яка

визначає пріоритети та забезпечує реалізацію програми ядерного стримування.

Генеральний секретаріат з питань оборони та національної безпеки (фр., Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN) створений в урядовій вертикалі Франції в 2009 р. у зв'язку з поширенням у світі проявів тероризму та розповсюдженням кіберзагроз. Його основною задачею стало забезпечення державної політики у сфері оборони та безпеки, він відповідає за проведення Францією міжнародної політики з безпеки. SGDSN відіграє у галузі безпеки об'єднуючу роль між урядом та Президентом республіки Франція. Вносить питання до розгляду Ради з питань оборони та національної безпеки (фр., Conseil de Défense et de Sécurité nationale, CDSN) під головуванням глави держави, для обговорення яких залучає представників виконавчої влади. У взаємодії з зацікавленими міністерствами і відомствами проводить підготовчу роботу до засідань CDSN.

Водночас SGDSN повністю відповідає за організацію захисту КІ: аналізує відкриту інформацію та розвіддані у сфері захисту КІ, слідкує за недопущенням загроз, координує міжвідомчу політику безпеки та оборони, забезпечує підготовку та дотримання рішень президента та прем'єр-міністра у цій сфері, включаючи безпеку інформаційно-телекомунікаційних систем. Політику щодо безпеки інформаційних систем на національному рівні проводить Наці-

ональне агентство з безпеки інформаційних систем (ANSSI). До захисту КІ також залучені Центр державних комунікацій та Міжвідомча контрольна група [40].

Підрозділ з державного захисту та безпеки (англ., State Protection and Security – PSE) при SGDSN займається питаннями планування безпекових заходів, навчання та розробки технологій безпеки, в тому числі стосовно сфери захисту КІ.

Національне агентство з безпеки інформаційних систем (ANSSI) входить до структури SGDSN. Агентство виконує функції національного регулюючого органу в галузі безпеки інформаційних систем. Відповідає за впровадження та надання послуг у сфері захисту КІ, відповідних технологій, продуктів та ноу-хау для експертів і широкої громадськості. ANSSI здійснює оцінку загроз інформаційним системам, надає інформацію, консультації та технічну допомогу щодо боротьби з кіберзагрозами державі, адміністраціям та компаніям КІ.

Центр операцій з безпеки інформаційних систем (фр., Centre Opérationnel en Sécurité des Systèmes d'Information, COSSI) входить до SGDSN. COSSI є одним з підрозділів ANSSI, що звітує Генеральному секретарю з питань оборони та національної безпеки. Структурними підрозділами COSSI є Центр урядової експертизи протидії кібератакам (фр., Centre d'expertise governemental de reponse et de

[40] http://www.sgdsn.gouv.fr.

traitment des attaques informatique, CERTA) та Центр моніторингу й узагальнення (Centre de Veille Permanente de Conduite et de Synthese, CEVECS). Серед задач COSSI основними є захист інформаційний систем, включаючи урядові мережі. Він координує заходи міністерств у випадку атак на об'єкти КІ. Він також готує та реалізує конкретні заходи безпеки інформаційно-телекомунікаційних систем проти терористичних нападів за планом «Vigipirate», що контролюється PSE. COSSI у сфері захисту КІ також здійснює: аналіз загроз; виявлення вразливих місць щодо захисту КІ; класифікацію поточних загроз та пропозиції щодо заходів реагування на них; допомогу у кризових ситуаціях державним органам, органам влади та операторам КІ.

Міжвідомчий кризовий центр (фр., Centre interministériel de crise, CIC) був створений в 2008 р. після прийняття Білої книги з питань оборони та національної безпеки. Метою його створення стала необхідність для координації заходів держави у випадку значної події, що впливає на безпеку країни (бомбардування, стихійні лиха, великомасштабні культурні або спортивні заходи)[41].

CIC, під керівництвом МВС, забезпечує оперативне міжміністерське управління кризовими ситуаціями. CIC здійснює навчання персоналу державних органів з метою

[41] https://www.interieur.gouv.fr/Publications/Nos-infographies/Securite-des-biens-et-des-personnes/ Mobilisation-de-l-Etat-en-temps-de-crise/Centre-interministeriel-de-crise-CIC.

оперативної реакції на надзвичайні події, постійного контролю інформаційних потоків та прогнозу можливого розгортання кризи для прийняття відповідних рішень. Крім того, проводить інформаційно-роз'яснювальну роботу з громадськістю та ЗМІ.

Головне управління цивільного захисту та керування кризовими ситуаціями (фр., La direction générale de la sécurité civile et de la gestion des crises, DGSCGC), раніше Управління громадської безпеки (DSC) та Управління оборони та цивільної безпеки (DDSC), є підконтрольним МВС. Загалом система громадської безпеки (Sécurité civile en France) ділиться на два рівні: а) на національному рівні: Головне управління цивільного захисту та керування кризовими ситуаціями; б) на територіальному рівні – пожежники. У розпорядженні DGSCGC налічується близько 3 тисяч цивільних і військових працівників, розташованих на 60 об'єктах.

Основними задачами DGSCGC є забезпечення цивільної безпеки, пожежна безпека, планування діяльності на випадок кризових ситуацій. Управління проводить моніторинг цивільної безпеки, аналізує ризики незалежно від їх походження (природне, технологічне, ядерне забруднення, забруднення навколишнього середовища тощо), вживає заходів щодо запобігання та припинення, розробляє пожежні правила, проводить інформаційну роботу в суспільстві.

Міжвідомчий центр операцій з управління кризовими

ситуаціями (фр., Centre opérationnel de gestion interministérielle des crises, COGIC) створений урядом та МВС з метою управління в кризових ситуаціях, для цивільної оборони та забезпечення безпеки КІ та населення. У випадку кризи COGIC координує рятувальні команди – як державні, так і приватні, місцеві та національні.

Під час природних та техногенних катастроф здійснює аналіз ситуації та управління силами та засобами. Надає інформацію щодо загроз за допомогою телекомунікаційних засобів іншим зацікавленим міністерствам. Тісно співпрацює з Центром операцій Національної поліції та Центром планування і проведення операцій Міністерства оборони.

Відомчий оперативний центр (фр., Centre opérationnel départemental, COD) є інструментом врегулювання кризових ситуацій, доступний префекту, який активується, коли на його території відбувається значна подія (надзвичайні ситуації техногенного чи природного характеру, що впливають на безпеку дорожнього руху, великомасштабні аварії тощо). У разі таких ситуацій префект об'єднує всіх учасників для забезпечення громадської безпеки, поліцію та жандармерію, необхідні державні органи та представників громад.

План NOVI (Le plan NOVI, NOmbreuses VIctimes) – це план, що застосовується у випадку надзвичайних ситуацій для врятування великої кількості жертв. Є частиною планів

з надзвичайних ситуацій, розроблених в рамках ORSEC для забезпечення громадської безпеки. План NOVI запускається префектом і мобілізує всіх залучених учасників рятувального ланцюга.

План ORSEC, також відомий як «червоний план», – це французький загальний план на випадок надзвичайних ситуацій. Застосовується, коли місцевих засобів недостатньо, при широкомасштабних чи тривалих стихійних лихах (повені, сильні шторми, землетруси або великі промислові катастрофи). Цей план може активізуватися префектом чи прем'єр-міністром залежно від зони поширення загроз.

Міністерство внутрішніх справ (фр., Ministère de l'Intérieur) відповідає за внутрішню безпеку, підтримку державних інституцій на всій території та громадську безпеку. В цій частині він і є учасником захисту КІ. Забезпечує громадянам здійснення прав та свобод, гарантованих конституцією.

Починаючи з 2014 р. міністр внутрішніх справ готує та реалізує політику Уряду у справах внутрішньої безпеки, безпеки дорожнього руху, територіального управління державою, імміграції громадянських свобод. Він також відповідає за координацію дій з попередження злочинності та боротьби з незаконним обігом наркотиків та захист населення від стихійних лих.

До складу МВС входять: Генеральний секретаріат міністерства; Генеральний директорат місцевих органів вла-

ди (DGCL); Генеральне управління Національної поліції (DGPN); Генеральний директорат внутрішньої безпеки (DGSI); Генеральна дирекція Національної жандармерії (DGGN); Генеральне управління іноземців у Франції (DGEF); Генеральний директорат з питань цивільної безпеки та управління кризовими ситуаціями (DGSCGC); підрозділи з безпеки дорожнього руху.

Генеральний директорат внутрішньої безпеки (фр. Direction générale de la Sécurité intérieure, DGSI) – провідний орган національної контррозвідки, підвідомчий міністерству внутрішніх справ Франції. Створений в 2014 р. Фактично замінив собою колишнє Центральне управління внутрішньої розвідки (фр. Direction centrale du Renseignement intérieur, DCRI), яке було створене 1 липня 2008 р. шляхом об'єднання двох спецслужб: Центрального директорату загальної розвідки (RG) і Директорату нагляду за територіями (DST).

Завдання DGSI: боротьба з іноземним втручанням, включаючи шпигунство; виявлення і припинення терористичних проявів або підриву національної державності, територіальної цілісності або функціонування французьких держустанов; моніторинг діяльності міжнародних злочинних організацій, які можуть становити загрозу національній безпеці; попередження та припинення злочинів у кіберпросторі тощо.

Координаційна група по боротьбі з тероризмом (фр., Unité de coordination de la lutte anti-terroriste, UCLAT) забезпечує координацію всіх служб, що беруть участь у боротьбі з тероризмом. Створена у 1984 р., до її складу входять представники Національної поліції Франції та жандармерії. UCLAT організує обмін інформацією, в тому числі щодо захисту об'єктів КІ між оперативними підрозділами всіх органів влади, цивільними та військовими службами, які беруть участь у боротьбі з тероризмом, включаючи судову поліцію та тюремні адміністрації, тісно співпрацює з Центральною дирекцією внутрішньої розвідки, Генеральним директоратом зовнішньої безпеки, національною жандармерією та митною службою.

Міністерство оборони (фр., Ministère de la Défense) відповідає за оборону та безпеку французького народу, а також інтересів Франції за кордоном. Сприяє проведенню активної політики з питань міжнародного співробітництва, економічних та культурних питань на всіх континентах та дотримання міжнародних угод. Крім традиційних заходів щодо захисту держави від військової агресії міністерство активно здійснює заходи по захисту КІ і регулярно проводить зустрічі з МВС та Генеральним секретаріатом з питань оборони та національної безпеки для обговорення поза встановленими форматами (робочих груп, діяльності міжвідомчих центрів операцій тощо) загроз, планів військових операцій та інших тем, пов'язаних з ЗКІ.

Генеральний директорат зовнішньої безпеки (фр. Direction générale de la Sécurité extérieure, DGSE) – спецслужба французького розвідувального співтовариства, головний орган зовнішньої розвідки Франції. Підпорядковується міністру оборони.

Завдання Директорату закріплено в Кодексі оборони. До основних з них відносять: збір розвідувальної інформації, протидія шпигунській діяльності, розвідка за допомогою технічних засобів, в т.ч. і з використанням можливостей супутників розвідки, радіоелектронна розвідка «Frenchelon«, моніторинг громадських комп'ютерних мереж.

Директорат захисту та безпеки оборони (фр. Direction de la protection et de la sécurité de la défense, DPSD) – служба військової контррозвідки Франції, член французького розвідувального співтовариства. Взаємодіє з Генеральним директоратом зовнішньої безпеки (DGSE), Управлінням військової розвідки (DRM) і Головним управлінням внутрішньої розвідки (DCRI). Діяльність DPSD регулюється Кодексом оборони. До основних завдань відносять: захист від загроз (терористичної діяльності, шпигунства, підривної діяльності, диверсій та організованої злочинності); розробку та моніторинг виконання заходів у сфері безпеки збройних сил Франції; захист осіб, які мають допуск до інформації, що становить військову таємницю; проведення досліджень, пов'язаних з обробкою інформації, та здійс-

нення контролю за IT-безпекою.

DPSD веде свою діяльність у всіх місцях присутності збройних сил Франції, а також виконує завдання у сфері економічної контррозвідки (промислової безпеки) для захисту високотехнологічних оборонних підприємств.

Служба центрального інформаційного агентства (SCSSI) відповідає за регулювання використання криптосистем французьким урядом. Користувачі виконують ряд вимог SCSSI для забезпечення конфіденційності в роботі. Є дещо схожим органом до англійської GCHQ[42].

Міністерство юстиції (фр., Ministere de la Justice) є одним з базових в уряді. Здійснює нагляд за діяльністю суддів та прокурорів, пенітенціарною системою, надає пропозиції з удосконалення законодавства у кримінальній та цивільній сферах, процесуального законодавства.

Міністерство економіки та фінансів (фр., Ministère de l'économie et des finances) здійснює управління державними фінансами та економічною політикою французької держави. Міністерство відповідає за управління фінансовими і бюджетними питаннями, регулювання економіки та фінансового сектору, промисловості, зовнішньої торгівлі, діяльності підприємств[43].

Національний директорат розвідки та митних розслідувань (фр., Direction nationale du renseignement et des

[42] http://www.ssi.gouv.fr.

[43] http://www.parisinfo.com/musee-monument-paris/71397/Ministere-de-l-economie-de-l-industrie-et-de-l-emploi.

enquêtes douanières, DNRED) – підрозділ Генерального Директорату митних та акцизних зборів Франції (міністерство економіки та фінансів), відповідає за розвідку, контроль та боротьбу з шахрайством у сфері митних та акцизних зборів. В 2009 р. в ньому створено новий підрозділ під назвою «Cyberdouane», роль якого полягає в боротьбі з кіберзлочинами економічного характеру, такими як торгівля людьми онлайн, відмивання грошей в онлайн-казино, продаж нелегальної продукції онлайн (наркотики, контрафактна продукція, зброя, дитяча порнографія тощо).

Управління розвідки та протидії підпільним фінансовим схемам (фр., Traitement du Renseignement et Action contre les Circuits Financiers clandestins, TRACFIN) засноване при міністерстві економіки та фінансів Франції. Відповідає за боротьбу з відмиванням грошей, протидію фінансуванню тероризму та протидію легалізації коштів, одержаних злочинним шляхом. Інформацію щодо виявлених загроз, в тому числі і загроз КІ, передає поліції, митній службі та податковій службі, судовим органам.

Генеральний секретаріат міністерств освіти і науки (фр., Secrétariat général des ministères de l'éducation nationale et de l'enseignement supérieur et de la recherche) – керує публічною системою освіти. Його соціальне значення є вагомим, адже право на освіту закріплено в Загальній декларації прав людини. Це міністерство є найбільшим за штатом, а стаття витрат в бюджеті на освіту – однією з найбільших

по країні. Забезпечує наукове підґрунтя для захисту КІ.

Міністерство сільського господарства та продовольства (фр., Ministère de l'Agriculture et de l'Alimentation) відповідає за політику в галузі сільського господарства, рибальства, продовольства і лісового господарства. Організовує навчання і дослідження в цих сферах.

Міністерство екології (фр., Ministère de la Transition écologique et solidaire) відповідає за підготовку та реалізацію політики уряду в галузі сталого розвитку, навколишнього середовища та розвитку екологічних і зелених технологій, запобігання природним та технологічним ризикам, промислову безпеку, транспорт та інфраструктуру, охорону моря.

2.3. Німеччина розпочала визначати і захищати критичну інфраструктуру однією з перших у Європі. Федеральне відомство інформаційної безпеки, створене в 1991 р. на базі криптографічного відділу Служби зовнішньої розвідки Німеччини (BND), в подальшому передане в МВС, починаючи з 1998 р. є головним органом з питань забезпечення інформаційної безпеки у сфері захисту КІ. На базі BSI Information Security функціонує Національний центр кіберзахисту (Cyber-AZ). Для координації міжвідомчої діяльності з захисту КІ при МВС в 2002 р. створено міжміністерську робочу групу «AG KRITIS».

Критична інфраструктура (KRITIS) – це організації та установи, що мають надзвичайно важливе значення для держави та суспільства, вихід з ладу або погіршення функціонування яких можуть призвести до стійких зривів постачання, суттєвого порушення державної безпеки або інших драматичних наслідків[44].

Згідно з позицією німецької влади порушення цілісності КІ часто може мати «каскадний ефект», тобто шкода може швидко зростати у геометричній прогресії.

Федеральне міністерство внутрішніх справ виділяє 9 секторів критичної інфраструктури за відповідними галузями: енергетика (електрика, газ, нафта); вода (громадське водопостачання, комунальне водопостачання); харчування (харчова промисловість, торгівля продуктами харчування, забезпечення населення якісною їжею); інформаційні технології та телекомунікації; здоров'я (медичне обслуговування, лікарські засоби та вакцини, діагностика та лабораторні дослідження); фінанси та страхування (банки, біржі, страхові компанії, провайдери фінансових послуг); транспорт (авіація, морське судноплавство, внутрішнє судноплавство, залізничний транспорт, автомобільний транспорт, логістика); держава та адміністрація (уряд та адміністрація, парламент, судові органи, служби екстреної допомоги, включаючи цивільний захист); ЗМІ та культура (радіо, телебачення, друкована та електронна преса, культурна спа-

[44] https://sicherheitswiki.org/wiki/Kritische_Infrastrukturen.

дщина, пам'ятки архітектури). У зв'язку з інтенсивним використанням інформаційних технологій у критичних інфраструктурах інтерес також викликає інформаційна інфраструктура[45].

Німецька влада вважає, що процвітання Німеччини є можливим завдяки постійним державним інвестиціям у науково-практичні дослідження і розробки, які, в свою чергу, забезпечують значний ріст інновацій і ноу-хау. Ця ситуація є вирішальним фактором для активізації спецслужб іноземних держав та бізнес-конкурентів з отримання необхідних даних. Так, іноземні розвідувальні служби намагаються зібрати інформацію про нові технології і результати досліджень, щоб зменшити на це витрати власної економіки. Саме тому ефективний розвиток бізнесу в державі вбачається можливим завдяки покращенню системи захисту економіки – її як державного, так і приватного секторів. Загрози економіці несуть небезпеки, починаючи від терористичних актів, кібератак і закінчуючи економічним та промисловим шпигунством, диверсіями і конкурентною розвідкою[46].

Враховуючи зазначене, з кінця 1990-х рр. німецька влада почала створювати центри захисту КІ у складі органів безпеки. Для координації міжвідомчої діяльності з захисту КІ при МВС в 2002 р. створили міжміністерську ро-

[45] BSI-Kritisverordnung (BSI-KritisV), 22.04.2016. доступ https://www.buzer.de.

[46] https://www.bmi.bund.de/DE/startseite/startseite-node.html.

бочу групу AG KRITIS. Після реформ 2006 р. позиції підрозділів безпеки ще більш посилились[47]. Стратегічний розвиток КІ та заходи координуються за допомогою залучених міністерств.

Організаційна модель. Централізована правоохоронна модель ЗКІ, де важливу роль відіграють органи забезпечення державної безпеки та інші підрозділи МВС (BMI) із захисту громадської безпеки. Для координації міжвідомчої діяльності з захисту КІ при BMI створено міжміністерську робочу групу «AG KRITIS».

Нормативно-правове регулювання. Національна стратегія захисту критичної інфраструктури, 2009 р.; Стратегія кібербезпеки Німеччини, 2016 р.; Закон «Про безпеку інформаційних технологій«, 2015 р.; UP KRITIS: державно-приватне партнерство із захисту критичних інфраструктур, BSI, 2014 р.; Спільна інтернет-платформа BSI та BBK щодо захисту критичної інфраструктури; плани захисту КІ.

Основні учасники / обов'язки: Федеральне міністерство внутрішніх справ Німеччини (нім. Bundesministerium des Innern, BMI) виконує координаційну функцію щодо захисту критичної інфраструктури. Це випливає, зокрема, з його задач. BMI відповідає за забезпечення державної та громадської безпеки, захист населення від надзвичайних ситуацій, адміністративні питання.

[47] https://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx?pol=Civil%20Protection&c1=Poland&c2=Germany.

Сфера діяльності BMI охоплює захист конституційного ладу, а також захист громадян від насильства, злочинності і тероризму, видачу паспортів, посвідчень особи тощо[48].

Серед основних напрямів діяльності міністерства у сфері захисту КІ особливу увагу приділено контррозвідці, протидії кібершпигунству, захисту економіки (бізнесу) та державній безпеці.

Але не тільки уряд та великі компанії страждають від шпигунства – навіть невеликі компанії потенційно стають об'єктами розвідінтересу чи промислового шпигунства. Індивідуальні консультації і надання допомоги для всіх компаній, які потребують допомоги, розробляються спільно органами безпеки під егідою МВС і промисловістю в ініціативі Wirtschaftsschutz, розпочатій у 2016 р. та спрямованій на підвищення рівня захисту КІ.

Розвиток сучасних інформаційних і комунікаційних технологій впливає на порядок роботи іноземних розвідувальних служб та організацію контрзаходів[49]. Поряд з традиційними розвідувальними заходами із залученням людського ресурсу останнім часом значно зросла кількість кібератак на мережі і комп'ютерні системи урядових установ, а також приватних підприємств.

Основну участь у захисті КІ в структурі МВС покла-

[48] https://www.bmi.bund.de/DE/startseite/startseite-node.html.
[49] Там само.

дено на такі установи, що входять до сфери її управління: Федеральне відомство з інформаційної безпеки, Федеральне відомство з охорони Конституції, Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих, Федеральна кримінальна поліція, Федеральне агентство технічного сприяння.

Федеральне відомство інформаційної безпеки (Bundesamt für Sicherheit in Informationstechnik, BSI) – створене в 1991 р. на базі криптографічного відділу Служби зовнішньої розвідки Німеччини (BND). Інформація щодо формату співпраці між BSI та BND у сфері КІ не розголошується. BSI є головним органом з питань забезпечення інформаційної безпеки. Наділення органу повноваженнями щодо захисту КІ пов'язують із прийняттям директиви американського президента PDD-63 від 1998 р., яка стосується захисту КІ. Його задачі визначені Законом «Про Федеральне відомство інформаційної безпеки». Основними з них є: забезпечення інформаційної та кібербезпеки; сприяння безпечному функціонуванню інформаційно-комунікаційних систем у державі, для бізнесу та суспільства; тестування, сертифікація та акредитація ІТ-продуктів та послуг; заходи з попередження неякісного програмного забезпечення та виявлення вразливості в ІТ-продуктах та послугах; розробка стандартів та відповідних рекомендацій щодо захисту ІТ та проведення роз'яснювальної роботи з підвищення обізнаності громадян про безпеку інформа-

ційної сфери та мережі Інтернет; розробка криптосистем (таких як, наприклад, шифр Libelle) для державних потреб.

BSI тісно співпрацює з операторами КІ та здійснює обмін інформацією щодо загроз, готує узгоджену стратегію кібербезпеки.

На базі BSI з 2011 р. функціонує Національний центр кіберзахисту (Cyber-AZ), створений у ході виконання положень попередньої Стратегії кібербезпеки від 2011 р. для протидії кібершпигунству, кібертероризму та іншим кіберзлочинам. Основна мета його створення – пришвидшення обміну інформацією, оперативна оцінка та вжиття відповідних заходів реагування. Протягом кількох років центр розвинувся від звичайної інформаційної структури до центральної платформи співпраці органів безпеки в ІТ сфері.

З метою поглиблення державно-приватної співпраці у сфері ЗКІ та підтримки надання послуг операторами критичної інфраструктури (KRITIS) між ними, їх асоціаціями та відповідними державними установами, такими як BSI, у більшості секторів КІ запроваджено взаємодію «UP KRITIS» (державно-приватне партнерство).

Іншим прикладом державно-приватного партнерства у сфері захисту КІ є «CERT-Verbund» – коли групи безпеки і команди реагування на комп'ютерні інциденти (CERT) сприяють обміну інформацією (наприклад, про вразливість або інциденти) та співпрацю щодо усунення загроз. Спів-

праця з ними базується на угодах про нерозголошення інформації та на кодексі поведінки.

Федеральне відомство з охорони Конституції (нім., Bundesamt für Verfassungsschutz, BfV) – це одна з трьох розвідувальних служб Німеччини у сфері управління МВС, що здійснює контррозвідувальну діяльність. Діє на підставі Федерального закону про захист конституції та проводить пошукові заходи, спрямовані на контроль за діяльністю організацій антиконституційної спрямованості, діяльність яких загрожує вільному і демократичному порядку у Німеччині. У сфері оперативного контролю служби перебувають ультраправі, в тому числі неонацистські партії, ультраліві, ісламістські та інші екстремістські організації, крайньоналаштовані іноземні громадяни, розвідувально-підривна діяльність спецслужб іноземних держав. До компетенції органу також відносять притаманні для захисту від загроз КІ захист від диверсій, зривів виробництва (саботажу) і запобігання розголошенню інформації з обмеженим доступом тощо[50].

Досить важливою задачею BfV є захист економіки держави. З метою належного захисту об'єктів КІ та інформації, що функціонує на цих об'єктах, в тому числі комерційної таємниці, постійно здійснюється робота з покращення державно-приватного партнерства. BfV проводить інформаційно-роз'яснювальну роботу, розробляє рекомен-

[50] https://www.verfassungsschutz.de.

дації для операторів та проводить перевірку персоналу, якому надається доступ до роботи з інформацією з обмеженим доступом[51]. BfV надає рекомендації щодо захисту КІ. Вони в першу чергу включають протидію розвіддіяльності, організованій спецслужбами іноземних держав, протидію кібершпигунству. Досить тісно BfV взаємодіє з бізнесом.

Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих (нім., Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) – було створено в травні 2004 року у складі Федерального міністерства внутрішніх справ (BMI). Згідно з вимогами Закону «Про цивільний захист« виконує федеральні завдання у сферах цивільного захисту та ліквідації наслідків стихійних лих і є яскравим проявом реалізаії нової стратегії захисту населення та КІ в Німеччині із залученням різних учасників.

BBK для захисту КІ співпрацює з іншими зацікавленими державними і приватними гравцями у сфері. Координує заходи з ліквідації наслідків стихійних лих, займається фізичним захистом КІ та населення і його здоров'я, здійснює аналіз коротко-, середньо- і довгострокових ризиків для КІ, розробку планів захисту КІ та рекомендацій щодо комплексного управління ризиками та кризовими ситуаціями (взаємодія між державним і приватним секто-

[51] https://www.verfassungsschutz.de.

ром), консультації державних і приватних структур щодо планування та захисту КІ[52].

До обов'язків ВВК також входить підтримка адміністрації та громад, гармонізація федерального планування, аналіз досліджень, навчання персоналу, громадська інформація, стандартизація та забезпечення якості послуг у сфері захисту населення.

Бере участь у роботі Національного центру кіберзахисту (Cyber-AZ), який знаходиться у BSI.

Федеральне агентство технічного сприяння (нім., Technisches Hilfswerk, THW) є частиною німецьких сил цивільного захисту. Хоча організація входить в сферу управління МВС, 99% її членів є добровольцями. Їх загальна кількість у 2018 р. перевищує 83 тис. осіб. В 1950 році створювалась з метою організації цивільної оборони у випадку війни, однак наразі серед її основних завдань, визначених в Законі THW-Gesetz, виділяють: технічну та матеріально-технічну підтримку пожежних бригад, поліції, митних й інших органів на території Німеччини; відновлення критичної інфраструктури після великих пожеж або стихійних лих[53]. Серед основних послуг доцільно виділити боротьбу з повенями та затопленнями, вибухо-технічні роботи, забезпечення підтримки електропостачання, відновлення мостів, забезпечення питною водою, відведення сті-

[52] www.bbk.bund.de.
[53] http://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html.

чних вод. У випадку надзвичайних ситуацій – створення та функціонування командного пункту, тимчасових телекомунікаційних систем. THW є загальнонаціональною організацією надання технічної та гуманітарної допомоги в Німеччині та за її межами у випадку надзвичайних ситуацій, що здатна оперативно реагувати на загрози критичній інфраструктурі місцевого, регіонального та національного рівнів[54].

Федеральна кримінальна поліція (нім., Bundeskriminalamt, BKA) – відомство при Міністерстві внутрішніх справ Німеччини. Його функції схожі на функції Федерального бюро розслідувань США або Національної поліції Франції. BKA займається розслідуванням тяжких злочинів у важливих для держави сферах, для чого, у разі необхідності, залучає інші правоохоронні органи та координує спільні заходи. Співпрацює з поліцією земель Німеччини.

BKA відповідає за виявлення та припинення злочинів проти внутрішньої та зовнішньої безпеки Федеративної Республіки Німеччина. Підрозділи кримінальної поліції протидіють злочинам, що завдають шкоди або можуть спричинити знищення КІ, або стати серйозною загрозою для життя, здоров'я чи функціонування суспільства. До основних задач відносять: боротьбу з тероризмом, забезпечення безпеки в міжнародних аеропортах і на залізниці,

[54] www.thw.de.

забезпечення безпеки кордону, включаючи охорону морського узбережжя та повітряного простору, захисту офіційних осіб під час проведення заходів в межах країни.

Окрім BMI, кілька ключових міністерств забезпечують заходи із ЗКІ на федеральному рівні. Вони перелічені нижче.

Федеральне міністерство економіки і енергетики (нім., Bundesministerium für Wirtschaft und Energie, BMWi) – утворено в 2013 р., реалізує економічну політику та нагляд за кількома критичними секторами[55]. Воно відповідає за промислову, цифрову та інноваційну політику, послуги енерго-, електропостачання і безпеку мереж.

Федеральна мережева агенція (нім., Bundesnetzagentur, BNetzA). Входить у сферу управління BMWi. Регуляторний орган з питань електроенергетики, газу, телекомунікацій, поштових та залізничних мереж. Забезпечує умови конкурентності у цих сферах. Федеральна мережева агенція також відповідає за технічне регулювання в сфері телекомунікацій, забезпечує дотримання вимог використання частот, акредитує провайдерів, контролює діяльність та безпеку поштового зв'язку і надання послуг у залізничній та енергетичній сферах.

Федеральне Міністерство транспорту та цифрової інфраструктури (нім., Bundesministerium für Verkehr und digitale Infrastruktur, BMVI) створено в 2013 р. Зона відпо-

[55] www.bmwi.de.

відальності включає федеральну транспортну інфраструктуру (магістралі, шосе, залізничні мережі, водні шляхи та маршрути повітряного руху), цифрову інфраструктуру (загальнонаціональне постачання швидкого Інтернету та загалом розвиток і впровадження IT-технологій), а також пошук альтернативних джерел енергії та впровадження ноу-хау в цих сферах. До завдань також входить забезпечення безпеки на транспорті, а також планування та фінансування, спрямовані та підтримку і розширення інфраструктури[56].

Федеральне міністерство продовольства та сільського господарства (нім., Bundesministerium für Ernährung und Landwirtschaft, BMEL) основними задачами має проведення сільськогосподарської політики та політики в сфері продовольчих і харчових продуктів, а також забезпечення їх безпеки. У міністерстві окремий підрозділ слідкує за дотриманням безпеки продуктів та відповідає за забезпечення безпечної їжі. Саме гарантування здорової їжі в достатній кількості є головною умовою уникнення загроз в цій сфері критичної інфраструктури[57].

Федеральне міністерство навколишнього середовища, охорони природи, будівництва та безпеки ядерних реакторів (нім., Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, BMUB) виконує широкий спектр ос-

[56] http://www.bmvi.de/DE/Home/home.html.
[57] https://www.bmel.de.

новних задач, які прямо чи опосередковано впливають на критичну інфраструктуру. Проводить заходи, спрямовані на охорону навколишнього середовища, будівництва та містобудівну політику, управління водними ресурсами та їх захист, збереження та стале використання природних ресурсів, протидію забрудненню довкілля, забезпечення надійності будівництва, хімічної безпеки та безпеки ядерних реакторів, захист від опромінення, перевезення ядерних матеріалів та утилізація радіоактивних відходів.

Федеральне міністерство охорони здоров'я (нім., Bundesministerium für Gesundheit, BMG) проводить політику у сфері охорони здоров'я; є відповідальним за розробку законопроектів, розпоряджень та відомчих адміністративних правил[58]. Проводить роботу, спрямовану на розвиток якісної системи охорони здоров'я, поліпшення здоров'я населення, запобігання ризикам наркозалежності, підвищення безпеки лікарських засобів та захисту пацієнтів і безпеки у сфері загалом[59].

Федеральне міністерство фінансів (нім., Bundesministerium der Finanzen, BMF) відповідає за економічне зростання та фінансову стабільність країни. Забезпечує функціонування фінансової та фіскальної системи країни та її вихід на глобальний міждержавний рівень, в тому числі зміцнення позицій в ЄС. Несе відповідальність за підготовку

[58] http://www.bmg.bund.de/EN/Ministerium/ministry_node.html.
[59] https://www.bundesgesundheitsministerium.de.

федерального бюджету, формує бюджетну політику, оподаткування, здійснює нагляд за розвитком німецького ринку акцій та облігацій[60]. Крім того, сприяє європейській інтеграції і глобалізації фінансових ринків та європейській фіскальній політиці. При міністерстві функціонують: Федеральний орган фінансового нагляду (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin), Федеральна установа стабілізації фінансового ринку (Bundesanstalt für Finanzmarktstabilisierung, FMSA), Федеральне агентство з управління нерухомістю (Bundesanstalt für Immobilienaufgaben, BImA), Федеральний інститут спеціальних об'єднавчих завдань (Bundesanstalt für vereinigungsbedingte Sonderaufgaben), Федеральне центральне податкове управління (Bundeszentralamt für Steuern), Центр інформаційних технологій (Informationstechnikzentrum Bund, ITZ Bund), Митниця (Федеральна митна адміністрація, Zoll, Bundeszollverwaltung).

Спільно з зазначеними державними органами Мінфін контролює критично важливі для економіки Німеччини сфери ринку надання фінансових послуг, монетарної та цінової політики, здійснення контролю за банківськими установами.

Федеральне міністерство освіти та науки (Bundesministerium für Bildung und Forschung (BMBF) – Federal Ministry of Education and Research (BMBF)

[60] https://www.bundesfinanzministerium.de/Web/DE/Home/home.html.

Bundesministerium für Bildung und Forschung)[61] займається науковою розробкою проблематики захисту КІ; зазначену проблему включено в дослідницькі програми. Міжвідомчий підхід до захисту критичної інфраструктури реалізується в рамках Національної дослідницької програми «Дослідження для громадської безпеки» (Forschung für die zivile Sicherheit)[62].

2.4. В **Іспанії** у листопаді 2007 р., враховуючи напрямки глобальної політики безпеки та ініціативу Європейського Союзу щодо захисту критичної інфраструктури, також був створений Національний центр захисту критичної інфраструктури. Центр підзвітний Державному секретарю з питань безпеки, який затверджує та контролює виконання Національного плану захисту критичної інфраструктури. З питань захисту КІ державний секретар контактує із Європейською комісією та іншими державами.

Під *«критичною інфраструктурою»* Іспанії (дослівно перекладається «критично важлива»), як і в європейському законодавстві, розуміють: об'єкти, мережі, послуги, фізичне обладнання та інформаційні технології, пошкодження або знищення яких може суттєво вплинути на здоров'я, безпеку та економічний добробут громадян або на ефекти-

[61] https://www.bmbf.de.

[62] https://www.bmbf.de/de/sicherheitsforschung-forschung-fuer-die-zivile-sicherheit-150.html.

вне функціонування держави.

Вона включає такі сфери: електростанції та мережі, зв'язок, фінанси, сектор охорони здоров'я, продовольство, водосховища, зберігання, обробку та мережі, транспорт, аеропорти, морські та інші порти, пам'ятки національних меншин, а також виробництво, зберігання та транспортування небезпечних вантажів, таких як хімічний, біологічний або ядерний матеріал. Критерієм включення об'єктів до каталогу об’єктів КІ є сукупність факторів: масштаб, наслідки, час, завдані збитки, вплив на економіку та основні послуги.

Організаційна модель. В Іспанії захист КІ здійснюється централізовано, під чітким контролем з боку Уряду держави. Основні органи ЗКІ функціонують у сфері управління МВС, яке також є органом державної безпеки. Діяльність по ЗКІ координує Державний секретар з питань безпеки.

Національний центр захисту критичної інфраструктури (CNPIC) звітує Державному секретарю з питань безпеки. Головне управління з питань цивільного захисту (DGPCE) **є** відповідальним за розробку національного плану захисту КІ. Механізм протидії загрозам КІ побудований так, що оператор КІ інформує Національний Центр про загрози, Національний Центр інформує компетентні розвідувальні служби, а у випадку настання кризи – відповідні служби протидії.

Нормативно-правове регулювання. Іспанія розробляє стратегію національної безпеки та стратегію захисту критичної інфраструктури, Національний план захисту критичної інфраструктури та Національний каталог критичної інфраструктури, Програму попередження надзвичайних ситуацій. Серед основних нормативних актів, які регулюють захист критичної інфраструктури, доцільно вказати Конституцію Іспанії 1978 р., Закон 2/1986 від 13 березня 1986 р. «Про сили та органи безпеки», Королівський указ 770/2017 від 28 липня 2017 р., в якому розроблена структура Міністерства внутрішніх справ.

Основні учасники / обов'язки: Міністерство внутрішніх справ, МВС (ісп., Ministerio del Interior, MI) – є одним з тринадцяти міністерств Уряду та основним відомством, що відповідає за забезпечення безпеки громадян. До його сфери управління входять державні органи безпеки та органи правопорядку, пенітенціарні установи, цивільний захист населення; міністерство здійснює забезпечення безпеки дорожнього руху тощо[63].

У міністерстві основні повноваження з контролю за захистом критичної інфраструктури здійснює Державний секретар з питань безпеки (ісп., Dirección General de Administración de la Seguridad; англ., State Secretariat for Security), посада заступника міністра, який координує заходи Центру розвідки щодо протидії терористичним орга-

[63] http://www.interior.gob.es.

нізаціям та організованій злочинності (CITCO), Головне управління поліції, Генеральне управління цивільної гвардії. Інший заступник міністра МВС відповідає за діяльність Головного управління з питань цивільного захисту, надзвичайних ситуацій та Головного управління протидії тероризму та інші напрямки.

До повноважень МВС через які реалізується захист КІ, входять: підготовка та реалізація політики уряду стосовно забезпечення безпеки громадян; керівництво і координація сил та органів державної безпеки; забезпечення безпеки організацій та приватного персоналу; цивільний захист населення від надзвичайних ситуацій.

Державний секретар з питань безпеки також контролює діяльність спецслужб. Захисту КІ сприяють: Служба інформації цивільної гвардії (icп., Servicio de información de la Guardia Civil) та Генеральний комісаріат інформації (icп., Comisaria general de informacion, CGI), який ще називають «таємна поліція». Служба інформації цивільної гвардії забезпечує державну безпеку та громадський порядок, проводить оперативно-пошукові заходи для отримання даних щодо екстремістських та диверсійних проявів, організованих злочинних угрупувань, радикально налаштованих груп, поширення зброї масового знищення, а також відповідає за протидію тероризму[64].

Спільно зі спецслужбами у складі МВС заходи, спря-

[64] https://www.intelpage.info/comisaria-general-de-informacion.html.

мовані на захист КІ, проводять розвідувальні органи у структурі міністерства оборони. Центр розвідки збройних сил Іспанії (ісп. скороч., CIFAS) є допоміжним органом військової розвідки. До його задач входить оперативне забезпечення розвідувальною інформацією щодо зовнішніх загроз сухопутні війська, флот та повітряні сили.

Національний центр розвідки (ісп., Centro Nacional de Inteligencia, CNI) створений в 2002 р. як національний розвідувальний та контррозвідувальний орган. Здійснює збір інформації та інформує з важливих питань безпеки Уряд та територіальні адміністрації. В структурі CNI функціонує Бюро національної безпеки (ONS) – цей підрозділ відповідає за функціонування національної мережі захисту інформації з обмеженим доступом. Перевіряє стан охорони інформації, захищеність систем державного та приватного сектору та надає їм ліцензії для роботи з секретною інформацією. Іншим важливим підрозділом для захисту КІ, що функціонує у складі CNI, є Національний криптологічний центр (CCN). Він відповідає за забезпечення безпеки інформаційно-комунікаційних систем державних адміністрацій та тих, хто обробляє, зберігає або передає секретну інформацію. Здійснює криптоаналіз та шифрування електронними засобами, проводить технологічно-криптографічні дослідження і навчання персоналу з питань безпеки. При CCN діють орган сертифікації безпеки інформаційних систем та національна комп'ютерна команда криптологічного

центру реагування на комп'ютерні інциденти (CCN-CERT). Центр реагування на комп'ютерні інциденти (icп., Instituto Nacional de Ciberseguridad de España) займається збором інформації про інциденти у кіберпросторі, їх класифікацією та організацією протидії.

Виникнення структури «CERT» тісно пов'язано з боротьбою проти комп'ютерних вірусів, так званих «мережевих черв'яків«. Комп'ютерна команда екстреної готовності – Computer emergency response team, або CERT – у Європі носить назву «TF-CSIRT»[65].

Національний центр захисту критичної інфраструктури (icп., Centro Nacional de Protección de Infraestructuras Críticas, CNPIC). Основною метою створення CNPIC було вжиття заходів з підвищення безпеки та антитерористичної захищеності основних об'єктів іспанської економіки відповідно до назрілих проблем у сфері державної безпеки та зважаючи на директиву Європейської комісії від 20 жовтня 2004 року[66].

Центр підзвітний Державному секретарю з питань безпеки та діє у тісній взаємодії з ним. Державний секретар з питань безпеки, починаючи з 2007 р., затверджує та контролює виконання Національного плану захисту критичної інфраструктури. Він контактує з питань захисту КІ із Європейською комісією та іншими державами.

[65] https://www.incibe.es/que-es-incibe/como-trabajamos.
[66] http://www.interior.gob.es.

Центр відповідальний за захист КІ, внесення змін і підготовку Національного плану захисту критичної інфраструктури та Національного каталогу об'єктів критичної інфраструктури[67]. Каталог має гриф обмеження доступу «Таємно», оскільки містить інформацію про всі найважливіші об'єкти на території країни, їх місцезнаходження, право власності, їх послуги, необхідний для них рівень забезпечення безпеки.

CNPIC забезпечує цілодобовий моніторинг понад 3500 об'єктів КІ, таких як дороги, електроенергія або водопостачання та продовольство, що входять до каталогу критичної інфраструктури. Фахівці займаються спостереженням за фізичною і IT-безпекою, сприяють підвищенню стійкості і надійності мереж електронного зв'язку. CNPIC забезпечує керівництво, координацію дій залучених учасників та контроль за захистом національної критичної інфраструктури.

До основних задач Центру відносять: отримання від державних органів, органів безпеки і приватного сектору інформації щодо стану захищеності КІ, здійснення її аналізу та оцінки; оцінка загроз та аналіз ризиків для об'єктів КІ; підготовка інформаційних, комунікаційних та попереджувальних механізмів; залучення державних установ та організацій для захисту КІ.

У разі виявлення загроз в інформаційній сфері встано-

[67] http://www.cnpic.es.

влено такий порядок взаємодії. Оператор КІ інформує CNPIC, який у свою чергу інформує компетентні розвідувальні служби та, у випадку настання негативних наслідків, команду надзвичайних ситуацій (CERT).

Головне управління з питань цивільного захисту (ісп., Dirección General de Protección Civil y Emergencias, DGPCE) є підрозділом МВС Іспанії, що відповідає за розробку програми попередження надзвичайних ситуацій. Планує та координує співпрацю між відомствами з метою подолання надзвичайних ситуацій. У разі необхідності організовує надання чи отримання міжнародної допомоги[68].

DGPCE виступає як оперативно-координаційний центр з питань надзвичайних ситуацій на національному рівні. До його основних задач відносять: підготовку планів захисту населення; проведення досліджень, пов'язаних з аналізом ризиків, а також пілотні проекти профілактичного характеру, що сприяють запобіганню надзвичайним ситуаціям та катастрофам; розробка навчально-інформаційних програм для населення, а також сприяння участі громадськості у цивільному захисті від надзвичайних ситуацій; розробка освітніх програм для підвищення освіченості населення; сприяння проведенню досліджень з соціологічних, правових, економічних та інших аспектів, що стосуються цивільного захисту та надзвичайних ситуацій; надання пропозицій щодо бюджетного фінан-

[68] http://www.proteccioncivil.es.

сування сфери; координація навчання та підготовки персоналу Національної системи цивільного захисту для ефективної відповіді на надзвичайні ситуації; моніторинг перебігу надзвичайних ситуацій та залучення у разі необхідності додаткових суб'єктів для локалізації наслідків; сприяє діяльності Національного центру з надзвичайних ситуацій та національній мережі оповіщення, оперативному управлінню в надзвичайних ситуаціях[69].

Іспанська громадська гвардія (ісп., Guardia Civil, GC) входить до складу сил безпеки держави і перебуває у подвійному підпорядкуванні Міністерства Внутрішніх Справ та Міністерства оборони. Конституцією передбачено її обов'язок із забезпечення захисту прав і свобод іспанців та забезпечення громадської безпеки. GC патрулює сільські райони (включаючи дороги та порти, кордон, узбережжя та автомагістралі) і розслідує злочини, а національна поліція займається безпекою в містах, що перевищують 20 000 жителів.

Серед основних завдань, що пов’язані із критичною інфраструктурою, можна виділити: розвідка, боротьба з тероризмом та контррозвідка (SIGC); виявлення вибухових речовин (TEDAX); протидія інтернет-злочинності та кібератакам; пошук і збереження гірських порід (GREIM); охорона навколишнього середовища (SEPRONA); захист короля Іспанії та інших членів Іспанської королівської сі-

[69] https://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx.

м'ї; безпека аеропортів.

Національна поліція (ісп., Cuerpo Nacional de Policía, CNP) – поліцейська структура у складі МВС. Є складовою частиною сил безпеки держави, має п'ять основних підрозділів. Серед повноважень, які застосовуються з метою захисту КІ, за підрозділами можна виділити такі: судова поліція (здійснює виявлення та припинення діяльності організованої злочинності, незаконної міграції, економічних, фінансових злочинів, кримінальне переслідування діяльності, яка передбачає використання інформаційно-комунікаційних технологій (ІКТ) та кіберзлочинності на національному та транснаціональному рівнях, виявлення та припинення злочинів проти інтелектуальної та промислової власності), розвідка (включає антитерористичні підрозділи, знешкодження вибухових речовин), наукова поліція, громадський порядок (здійснює захист будівель та громадських об'єктів, високопосадовців, забезпечує безпеку приватних компаній), документи та іноземці. У випадку надзвичайних ситуацій CNP співпрацює зі службами цивільної оборони.

Міністерство енергетики, туризму та цифрових програм (ісп., Ministerio de Energía, Turismo y Agenda Digital, METAD) – створено у 2016 р. з метою реалізації урядової політики у сфері енергетики, туризму, телекомунікацій та інформаційного суспільства, а також розробки цифрової програми і переходу на цифрові технології.

Державний секретаріат з інформаційного суспільства та Цифрової програми (ісп., Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, SESIAD) – створений відносно нещодавно. До 2016 р. подібні задачі були покладені на державного секретаря з телекомунікацій та інформаційного суспільства в реорганізованому Міністерстві науки і техніки, промисловості, торгівлі, енергетики та туризму. До основних задач входить: проведення досліджень та реалізація політики щодо телекомунікаційної та інформаційної сфер; розвиток інфраструктури, сучасних телекомунікаційних послуг та інформаційного суспільства; підготовка та реалізація проектів, що сприяють впровадженню інформаційних технологій в усі сфери економічної та соціальної діяльності; сприяння забезпеченню безпеки інформаційних та комунікаційних технологій; залучення Міністерства енергетики, туризму та цифрових програм й інших органів з метою підвищення довіри до цифрової програми та безпеки інформаційно-комунікаційних мереж; контроль, перевірка та заходи впливу у сфері телекомунікацій, аудіовізуальних послуг та інформаційного суспільства.

Міністерство економіки, промисловості та конкурентоспроможності (ісп., Ministerio de Economía, Industria y Competitividad, MEIC) – відповідає за підготовку та впровадження політики уряду щодо різних економічних сфер та проведення реформ з метою підвищення конкурентос-

проможності вітчизняних суб'єктів господарювання, наукових досліджень, технологічного розвитку та інновацій у державному і приватному секторах, а також за торгівельну політику й підтримку підприємств та організацій на ринку.

2.5. У **Данії** відповідальність за захист критичної інфраструктури лежить на різних учасниках і включає як державний, так і приватний сектор. В ЗКІ беруть участь уповноважені міністерства. Важливе місце займають і спецслужби.

Під захистом КІ в основному розуміють збереження та продовження важливих функцій держави та суспільства у разі аварій і катастроф. Дещо менша увага приділена іншим видам загроз, наприклад у сфері державної безпеки, загроз фізичного знищення КІ, кіберзагроз тощо. Відповідно, центральну роль тут займає Данське агентство з управління надзвичайними ситуаціями (DEMA). Агентство контролює складання планів на випадок надзвичайних ситуацій та порядок дій залучених учасників тощо. Захист від кіберзагроз, терактів та шпигунства покладається на спецслужби (в складі МО та поліції), при них функціонують відповідні центри, до яких залучаються представники з різних зацікавлених відомств.

У Данії вживається таке поняття, як «критичні функції» для суспільства. *«Критичні функції»* – види діяльнос-

ті, товари та послуги, які забезпечують стале функціонування суспільства та потребують підтримки та відновлення у випадку аварій або катастроф.

Основні критичні функції зосереджені в секторах енергетики, транспорту, хімічної промисловості, інформаційних технологій та телекомунікацій.

Організаційна модель. Важливе місце у захисті КІ посідає міністерство оборони, до складу якого входить Данське агентство з управління надзвичайними ситуаціями (DEMA). Агентство є державним відомством, одним із основних учасників роботи з координації захисту КІ, та виконує низку оперативних, наглядових та регуляторних функцій щодо управління діями під час надзвичайних ситуацій та підготовки до них з метою збереження важливих функцій для суспільства.

Данська розвідувальна служба з питань оборони (DDIS) підпорядкована міністерству оборони. На базі Центру кібербезпеки DDIS (DDIS CSC) діє міжвідомча контактна група Cyber Security, до якої залучені керівники міністерств та приватного сектору. DDIS CSC є відповідальним за сферу кібербезпеки та виступає національним органом у сфері інформаційної безпеки.

Національна служба безпеки та розвідки Данії (DSIS) є спецслужбою, частиною данської поліції. Основними офіційно заявленими задачами DSIS є: боротьба з тероризмом, боротьба з екстремізмом, боротьба з шпигунством,

запобігання розповсюдженню зброї масового знищення та забезпечення державної безпеки. Центр консультування з питань безпеки (SD DSIS) надає різноманітні консультації щодо того, як захистити себе від загроз, таких як тероризм, екстремізм та шпигунство, з метою посилення безпеки та надійності данського суспільства. Консультує установи та суб'єкти, які є особливо вразливими або критичними для данського суспільства, власників та операторів данської критичної інфраструктури. Центр аналізу терористичних загроз (CTA) консультує данські органи влади щодо запобігання загрозам терористичних актів. До складу CTA входять працівники Національної служби безпеки та розвідки Данії, Міністерства закордонних справ Данії та Данського агентства з управління надзвичайними ситуаціями.

Нормативні акти. Законодавчою основою для захисту КІ в Данії є Закон «Про надзвичайні ситуації» від 2009 р. № 660, Акт керування діями (Інструкція) у випадку надзвичайної ситуації, Закон «Про Службу безпеки та розвідки Данії» від 2014 р. Закон «Про мережу та інформаційну безпеку» від 2016 р. запровадив систему добровільного інформування операторами КІ щодо загроз та конкретних випадків кібератак. Діє Національний план з надзвичайних ситуацій.

Методологія дій з організації захисту об'єктів критичної інфраструктури у випадку аварій, катастроф, стихійних лих розроблена у Законі «Про надзвичайні ситуації» від

10.06.2009 № 660 і міститься в частині «Аварійне планування». Згідно з цими правилами «окремі міністри повинні планувати збереження та продовження функцій у суспільстві у разі аварій та катастроф шляхом складання планів на випадок надзвичайних ситуацій. Плани повинні бути переглянуті в необхідних межах не рідше ніж раз у чотири роки»[70]. Органи місцевого самоврядування несуть відповідальність за організацію готовності до надзвичайних ситуацій, а також за підготовку планів заходів у випадку їх настання[71]. Міська рада готує план управління надзвичайними ситуаціями муніципалітету, який затверджується міською радою на засіданні. Районна рада готує план управління надзвичайними ситуаціями у регіоні. План приймається обласною радою на засіданні. Плани та пропозиції з внесення змін надсилаються до Данського агентства з надзвичайних ситуацій. Міністр оборони координує індикативні керівні принципи для підготовки планів[72].

Основні учасники / обов'язки: Данське агентство з управління надзвичайними ситуаціями (данс. Beredskabsstyrelsen; англ. The Danish Emergency Management Agency – DEMA) є державним відомством Данії в структурі Міністерства оборони. Агентство було створено відповідно до Закону «Про управління надзви-

[70] Закон Данії "Про надзвичайні ситуації" № 660 від 10.06.2009.

[71] http://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx.Denmark.

[72] Закон Данії "Про надзвичайні ситуації" № 660 від 10.06.2009.

чайними ситуаціями в Данії», від 1993 р. DEMA працює у тісній співпраці з ЄС, ООН, НАТО та кількома сусідніми країнами.

DEMA очолює контактну групу із захисту КІ (KG/KI), в межах якої організовано міжгалузеву співпрацю з питань захисту від аварій, катастроф, пожеж, військових дій.

Загальна мета контактної групи із захисту КІ – служити форумом для обміну інформацією та даними між національними органами щодо ризиків та загроз і протидії їм. Питання стосовно заходів ЗКІ по секторах вирішуються на рівні кожного відповідального міністерства/агенції. Всі владні органи Данії повинні планувати підтримку своїх найважливіших функцій у випадку великих аварій та криз.

Основна задача DEMA – мінімізувати наслідки аварій та катастроф для суспільства та запобігти спричиненню шкоди людям, майну та навколишньому середовищу. Відповідно, DEMA має низку оперативних, наглядових та регуляторних функцій щодо управління надзвичайними ситуаціями та підготовки до них. Данська пожежна та рятувальна служба складається з муніципальної пожежної та рятувальної служби, муніципальних та національних центрів підтримки, а також національної, регіональної пожежної та рятувальної служби. Пожежні та рятувальні центри можуть допомагати місцевим пожежним та рятувальним службам, міліції та іншим органам влади у випадку великих або тривалих нещасних випадків або катастроф,

де існує потреба у додатковій робочій або спеціалізованій техніці[73].

DEMA надає експертну пораду та допомогу органам влади з приводу інцидентів, пов'язаних із небезпечними хімічними або невідомими речовинами, а також від імені влади відповідає за захист населення та навколишнього середовища у випадку ядерної загрози, в тому числі і за межами держави. DEMA здійснює нагляд та надає поради місцевим пожежним та рятувальним службам та координує планування готовності на національному рівні до загроз надзвичайних ситуацій та стихійних лих, які можуть мати серйозний негативний вплив на критичні функції суспільства.

DEMA несе відповідальність за організацію планування, координацію Національного плану надзвичайних ситуацій, оцінку та моніторинг національних та міжгалузевих вразливостей, локалізацію аварій та катастроф, які можуть мати серйозний негативний вплив на критичні функції суспільства[74].

Модель аналізу ризиків та загроз DEMA (модель RVA) розроблена для державних установ, відповідальних за захист критичної інфраструктури суспільства. Модель має вигляд таблиць для ідентифікації та оцінки і базується на сценаріях для аналізу ризиків та загроз. Основна увага

[73] http://brs.dk.
[74] http://brs.dk/eng/inspection/contingency_planning/Pages/contingency_planning.aspx.

приділена вжиттю контрзаходів. Модель RVA складається з чотирьох частин:

– у частині 1 визначається мета та обсяг аналізу;

– у частині 2 містяться розроблені сценарії дій. Користувачі генерують власний сценарій дій на основі найбільш відповідних для них;

– у частині 3 користувачам надаються роз'яснення щодо оцінки ризиків та загроз, пов'язаних з кожним сценарієм. Ризики оцінюються за критерієм можливості настання та наслідків від них. Вразливість залежить від існуючих можливостей для відновлення та відповіді за кожним видом інциденту;

– у частині 4 представлені графічні сценарії у форматі ризику та вразливостей.

Модель супроводжується посібником користувача.

Міністерство оборони Данії (данс., Forsvarsministeriet) – до завдань міністерства входить загальне планування, розробка, управління та повний контроль питань, пов’язаних із військовим захистом. До складу міністерства входять: DEMA, командування оборони Данії (англ., Defence Command Denmark), командування внутрішньої гвардії (англ., Home Guard Command), Розвідувальна служба з питань оборони (англ., the Defence Intelligence Service), Генеральний суддя-захисник з питань оборони, Служба побудови оборони (англ., the Defence Construction Service), Данське Королівське управління навігації та гід-

рографії, Служба інформації та соціального забезпечення (англ., the Office for Information and Welfare Service), внутрішній аудит Данії, Секретаріат бухгалтерії та інші служби.

Міністерство оборони є відповідальним за організацію оборонних адміністративних та цивільних заходів, а також міжнародну співпрацю з питань забезпечення миру та суверенітету. До завдань також входить створення умов для безпечної навігації та спостереження за водами навколо Данії, Гренландії та Фарерських островів, а також контроль повітряного простору країни.

Данська розвідувальна служба з питань оборони (данс., Forsvarets Efterretningstjeneste, FE; англ., Danish Defense Intelligence Service, DDIS) є данською спецслужбою, відповідальною за зовнішню розвідку, а також військову розвідку. DDIS підпорядкована міністерству оборони.

Ця спецслужба є досить закритою, основні результати діяльності містяться у щорічному звіті, який оприлюднюється для загалу. DDIS збирає, аналізує та поширює інформацію щодо обставин, важливих для безпеки Данії, а також для безпеки данських військових частин, які беруть участь у міжнародних місіях[75]. Розвідувальна діяльність включає в себе збір інформації про політичний, фінансовий, науковий та військовий інтерес. Основу отриманої інформації складають дані, отримані переважно з-за кордо-

[75] https://fe-ddis.dk.

ну. Особлива увага приділена попередженню проявів терористичної діяльності. З цією метою отриману відповідну інформацію данська розвідувальна служба з питань оборони передає до МЗС, посольств та Національної служби безпеки та розвідки Данії для організації заходів протидії.

Після терористичних нападів у Парижі та Копенгагені у 2015 р. повноваження DDIS були розширені. Для посилення боротьби з тероризмом спецслужба отримала повноваження зі збору інформації та електронних даних щодо терористичних загроз, аналізу зазначеної інформації, попередження і розкриття терористичних проявів та боротьби з кібертероризмом[76].

До структури входять підрозділи: збору інформації та проведення операцій, аналізу, розвитку та ресурсів, а також центр кібербезпеки (данс. скороч., CFCS; англ., DDIS Cyber Security Center, DDIS CSC).

Протидію кіберзагрозам виділено як один з найважливіших пріоритетів. Шпигунство проти Данії може бути стратегічним, політичним та комерційним. Потенційна загроза з боку іноземних держав, наприклад через використання кібератак, впливає на формування громадської думки щодо захищеності та на соціально-економічні наслідки для держави. Кібершпигунство проти державних і приватних установ становить одну з найсерйозніших загроз Данії.

[76] https://fe-ddis.dk/SiteCollectionDocuments/FE/Beretning/FE_Beretning_2015_2016_printvenlig.pdf.

Окрім того, що Cyber Security Center є підрозділом DDIS, відповідальним за сферу кібербезпеки, він є національним органом у сфері забезпечення інформаційної безпеки. CSC розробляє рекомендації користувачам та постійно скеровує їм відповідні інструкції, як за наявності кібератак, так і з метою їх недопущення. За результатами аналізу кіберзагроз CSC готує додаткові аналітичні доповідні, де, в тому числі, містяться рекомендації із організації та покращення заходів безпеки користувачами. Державні органи та компанії можуть скористатися цим досвідом. У разі наявності даних про кібератаки важливих установ чи компаній CSC може ініціативно звертатись до них для сприяння у локалізації загрози[77].

Одним з основних завдань CSC є локалізація загроз від кібератаки і зменшення шкоди від неї. Спеціалісти кіберцентру діють за таким алгоритмом: визначення суб'єкта атаки, яким чином відбулася атака, можливі контрзаходи, розробка заходів із недопущення.

На базі DDIS CSC діє міжвідомча контактна група Cyber Security, до якої залучені керівники міністерств та приватного сектору. Також проводяться спільні заходи, конференції для зміцнення державно-приватного співробітництва.

Національна служба безпеки та розвідки Данії (данс.,

[77] https://fe-ddis.dk/SiteCollectionDocuments/FE_Beretning_2015_2016_printvenlig.pdf.

Politiets Efterretningstjeneste, PET; англ., Danish Security and Intelligence Service, DSIS) відповідає за внутрішню безпеку. DSIS є частиною данської поліції, але звітує безпосередньо міністру юстиції. Вони мають представників у всіх поліцейських дільницях Данії.

Правові основи діяльності DSIS встановив Закон «Про Службу безпеки та розвідку Данії» від 2014 р.

Метою діяльності DSIS є запобігання, розслідування та протидія діям, які створюють або можуть становити загрозу збереженню Данії як вільної, демократичної та безпечної країни. DSIS відповідає за виявлення, запобігання, розслідування та протидію загрозам свободи, демократії та безпеки данського суспільства, в першу чергу спричиненим тероризмом, політичним екстремізмом та шпигунством[78].

Основними задачами DSIS є: забезпечення державної безпеки, боротьба з тероризмом, боротьба з екстремізмом, боротьба з шпигунством та запобігання розповсюдженню зброї масового знищення[79].

Контртероризм охоплює попередження та припинення терористичних нападів та запобігає використанню території Данії як бази для підготовки терактів в інших країнах. Крім того, вона збирає докази для переслідування терористів.

[78] https://www.pet.dk/English.aspx.
[79] Там само.

Окрім трьох основних напрямків, DSIS також надає консультації данським компаніям щодо того, як протидіяти шпигунству, безпосередньо бере участь у протистоянні промисловому шпигунству лише якщо виявлено іноземну сторону. Виконує роль радника з питань національної безпеки данського уряду, органів державної влади та інших гілок поліції, а також ряду інших заходів, загальних для вітчизняних організацій безпеки.

DSIS також забезпечує фізичну охорону політиків та інших осіб[80].

Основними структурними підрозділами є:

– Центр консультування з питань безпеки (англ., The Security Department) – надає різноманітні консультації щодо того, як захиститися суспільству від загроз, таких як тероризм, екстремізм та шпигунство. Консультації з питань безпеки проводяться установам та суб'єктам, які є особливо вразливими або критичними для данського суспільства. Це можуть бути члени парламенту, королівської сім'ї, міністерства та відомства, а також державні підприємства. DSIS також консультує власників та операторів данської критичної інфраструктури, увага особливо зосереджена на секторах енергетики, транспорту, інформаційних технологій та телекомунікацій. Крім того, DSIS також тісно співпрацює з Міністерством закордонних справ з питань захисту посольств Данії та їх персоналу від загроз безпеці. В

[80] http://www.pet.dk/English/About PET/PETs organisation.aspx.

рамках зусиль, спрямованих на зміцнення надійності та безпеки данських компаній у відповідь на загрозу тероризму, організованої злочинності та шпигунства, DSIS також взаємодіє з галузевою організацією «Конфедерація данської промисловості». У жовтні 2014 р. DSIS запустив консультативну програму, що називається RASK – «ризикована поведінка» або «культура безпеки». RASK спрямована на поліпшення ефективності державно-приватного партнерства у сфері захисту критичної інфраструктури, підвищення обізнаності приватного сектору, органів державної влади та правоохоронних органів. Акцентовано, що якісне протистояння загрозам залежить від ставлення до проблеми кожного громадянина[81]. З 2009 р. діяв проект «Projekt Sikkerhedsradgivning» (англ., Project Security Counselling) щодо консультацій у сфері безпеки критичних секторів;

– Центр аналізу терористичних загроз (англ., Center for Terror Analysis, CTA) був створений в 2007 р. в рамках виконання Урядового плану дій щодо боротьби з тероризмом. CTA аналізує загрозу тероризму всередині країни та за кордоном. До складу CTA входять працівники, які є аналітиками DDIS, DSIS, DEMA та Міністерства закордонних справ;

– Департамент превентивної безпеки (The Preventive Security Department) надає пропозиції з питань безпеки ор-

[81] https://www.pet.dk/Forebyggende/Afdeling/media/Afdeling/RASKmarkedsfringsbrevpdf.ashx.

ганам державної влади, організаціям та приватним компаніям. Налагоджує партнерські відносини з національними та міжнародними учасниками, які сприяють запобіганню радикалізації та крайньому екстремізму, а також консультує з питань безпеки в ряді галузей, включаючи фізичну безпеку, інформаційну безпеку та перевірку об'єктів.

Міністерство транспорту, будівництва та житлово-комунального господарства (данс., Transport-, Bygnings- og Boligministeriet; англ., The Ministry of Transport Building, and Housing) відповідає за дороги, забезпечення послуг на транспорті, залізниці, в аеропортах, гаванях та пошті.

Міністерство транспорту, будівництва та житлово-комунального господарства займається плануванням, будівництвом, експлуатацією та підтримкою державної транспортної інфраструктури, а також регулюванням та наглядом за транспортною системою Данії. Міністерство також управляє майном держави, регулює вимоги до будівництва, відповідає за забезпечення житлом громадян, оновлення міст.

Крім того, міністр транспорту, будівництва та житлово-комунального господарства здійснює стратегічне планування та формування політики в сфері діяльності міністерства, а також розробляє закони, розпорядження тощо з метою реалізації політики уряду[82].

[82] https://www.trm.dk/da/ministeriet.

Міністерство вищої освіти та науки (данс., Uddannelses- og Forskningsministeriet) відповідає за наукові дослідження та освіту шкільну і позашкільну. Основною задачею міністерства є сприяння та координація зусиль для взаємодії між промисловістю та торгівлею, центрами досліджень КІ та освіти, а також розвиток науково-дослідницької сфери.

Агентство з оцифрування (англ., Agency for digitisation) засноване в 2011 р. на базі Міністерства фінансів та відповідає за політику уряду щодо переходу на цифровий зв'язок та використання цифрових технологій в інтересах суспільства[83].

Агентство координує діяльність державних органів під час реалізації державної стратегії розвитку цифрових технологій 2016-2020 рр. Є власником програмного продукту для цифрової інфраструктури, що діє спільно з державним сектором. Сприяє та бере участь у спільній роботі державного сектору, бізнесу та неурядових організацій з метою пришвидшення переходу на цифрові телекомунікації. Крім того, розробляє бізнес-плани та плани підтримки, політики в галузі ІТ-технологій.

Данське енергетичне агентство (англ., The Danish Energy Agency) займається виробництвом і постачанням енергії на національному та міжнародному рівнях, а також вживає заходів зі скорочення викидів парникових газів.

[83] https://en.digst.dk/about-us.

Агентство відповідає за весь ланцюжок завдань, пов'язаних з виробництвом, постачанням та споживанням різних видів енергії, а також аналізом впливу на клімат, скорочення викидів парникових газів. Забезпечує правову основу для функціонування та формує політику розвитку енергетики в Данії. Це агентство при Міністерстві клімату, енергетики та комунальних послуг (англ., the Ministry of Climate and Energy).

Головне завдання Адміністрації данського бізнесу (англ., Danish Business Authority) – сприяти ефективному та стабільному економічному розвитку держави.

Низький ріст промисловості останніми роками послабив конкурентоспроможність Данії на світових ринках. Тому Адміністрація зміцнює умови для росту прибутку в тих сферах, де Данія має сильні та потенційні можливості, наприклад сфера туризму.

3. ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Узагальнення організаційно-правових підходів до захисту КІ у різних європейських державах дозволяє сформувати думку про те, що владні органи зазвичай приділяють досить важливу увагу процесу визначення загроз та формуванню їх переліків. У різних країнах спектр загроз критичній інфраструктурі та зміст поняття, хоч загалом і містять багато схожого, проте визначаються індивідуально з урахуванням безпекової ситуації та пріоритетів розвитку, визначених державною політикою[84]. Якщо в більшості держав вони законодавчо передбачені, то, поряд з цим, деякі з них можуть не мати чіткого переліку загроз. Так, на відміну від європейської, зокрема німецької, системи розподілу загроз для об'єктів КІ, де чітко вирізнено основні їх види та підвиди і дається вичерпний їх перелік, США чіткого переліку таких загроз не мають. При цьому не існує

[84] Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав // Актуальні проблеми вдосконалення чинного законодавства України. Івано-Франківськ, 2017. № XLIV. С. 224-235.

загального єдиного підходу і до організації протидії їм[85].

Європейський дослідник у сфері захисту КІ М. Сметана стверджує, що останніми десятиліттями у Європі питання аналізу загроз значно актуалізувалось. Питання ідентифікації загроз та організації заходів з протидії їм стає актуальним для більшості держав та особливо пов'язується із загрозами природного характеру. При цьому значення роботи з визначення та своєчасної ідентифікації загроз для вжиття адекватних заходів реакції з кожною такою подією зростає. Водночас росте і глобальність підходів до визначення загроз. Якщо спочатку цей процес характеризувався локальним чи державним рівнем, то зараз можна стверджувати про його вихід на загальноєвропейський чи міжконтинентальний формат.

У США під *«загрозами КІ»* розуміють природні або техногенні явища, фізичних осіб, суб'єкти чи дії, що містять або несуть потенційну шкоду для життя, інформації, операцій, навколишнього середовища та/або власності[86].

Відповідно до національної політики США щодо захисту КІ, першочерговою загрозою для безпеки вбачаються кібератаки. Саме тому США були серед ініціаторів гло-

[85] Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США // Науковий вісник ДДУВС. Дніпро. 2017. № 3. С. 135-140.

[86] National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication.

балізації та об'єднавчих процесів у питанні міжнародної кооперації з протидії кіберзлочинності[87]. Завдяки зусиллям американців значно активізувались процеси створення відповідних центрів та виділення сил і засобів в інших світових державах для боротьби з небезпеками такого роду. Серед інших основних видів загроз для КІ США виділяють терористичні атаки (зокрема, на підприємствах хімічної промисловості, тобто такі, які у разі знищення або ураження можуть призвести до техногенних катастроф та масової загибелі людей) та стихійні лиха.

США значно вплинули на формування європейських підходів до виявлення та протидії загрозам КІ. Наразі об'єднана Європа має власні органи із захисту КІ. Діють експертні групи з критичної інфраструктури (CIP), інформаційна мережа з попередження загроз критичній інфраструктурі (CIWIN) тощо. Європейська комісія визначає принципи та інструменти, необхідні для впровадження Європейської програми захисту критично важливої інфраструктури (EPCIP), спрямованої на європейську та національну інфраструктуру кожної держави-учасниці.

Серед основних загроз відповідальні інстанції ЄС визначають: кіберзагрози, тероризм, злочинні дії, природні

[87] Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / Бык В.В., Климчук А.А., Панченко В.Н., Петров В.В. К., 2013. 220 с.

небезпеки, аварії та інші причини нещасних випадків[88].

Згідно з нормативно-правовими актами ЄС, *загроза* – будь-яка подія, яка може порушити або знищити критичну інфраструктуру або будь-який з її елементів[89]. Майже ідентичне визначення загроз дається в Зеленій книзі щодо захисту КІ ЄС, де під цим терміном розуміються будь-які обставини або події, що можуть порушити стале функціонування або знищити критичну інфраструктуру чи будь-який її елемент. Вони також включають спроби та наміри завдання шкоди критичним активам[90].

Часто дія загроз може спричиняти «каскадний ефект» («ефект доміно»), коли дестабілізація однієї складової КІ тягне за собою порушення нормального функціонування інших складових та викликає широкомасштабне катастрофічне явище. Під **«каскадним ефектом»** від порушення функціонування КІ пропонується розуміти серію пов'язаних подій, кожна наступна з яких спричинена попередніми та тягне за собою настання нових.

Серед європейських країн доцільно виділити активну

---

[88] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260 / European Program for Critical Infrastructure Protection; Повідомлення Комісії Раді та Європейському Парламенту від 20 жовтня 2004 року «Запобігання, готовність та реагування на терористичні напади» / COM (2004) 698 final – Official Journal від 20.01.2005. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex: 52004DC0702.

[89] Там само.

[90] https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

діяльність з ідентифікації та аналізу загроз КІ, що проводиться Німеччиною. Згідно з «Концепцією основних заходів із захисту КІ Німеччини» поняття *«загроза»* визначається як можливість настання подій (стихійних явищ, технічних збоїв чи людських прорахунків, помилок в поведінці людей), що можуть спричинити шкоду особам, матеріальним цінностям і навколишньому середовищу чи призвести до розладу соціальних та економічних відносин.

Загрози для КІ поділяють на три основні види: загрози від стихійних явищ, від людських прорахунків та технічних збоїв, а також загрози від тероризму і злочинних дій. У свою чергу, в Німеччині чітко визначено, що екстремальними погодними умовами є: паводки (включаючи підвищення рівня ґрунтових вод), повені, затоплення, штормові припливи, сніг, лід, посухи, а також бурі, урагани, землетруси, пожежі та штормові явища, також епідемії та пандемії. Пожежі можуть виникати природним шляхом у результаті удару блискавки, самозаймання або навмисного чи ненавмисного підпалу в поєднанні з тривалою посухою. Зсув може викликатися геофізичними явищами (наприклад, землетрусом, ерозією), метеорологічними впливами (наприклад, сильними опадами, повенями, таненням снігів і льоду) і антропогенними впливами (наприклад, будівельними роботами, землетрусами, вирубкою лісів). Прикладами зміщення мас є лавини, зсуви і розрідження ґрунту.

Також виділяють загрози від фізичного впливу зсере-

дини і зовні об'єктів КІ, загрози, які виходять від людських прорахунків та технічних збоїв, тероризму або злочинних діянь.

Прикладом загрози зсередини об'єкта може бути так звана «навмисна помилка» (авт. назва), наприклад умисне неправильне програмування систем управління, що призводить до аварій чи зупинки виробництва, втручання в роботу важливих частин установки з використанням наявних на будь-якому підприємстві допоміжних засобів й інструментів. Зовнішніми загрозами може вважатись аварія транспортного засобу, підпал, використання вибухових речовин, обстріл, авіакатастрофа, застосування хімічної, біологічної, радіологічної або ядерної зброї (ХБРЯ). Зловмисниками можуть бути застосовані і комбіновані дії.

Франція спочатку розпочала захищати критичну інфраструктуру в інформаційно-комунікаційній сфері. Однак, у зв'язку з розповсюдженням у світі кіберзагроз та ростом терористичних проявів, з 2009 р. організація протидії цим загрозам була покладена на Генеральний секретаріат з питань оборони та національної безпеки (SGDSN). SGDSN аналізує відкриту інформацію та розвіддані у сфері захисту КІ, слідкує за недопущенням різного роду внутрішніх та зовнішніх загроз[91].

У Великобританії з початку побудови системи захисту КІ в першу чергу звернули увагу на необхідність захисту

[91] http://www.sgdsn.gouv.fr.

від загроз у сфері державної безпеки. Тому тривалий час функціонував Національний координаційний центр з безпеки інфраструктури (NISCC) та Центр консультацій з національної безпеки (NSAC, був підрозділом контррозвідки MI-5). Згодом на їх базі був утворений Центр по захисту національної інфраструктури (CPNI), що надає комплексні консультації з питань безпеки підприємствам і організаціям, які є операторами критичної інфраструктури, включаючи інформаційні, кадрові та технічні аспекти безпеки, допомагаючи знизити вразливість національної критичної інфраструктури від тероризму та інших загроз.

Згодом функції з протидії загрозам у сфері комп'ютерної безпеки були передані Національному центру кібербезпеки (NCSC).

Забезпечення стійкості та підвищення захищеності Великої Британії у боротьбі з надзвичайними ситуаціями та відповідного широкого кола загроз є завданням Секретаріату з питань надзвичайних ситуацій (CCS), який сприяє діяльності Центру управління кризовими ситуаціями (COBR), що забезпечує швидке вироблення єдиної позиції та вжиття скоординованих заходів протидії наявним загрозам[92].

На відміну від вищерозглянутих країн Данія у сфері КІ серед основних виділяє та вживає заходи з протидії загрозам від надзвичайних ситуацій (аварій, катастроф, сти-

[92] http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.

хійних лих). Тому значними повноваженнями наділене Данське агентство з управління надзвичайними ситуаціями (DEMA). Під захистом КІ в основному розуміють збереження та продовження важливих функцій держави та суспільства у разі аварій та катастроф.

У Нідерландах діє міжміністерська група та міжвідомча програма «національної оцінки ризиків», останні визначаються на основі аналізу загроз. Очолюють зазначену групу Директорат національної безпеки та Міністерство внутрішніх справ та королівських відносин. Важлива увага приділяється протидії загрозам від тероризму, кіберзагрозам, забезпеченню національної безпеки та кризового управління, за що відповідає Національний координаційний центр з питань боротьби з тероризмом та забезпечення безпеки (NCTV).

Питання протидії загрозам, пов'язаним з терористичними проявами, для Нідерландів стало актуальними давно. Ще в 2004 р. було створено Національний координаційний центр протидії тероризму (NCTb), метою якого була координація діяльності поліції, судової влади, служб безпеки (наприклад, Генеральна служба розвідки і безпеки – AIVD) та інших організацій у сфері боротьби з тероризмом. З часом Нідерланди почали ширше розглядати загрози КІ та для протидії їм у 2012 році об'єднали NCTb з Дирекцією національної безпеки та Командою з реагування на інциденти в комп'ютерній сфері (GOVCERT.NL). Новостворе-

ною організацією став Національний координаційний центр з питань боротьби з тероризмом та забезпечення безпеки.

Генеральна служба розвідки і безпеки зосереджується головним чином на внутрішніх невійськових загрозах та протидії внутрішнім і зовнішнім загрозам національній безпеці. Служба військової розвідки та безпеки (MIVD) зосереджується на міжнародних загрозах, зокрема на військових та загрозах державній безпеці, таких як шпигунство.

Румунія здійснює поділ загроз КІ на такі, які можуть мати природний, випадковий або умисний характер.

Притаманні для України загрози КІ можуть мати різновекторні спрямування та прояви. Вони можуть проявлятися у припиненні надання товарів та послуг, що є життєво важливими для населення, економіки, державного управління. Такими є забезпечення населення, суб'єктів господарювання та органів державної влади і самоврядування електроенергією, зв'язком, послугами з транспортних перевезень, водопостачання, водовідведення, каналізації тощо. Припинення надання таких товарів та послуг, в деяких випадках навіть суттєве підвищення вартості тарифів, може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

Особливу загрозу становить збройний конфлікт та гібридна війна, що активно проводяться стосовно України,

та пов'язані із ними загрози деструктивних дій з боку диверсійних груп, вчинення терактів, диверсій, шпигунства, кібератак, економічної експансії стосовно об'єктів КІ тощо.

Завжди актуальними є загрози від надзвичайних ситуацій, які поєднують в собі загрози природнього, техногенного характеру тощо.

Саме тому Стратегією національної безпеки України, яка введена в дію Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»« від 26.05.2015 № 287/2015, визначено актуальні загрози національній безпеці та критичній інфраструктурі зокрема. Серед загроз безпеці КІ виділено такі: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення. Разом з цим серед загроз кібербезпеці і безпеці інформаційних ресурсів у Стратегії також визначено уразливість об'єктів критичної інфраструктури до кібератак.

Слід констатувати, що в Україні відсутнє законодавче визначення поняття «загроза критичній інфраструктурі» та немає загального підходу щодо їх класифікації. Як зазначають вітчизняні дослідники цієї наукової проблеми, така ситуація склалася природним чином: «кожне окреме ві-

домство виділяло певний спектр загроз для підпорядкованих об'єктів та володіло певним набором інструментів і ресурсів для забезпечення їх безпеки»[93]. У результаті в чинному законодавстві України визначено низку категорій об'єктів, для яких регламентуються особливі умови забезпечення захисту, зокрема підприємства, що мають стратегічне значення для економіки та безпеки держави; особливо важливі об'єкти електроенергетики й нафтогазової галузі; потенційно небезпечні об'єкти, об'єкти підвищеної небезпеки; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони, та об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій та в особливий період; інші об'єкти й системи, такі як системи зв'язку, платіжні системи тощо.

Водночас у нашій державі протидія загрозам КІ здійснюється з використанням трьох існуючих державних систем реагування та захисту, зокрема: 1) єдиної державної системи цивільного захисту (Положення затверджено постановою Кабінету Міністрів України від 09.01.2014 № 11); 2) єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджено постановою Кабінету Міністрів України від 15.08.2007 № 1051); 3) державної системи фізичного захисту (Порядок функціонування затверджено постановою

[93] Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі // Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 90-92.

Кабінету Міністрів України від 21.12.2011 № 1337).

Крім того, наразі на виконання положень введеної у дію Указом Президента України від 16 березня 2016 р. Стратегії кібербезпеки України створюється Національна система кібербезпеки, завдання якої тісно пов'язані із захистом критичної інфраструктури.

У частині 4 ст. 1 Закону України «Про основи національної безпеки» (в редакції від 19.06.2003 № 964-IV) законодавцем визначено «загрози національній безпеці» як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України. У частині 6 ст. 1 чинного Закону України «Про національну безпеку України» (від 21.06.2018 № 2469-VIII) під «загрозами національній безпеці України» розуміють явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Аналіз ст. 19 Закону України «Про національну безпеку» дає можливість стверджувати, що основними загрозами КІ у сфері державної безпеки є: розвідувально-підривна діяльність, тероризм, кіберзагрози, загрози економічного характеру та державності, спрямування до державної таємниці. Стаття 22 розширює зону протидії загрозам в інформаційній сфері, окрім державної таємниці, до кіберзахисту критичної інформаційної інфраструктури, державних

інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Крім того, у п. 6 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» дається визначення одного із видів загроз критичній інфраструктурі. Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів. Вводяться такі терміни, як кіберрозвідка, кібертероризм, кібершпигунство, що дозволяють більш широко розглядати проблему загроз КІ у сфері забезпечення кібербезпеки.

Відповідно до Стратегії кібербезпеки України, затвердженої указом Президента України від 15.03.2016 № 96/2016, поміж об'єктів, на які можуть бути спрямовані кіберзагрози, виділено такі: економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України.

Серед загроз кібербезпеці також виділено: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інфор-

мації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Згідно з розпорядженням Кабінету Міністрів України від 06 грудня 2017 р. № 1009-р «Про схвалення концепції створення державної системи захисту критичної інфраструктури» серед загроз КІ виділено такі: загрози природного і техногенного характеру, загрози, спричинені протиправними діями та будь-якими комбінаціями з переліченого.

На думку низки науковців, загрози КІ також доцільно розподіляти на три групи, що включають: аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії)[94].

У своїх наукових напрацюваннях О.М. Суходоля серед основних загроз КІ виділяє: надзвичайні ситуації (при-

[94] Радаев Н. Оценка террористической угрозы для объекта / Н. Радаев, А. Бочков. URL: http://mx1.algoritm.org/arch/77/77_3.pdf.

родні катастрофи, технологічні аварії), терористичні акти, диверсії, кіберзагрози тощо. На особливу увагу заслуговує позиція вченого щодо проблеми розширення загроз КІ, зокрема виділення втручання в систему управління КІ чи технологічний процес, руйнування об’єкта силами його ж персоналу. Таку загрозу ним пропонується ідентифікувати як чинник «внутрішнього порушника». Як вважає дослідник, саме цей чинник міг призвести до успіху кібератаки на енергорозподільчі компанії України[95].

На наше переконання, виділення загроз подібного характеру дійсно є необхідним, особливо за сучасних умов «гібридної війни», та відповідає існуючим тенденціям в іноземній практиці. Автором розглядається доцільність виділення такої категорії протиправних дій, як *«навмисна помилка»* – умисні дії для приведення будь-якої системи чи установки в критичний стан, що хоч частково і охоплюються об'єктивною стороною складу злочину «диверсія» (ст. 113 КК України), проте несуть меншу суспільну небезпеку, та суб’єктивною стороною діяння (зокрема, мета не має такого масштабного характеру – мається на увазі зниження економічного, науково-технічного потенціалу держави, а може полягати в бажанні дестабілізувати роботу лише певного вузла, припинити певний вид діяльності об'єкта КІ тощо. Прикладом «навмисної помилки» можуть

[95] Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України // Стратегічні пріоритети. Серія: Політика. 2016. № 3. С. 65-67.

бути дії в обслуговуванні обладнання, маніпуляціях з ними, такі як умисне неправильне програмування систем управління, втручання в роботу важливих частин установки з використанням наявних на будь-якому підприємстві допоміжних засобів і інструментів.

Серед основних загроз КІ Д. Бобро виділяє: техногенні аварії та технічні збої, викликані, зокрема, людськими помилками; природні лиха та небезпечні природні явища; зловмисні дії[96].

Науковці НІСД в „Зеленій книзі" обґрунтовують ймовірність виникнення загроз КІ від: аварій та технічних збоїв, небезпечних природних явищ, зловмисних дій[97].

У нормативно-правовій сфері нашої держави вже існує подібна класифікація. Так, статтею 5 Кодексу цивільного захисту України від 02.10.2012 № 5403-VI залежно від характеру походження події, що можуть зумовити виникнення надзвичайних ситуацій на території України, розподіляються на події: 1) техногенного характеру; 2) природного характеру; 3) соціальні; 4) воєнні.

Враховуючи національний досвід творення норм у сфері національної безпеки та міжнародну практику, доцільно сформулювати загальне визначення загроз КІ. Так,

[96] Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі // Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 90-92.

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

під **„загрозами об'єкту КІ"** пропонується розуміти наявні або потенційно можливі явища і чинники, що можуть нанести шкоду такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України.

Загалом, серед **загроз критичній інфраструктурі** автором пропонується виділяти такі їх **види:**

1) загрози у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвіддіяльність іноземних спецслужб, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка). Вони можуть включати внутрішні загрози та фізичне знищення КІ (при хуліганстві, підпалах, діяльності організованих злочинних угруповань, чинник «внутрішнього порушника»);

2) кіберзагрози (інформаційні атаки, кібертероризм);

3) загрози від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха, пожежі, епідемії та пандемії, застосування засобів ураження або інші небезпечні події).

Від мети дій, що їх спричиняють, для зручності кваліфікації загроз, у т.ч. крізь призму правової оцінки можливо протиправної діяльності, пропонується виділяти події та/або явища ненавмисного характеру (технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору), навмисні дії (терористичні акти, акти кібертероризму, диверсії, дії «внутрішнього порушника», «на-

вмисну помилку», розвідувальну діяльність, конкурентну розвідку тощо).

Також можна класифікувати загрози за значною кількістю критеріїв: від *характеру походження* (природного та техногенного характеру, а також навмисні дії), *ступеня поширення, розміру людських втрат та матеріальних збитків, втрат для безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку тощо*. Залежно від *наслідків, обсягів ресурсів, необхідних для їх локалізації*, доцільно виділити такі *рівні загроз: 1) державний; 2) регіональний; 3) місцевий; 4) об'єктовий.*

Важливою характеристикою загрози є її потенціал. В академічному тлумачному словнику української мови під ним розуміються приховані здатності, сили для якої-небудь діяльності, що можуть виявитися за певних умов; запас чого-небудь, резерв[98]. Під ***«потенціалом загрози»*** будемо розуміти ступінь прихованих здатностей загрози. Наприклад, енергетичних, ресурсних (матеріальних або нематеріальних, технічних та людських), діапазону кліматичних факторів та ін. Оцінка потенціалу загрози має важливе значення для визначення масштабів ураження об'єкта КІ загрозами і ризиків від них. Чим більшим є потенціал у загрози, тим більшим є ризик від неї для об'єкта КІ.

Потенціал загрози може бути оцінений кількісно з ви-

[98] Словник української мови: в 11 томах. 1976. Т. 7. С. 402.

користанням методів експертних оцінок[99]. Для кількісної оцінки потенціалу загрози ***(П)*** автором пропонується розглядати його як функцію комплексу з ***n*** параметрів a_i загрози:

$$П = f(a_1, a_2, \ldots, a_n).$$

Кожний з цих параметрів оцінюється експертами за однаковою бальною шкалою. Конкретний вид функції ***П*** може бути різним, але, коли важливість параметрів a_i є однаковою, потенціал загрози можна представити як середнє арифметичне їх бальних оцінок:

$$П = (a_1+a_2+ \ldots+a_n)/n.$$

У випадку коли важливість параметрів a_i є різною, використовується їх коефіцієнт значимості k_i. Тоді:

$$П= (k_1a_1 + k_2a_2+ \ldots + k_na_n),$$

причому $k_1 + k_2 + \ldots + k_n = 1$.

Крім того, потрібно враховувати, що потенціал загрози як явища або події може змінюватися з часом ***t***, а тому у загальному вигляді він матиме такий вигляд:

$$П = f(a_1, a_2, \ldots, a_n; t).$$

Тим самим з'являється реальна можливість здійснювати прогнозування зміни потенціалу загрози у часі, а також прогнозування небезпеки від ураження нею об'єкта КІ. Слід підкреслити, що комплексна оцінка потенціалу загрози є однією з важливих характеристик небезпеки для об'єктів КІ від загрози.

[99]Сиденко В.М., Грошко И.М. Основы научных исследований. Харьков, 1970. 200 с.

4. ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Захист КІ включає систему скоординованих організаційних, нормативно-правових, адміністративних, пошукових, охоронних, режимних інженерно-технічних, наукових та інших заходів, матеріальних та нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки критичної інфраструктури.

Основною метою захисту КІ є забезпечення її стійкості та безпеки, локалізація загроз та створення спроможностей для швидкого відновлення функціонування.

Ще з початку 1990-х років дослідники з Європи та Америки в різних галузях науки, працюючи над проблематикою захисту критичної інфраструктури, зменшення ризиків та безпосередньо «мінімізації наслідків» (англ. to mitigate – пом'якшити, зменшити, послабити, нейтралізувати) від впливу загроз, розпочали досить активно досліджу-

вати таку категорію, як стійкість[100]. Згідно з словником Мерріам-Вебстер (англ., Merriam-Webster dictionary) стійкість (англ., resilience) визначено як «здатність відновлюватися або легко адаптуватися до небезпеки або зміни».

У нормативних актах різних держав та у працях дослідників існують визначення поняття «стійкість критичної інфраструктури» (англ., critical infrastructure resilience, CIR). Проаналізувавши їх, можемо зазначити, що більшість авторів під цим визначенням розуміють миттєве припинення або зниження можливостей виконання функцій об'єктами КІ та подальшу їх здатність адаптуватись до дії деструктивного фактору та відновити нормальну продуктивність.

Наразі відсутня однозначна позиція й з питання, чи є «стійкість» характеристикою якостей об'єкта, чи є відображенням безперервного процесу, що відбувається під час функціонування такого об'єкта критичної інфраструктури.

Зокрема, в деяких європейських актах під стійкістю об'єкта КІ розуміють процес, що характеризується підвищенням його спроможностей для мінімізації негативних наслідків деструктивного впливу та здатністю гарантувати

[100] Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. John D. Moteff, Specialist in Science and Technology Policy. August 23, 2012. Prepared for Members and Committees of Congress. URL: https://fas.org/sgp/crs/homesec/R42683.pdf.

надання основних функцій та послуг[101].

На відміну від європейського бачення, у США в Плані захисту національної інфраструктури стійкість об'єкта КІ визначено як «здатність чинити опір, поглинати, відновлюватися або успішно адаптуватися до несприятливих умов або зміни умов»[102]. Під зміною умов розуміють теракти, руйнування, техногенні та природні катастрофи. Ці різного роду загрози разом іменуються як «усі небезпечні події» (англ., «all-hazard events», events – події, прояви, наслідки) та є важливими елементами стратегії національної безпеки[103].

Несприятливі фактори, які актуалізують негативний вплив загроз на об’єкти КІ, в нашій державі вважається за доцільне іменувати терміном «негативні чинники».

Оскільки відсутній єдиний підхід до визначення поняття стійкості об’єкта КІ, немає і єдиного підходу до її оцінки. Так, наприклад, для оцінки стійкості береться такий показник, як час для відновлення нормального функціонування об’єкта КІ після дії на нього певної загрози (ураження). Тобто чим менший час відновлення об’єкта КІ, тим більшою є його стійкість до впливу загрози. Для оцін-

[101] http://resilens.eu/about-resilience/critical-infrastructure-resilience.

[102] Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency. 2009. P. 111.

[103] Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. John D. Moteff, Specialist in Science and Technology Policy. August 23, 2012. Prepared for Members and Committees of Congress. URL: https://fas.org/sgp/crs/homesec/R42683.pdf.

ки стійкості об’єкта КІ використовується також такий показник, як втрата продуктивності. Зниження втрати продуктивності підвищує стійкість об’єкта КІ до впливу загроз.

За рахунок підвищення стійкості об’єкта КІ можна досягти зменшення ризику його ураження. Підвищення його стійкості досягається різними шляхами, в тому числі через вжиті запобіжні заходи з недопущення впливу загроз, від створення допоміжних систем, додаткових та резервних маршрутів, використання стійких матеріалів до певного виду актуальних загроз (наприклад у будівництві, стійких матеріалів до землетрусів чи повеней), створення умов для взаємозамінності імпортерів продукції та самої продукції і послуг, а також започаткування виробництва критичних імпортозамінних товарів, збільшення запасів критичної продукції тощо.

Водночас цікавим є той факт, що загалом стійкість критичної інфраструктури та її об’єктів в деяких державах розглядається не окремо, а як одна зі складових забезпечення безпеки регіону або держави в цілому. Крім того, забезпечення стійкості також включає не лише спеціально вжиті заходи, а розглядається як інтегрований елемент поведінки людей та соціально-економічних відносин у суспільстві, тобто регулюється не лише нормами права, а і нормами моралі у суспільстві.

Забезпечення стійкості об’єктів КІ досягається не тільки спеціальними заходами, а включає також підвищен-

ня інформованості персоналу об’єктів КІ та населення щодо можливих загроз і наслідків від них, навчання персоналу об’єктів КІ та постійного його тренування, розробки рекомендацій, процедур та правил поведінки працівників об’єкта КІ при впливі загроз для мінімізації можливих збитків, а також координацію дій уповноважених працівників державних органів влади та спеціальних служб і порядок їх взаємодії. Важливе значення приділяється заходам з підвищення інформованості населення щодо захисту об’єктів КІ, залучення його до участі з попередження та ліквідації наслідків ураження об’єктів КІ за встановленими правилами. Такі заходи розглядаються як важливий інструмент з формування поведінки окремих груп людей та суспільства у цілому при виникненні загроз критичній інфраструктурі держави та є запорукою формування ефективних соціально-економічних відносини.

Враховуючи вищевикладене, вбачається за доцільне під поняттям **«стійкість об’єкта критичної інфраструктури»** розуміти його здатність вжитими заходами забезпечувати протидію загрозам, мінімізувати наслідки їх впливу та негативних чинників, а також швидко відновлюватися.

Для операторів ідеальною моделлю забезпечення стійкості об'єктів КІ є така, коли навіть активна пряма дія різних загроз не заважає гарантуванню надання основних функцій та послуг, а відновлення основних функцій та послуг здійснюється у максимально стислий термін.

У вітчизняній літературі поняття «безпека» є достатньо дослідженим та визначеним, у тому числі й у нормативних актах. Над згаданою проблематикою працювали В. Горбулін, М. Галамба, М. Стрельбицький, О. Юрченко, В. Петров, В. Панченко, О. Суходоля, С. Горбатюк, П. Скурський та багато інших вчених, які досліджували її різні аспекти. Частина їх наукових доробків лягла в основу визначень у чинному законодавстві України.

Згідно з положеннями Закону України «Про національну безпеку» державна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру. Відповідне визначення існує і у сфері захисту КІ від кіберзагроз. Так, у Законі України «Про основні засади забезпечення кібербезпеки України» кібербезпека виражається захищеністю життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Антитерористична безпека передбачає використання всіх необхідних методів і засобів, якими можна було б мінімізувати або виключити можливість вчинення терактів. На

переконання автора, **безпека критичної інфраструктури** (англ. *safety*) є станом захищеності критичної інфраструктури від дії зовнішніх та внутрішніх чинників, що забезпечує її стабільне функціонування. Таке поняття є досить подібним до визначення науковців НІСД, які розглядають його як стан критичної інфраструктури, коли дія зовнішніх та внутрішніх чинників не призводить до аварій чи інших порушень її функціонування.

На думку провідних вчених, котрі займаються науковим аналізом системи захисту КІ в Україні, вона має будуватись за такими двома напрямами:

•аналіз ризиків, рівня загроз і вразливості КІ;

•реагування на можливе припинення критичною інфраструктурою виконання своїх функцій[104].

Для розуміння зазначених декларативних положень пропонується розглянути безпосередньо основні складові організації ЗКІ, провести їх аналіз і на основі порівняння з європейським досвідом запропонувати характерний для вітчизняної практики підхід щодо побудови вказаної системи.

На віднесення об’єктів національної інфраструктури до критичної значно впливають функції та послуги, якими вони забезпечують людину, суспільство, бізнес і державу.

[104] Суходоля О.М. Проблеми захисту енергетичної інфраструктури в умовах гібридної війни: аналіт. зап. URL: http://www.niss.gov.ua/articles/1891.

Зазначимо, що у провідних країнах світу до критичної інфраструктури відносять об’єкти за різними ознаками, проте за основу, як правило, береться *ризик настання негативних наслідків від їх ураження загрозами* (далі – **ризик**). На основі визначення (оцінки) ризику відбувається *формування переліку об'єктів КІ*.

Існує чимало підходів до розуміння змісту та визначення поняття «ризики».

З приводу класифікації ризиків досить цікавою та такою, що заслуговує на увагу, є позиція чеського вченого з Остравського університету М. Сметани. Він визначає поняття «глобальні ризики», що в інтерпретованому нами розумінні полягають у ймовірності настання глобальних наслідків, тобто таких, які мають широке географічне поширення, впливають на стан економіки та соціальну безпеку. З точки зору держави М. Сметана поділяє ризики на такі три основні групи: ті, яких можна уникнути (наприклад, пожежа); стратегічні ризики (виникають внаслідок помилкової оцінки ситуації та негативних наслідків управлінського впливу); зовнішні ризики (які не є підконтрольними державі чи окремому оператору).

Водночас ризики можуть бути відомі та невідомі (так званий Х-фактор), можуть визначатись залежно від їх розміру та ймовірності.

Основні документи ЄС щодо протидії загрозам критичній інфраструктурі загалом під *ризиками* розглядають

можливість втрати, травми або пошкодження об'єкта критичної інфраструктури[105].

У країнах ЄС рівень ризику для об'єкта КІ, як правило, формують такі складові, як можливість ураження певним типом загроз недостатньо захищених ділянок, а також вартісні наслідки від цього. Він може мати вираження у людських жертвах чи травмах, пошкодженнях, матеріальних збитках, завданні шкоди державній (національній) безпеці та дестабілізаційних процесах у суспільстві.

Деякі з європейських держав ознакою ризику для об'єкта КІ вважають масштаби небезпеки. Так, у Німеччині під *ризиком* розуміють можливість виникнення серйозної небезпеки для життя та здоров'я людей, економіки держави та сфери послуг, що може спричинити загрозу навколишньому середовищу і культурним та матеріальним цінностям[106].

В Європі багато в чому запозичили значення цієї категорії з нормативно-правових актів США, де під *ризиком* вбачається потенціал для небажаного результату внаслідок

[105] Повідомлення Комісії Раді та Європейському Парламенту від 20 жовтня 2004 року «Запобігання, готовність та реагування на терористичні напади» / COM (2004) 698 final – Official Journal від 20.01.2005. URL: https://eur-lex.europa.eu/legal-content/GA/TXT; URL: https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf. Зелена книга ЄС.

[106] Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий / Bundesministerium des Innern, 2006. URL: https://www.bmi.bund.de.

інциденту чи події, що визначається його вірогідністю та пов'язаними з нею наслідками[107].

З урахуванням міжнародних підходів до розуміння суті згаданої категорії понять для вітчизняного законодавства доцільно запропонувати визначити поняття **«ризик»** для об’єкта КІ як ймовірність настання максимально негативного наслідку від впливу загроз на цей об’єкт. Таке визначення ризику кореспондується з європейським законодавством у сфері захисту КІ та сприятиме адаптації вітчизняного законодавства до відповідних нормативних положень провідних держав.

В Україні визначення «ризику» доцільно здійснювати на підставі оцінки наявних або потенційних загроз та аналізу їх впливу на об'єкт національної інфраструктури з урахуванням його характеристик, проектної документації, технологічних регламентів та інших документів, пов'язаних з його функціями та експлуатацією. Така оцінка повинна бути проведена згідно з процедурою, затвердженою відповідними нормативно-правовими актами. Завдання щодо оцінки ризику від ураження загрозами об’єкту національної інфраструктури та його подальшої категоризації доцільно покласти на власників (розпорядників) об’єктів критичної інфраструктури на підставі письмового звернення уповноважених органів у сфері ЗКІ. За наказом вла-

[107] National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication.

сника (розпорядника) об'єкта, що може бути віднесений до КІ, утворюється відповідна комісія, до складу якої мають бути включені представники цього об'єкта, органу, у сфері управління якого він знаходиться (у разі наявності такого), СБ України та органів державної влади і місцевого самоврядування (далі – Комісія). Комісія визначає доцільність віднесення об'єкта національної інфраструктури до критичної та готує матеріали для його категоризації з метою визначення необхідного рівня захисту. Для цього Комісія повинна керуватись певними критеріями класифікації об’єктів, що мають затверджуватися відповідними нормативно-правовими актами.

У свою чергу, операторам КІ поряд з особою, яка відповідає за забезпечення безпеки, доцільно вводити посаду *відповідального на об’єкті КІ за визначення ризиків*. Саме вони у взаємодії з зацікавленими державними та від приватного сектору уповноваженими представниками спільно визначають ризики настання негативних наслідків від ураження загрозами об’єктів КІ, обґрунтовують необхідність належного захисту їх об'єкта органами у сфері ЗКІ та місцевою владою, а також розробляють концепцію ризик-менеджменту.

Шкала оцінювання ризику має містити градацію на «високий – середній – низький – вкрай низький – відсутній». Також доцільно проводити розробки відповідних програм для візуалізації із застосуванням графічного зо-

браження та кольорового наповнення змісту.

Саме оцінка ризиків дозволяє здійснювати завчасну та ефективну протидію притаманним для певного об'єкта КІ загрозам та забезпечити стабільне функціонування цього об’єкта із залученням оптимальних сил та засобів.

Ризик визначається щодо всіх об'єктів національної інфраструктури, які підлягають віднесенню до КІ. У подальшому він періодично оцінюється для об'єктів критичної інфраструктури з обов'язковим урахуванням потенціалу загроз та вжитих заходів з їх нейтралізації. Ризики визначаються на середньостроковий термін (5 років), але кожного року можуть уточнюватися залежно від зміни безпекової обстановки та запровадження нових заходів із захисту об’єктів КІ.

На зменшення ризику від впливу загроз прямо впливає підвищення стійкості, зменшення уразливості, планування на випадок надзвичайних ситуацій тощо. Їх комплексним показником, що включає всі ці та інші важливі компоненти, доцільно вважати *стан захисту* ***(С)***.

Важливість об'єкта ***(В)*** є показником, що характеризує значення цього об'єкта для отримання споживачами певних послуг чи функцій. Цей показник характеризує значення об'єкта і для життєзабезпечення, самоідентифікації, забезпечення необхідних духовних та культурних потреб населення. Він прямо впливає на негативні наслідки, адже включає і оцінку масштабності небезпеки від збоїв у

сталому функціонуванні об'єкта, і аналіз наявних на ньому небезпечних речовин (приклад: від вибухів чи аварій на підприємстві, де зберігається значна кількість твердого ракетного палива, є ймовірною значна зона забруднення території) тощо.

Враховуючи, що у практиці провідних світових держав існують різні підходи до визначення та обчислення ризиків настання негативних наслідків від ураження об'єктів національної інфраструктури та критичної інфраструктури (ризик – ***Р***), ми, доопрацювавши їх, спробуємо сформулювати власне його бачення. Ризик буде залежати від таких факторів, як стан захисту об'єкту ***(С)*** від певної загрози, з урахуванням раніше згадуваного потенціалу загрози ***(П)*** та тривалості її дії, прогнозованого терміну відновлення функціонування об'єкта КІ ***(Т),*** важливості об'єкта ***(В)*** для певного типу суб'єктів (держави, суспільства, бізнесу). Тоді у загальному вигляді ризик визначатиметься таким чином:

$$P = f(П, В, С, Т).$$

Кожна з цих складових ризику може бути оцінена експертами за відповідною бальною шкалою з використанням методів експертних оцінок, згаданих вище. У найпростішому варіанті з урахуванням коефіцієнтів значимості b_i функція ***Р*** має такий вигляд:

$$P = b_1П + b_2В + b_3С + b_4Т,$$

де $b_1 + b_2 + b_3 + b_4 = 1$.

Водночас в європейській практиці досить поширеною позицією щодо кількісного визначення ризику є така, в якій він виступає добутком розміру шкоди на ймовірність ураження.

Для якісної оцінки ризику деякі науковці використовують систему (групу) показників, наприклад[108]:

- ефективність чогось;
- стабільність чогось;
- відсутність чогось;
- рівень чогось;
- якість чогось;
- стан чогось.

Якісна оцінка цих показників переводиться у кількісний вимір за бальною шкалою з визначенням способу присвоєння кожній оцінці певного балу: менший рівень – більший бал, або більший рівень – більший бал. Шкала якісного оцінювання ризику має містити градацію на «високий – середній – низький – вкрай низький – відсутній». Також доцільно проводити розробки відповідних програм для візуалізації із застосуванням графічного зображення та кольорового наповнення змісту. Кількісна та якісна оцінка ризиків для об'єктів передбачає запровадження уніфікованих алгоритмів, затверджених відповідними нормативними актами.

[108] Малышева М.А. Теория и методы современного государственного управления: учебно-метод. пособие. СПб., 2011. 280 с.

З метою аналізу ризиків на об'єкті КІ необхідно виявити та проаналізувати всі ризики залежно від визначених у відповідних актах загроз (як правило, визначаються органами державної безпеки та правоохоронними органами) та з додатковим урахуванням найбільш характерних з них, індивідуального характеру. Для подальшого недопущення настання негативних наслідків створюється система раннього виявлення та попередження ризиків. Вносяться корективи в політику підприємства щодо фінансування у безпеку. Для цього розробляються проекти щодо переваг від належного захисту об'єкта КІ в умовах конкуренції.

Зазначені підходи до визначення ризиків для об’єктів критичної інфраструктури передбачають також проведення прогнозування ризиків, що полягає у здійсненні ймовірної оцінки динаміки зміни ризику у часі та очікуваних наслідків від ураження об’єкта КІ загрозами у майбутньому, а також оцінки потрібних ресурсів та необхідних організаційних заходів. Такі прогнози складаються на строк, визначений розпорядчими документами.

Існують різні методи прогнозування, які можна поділити на такі основні, як методи екстраполяції, методи експертних оцінок та методи моделювання[109]. Моделювання передбачає створення моделі об’єкта КІ з включенням моделей її складових критичних елементів, систем або ком-

[109] Сиденко В.М., Грошко И.М. Основы научных исследований. Харьков, 1970. 200 с.

плексів. Такі моделі (фізичні або математичні) повинні відображати основні властивості об'єкта та їх складових частин, опис основних процесів їх функціонування, а також моделі загроз та їх вплив на об'єкт КІ. Крім того, методи моделювання є одним з ефективних інструментів проведення аналізу ризиків, що дозволяє заздалегідь оцінити настання можливих загроз та їх вплив на об'єкт критичної інфраструктури, виявити слабкі місця у системах захисту об'єктів КІ та розробити заходи з їх нейтралізації. Враховуючи такі можливості, законодавство деяких країн навіть встановлює вимоги обов'язкового застосування методів моделювання, імітації і аналізу систем, що входять до складу критичної інфраструктури, особливо кіберінфраструктури, телекомунікаційної і фізичної інфраструктури, в цілях «підвищення розуміння великомасштабної складності таких систем і полегшення видозміни таких систем, щоб зменшити загрози для таких систем і критичних інфраструктур в цілому»[110].

У процесі визначення ризиків вагому роль відіграє дослідження уразливостей до кожного типу негативних чинників, зони можливого ураження, кількості ймовірних постраждалих, затрат, необхідних для відновлення функціонування об'єктів, видів загроз, ступеня поширення та інтенсивності кожної з них, стану основних виробничих фон-

[110] Public Law 107-56-Oct. 26, 2001. Critical Infrastructure Protection Act of 2001. 42 USC 5195c. URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56.

дів об'єктів КІ тощо.

Роль однієї з основних складових при оцінці ризиків відіграє *оцінка уразливостей* об'єктів КІ.

В актах Міністерства внутрішньої безпеки США, що є ініціатором глобалізації процесів ЗКІ у Європі та світі, під *уразливістю* об'єкта КІ розуміється здатність бути підданим нападу або травмованому, умисно чи випадково, обґрунтовано чи безпідставно[111].

Оцінка уразливостей (англ., vulnerability assessments) є одним з першочергових заходів із захисту об'єктів КІ та має на меті надати реальну характеристику стану їх захищеності, щоб максимально знизити ризики настання негативних наслідків. Це більшою мірою є задачею самих операторів. Представники державних органів у цьому процесі, як правило, забезпечують сприяння, надають методичні рекомендації та здійснюють контроль дій операторів. Оцінка уразливостей може проводитись у формі таких заходів:

– відвідування об'єктів для надання консультацій (включає: удосконалення заходів з координації дій із органом щодо ЗКІ; надання консультацій стосовно загальних питань щодо захисту КІ; забезпечення процесу огляду та аналізу існуючих компонентів та організації їх захисту; вивчення стану налагодження взаємодії з місцевою владою; часто супроводжуються перевіркою безпеки);

– перевірка безпеки (добровільний огляд стану захи-

[111] https://www.dhs.gov/critical-infrastructure-vulnerability-assessments.

щеності, який проводиться спеціалістами з безпеки органу із ЗКІ у взаємодії з операторами з метою визначення реального стану захищеності об'єктів та наявних недоліків, заходів для забезпечення безпеки і стійкості, сил і засобів, які для цього використовуються, управлінської діяльності у цій сфері, стану обміну інформацією; за результатами перевірки оператору надається підготовлений за бальною шкалою результат про уразливі місця (враховується узагальнена оцінка подібних об'єктів) та необхідні заходи реагування);

– візуалізація об'єктів КІ (використовується для покращення управлінського процесу, швидкої та об'єктивної оцінки ймовірних загроз і прийняття рішення, надає користувачеві інтегровані зображення об'єктів зовні та зсередини, прилеглих районів, під'їзних шляхів до них, супутникові дані тощо). До проведення цих заходів та збереження інформації залучаються правоохоронні органи та спецслужби.

Підготовка спеціалістів у сфері безпеки полягає у тому, що для ефективної оцінки уразливості всієї КІ залучаються спеціалісти, які отримують спеціальну підготовку органом, уповноваженим на здійснення ЗКІ (наприклад, у США це консультанти з безпеки (англ., Protective Security Advisors, PSAs), підготовку яких здійснює спецслужба DHS).

Разом з оцінкою уразливостей відбувається спільна

оцінка стійкості об'єктів КІ регіону, що супроводжується залученням уповноваженим органом на здійснення ЗКІ партнерів з місцевої та державної влади до цих заходів на їх території. Метою цієї діяльності є поглиблення розуміння та підвищення взаємодії учасників для підняття рівня захисту об'єктів КІ. Результати взаємодії відображаються у відповідних звітах з оцінки стійкості. Висновки щодо підвищення стійкості об'єктів КІ служать своєрідною основою для подальших заходів щодо їх захисту. У висновках та оцінках стійкості об'єктів КІ можуть міститись конкретні пропозиції щодо придбання засобів та вжиття конкретних заходів, удосконалення управлінської діяльності із захисту об'єктів КІ, навчання персоналу тощо.

Якість, достовірність та об'єктивність вищезазначених висновків багато в чому залежить від ефективності такої співпраці між партнерами, в тому числі з державного і приватного сектору[112].

Таким чином, уразливість, як і стійкість, об'єкта КІ залежить від типу наявних загроз їх потенціалу і вжитих заходів влади та операторів у сфері ЗКІ з підняття рівня захищеності такого об'єкта.

Враховуючи викладене, *уразливість об'єкта КІ від дії загроз* (далі – **уразливість)** пропонуємо вважати показником, що характеризує можливість завдання об'єкту КІ пошкоджень від дії загроз, різних засобів та чинників.

[112] https://www.dhs.gov/infrastructure-visualization-platform.

Важливо зважати на те, що у разі якщо загрози за характером походження є «навмисними діями», тобто спричинені людським фактором (наприклад, тероризм, кібератаки), то важливою складовою при виборі об'єктів ураження буде досягнення якомога більшої величини негативних наслідків.

Негативні наслідки від ураження об’єкта КІ (далі за текстом – **наслідки**, ***Н***) у контексті ЗКІ фактично є втратами.

Згідно зі словником української мови термін «наслідки» має значення: «те, що виходить, випливає з чого-небудь; результат»[113].

Основною *метою оцінки наслідків є визначення категорії об'єкта КІ, що у свою чергу дозволяє забезпечити необхідний рівень його захисту.* Вона визначається з урахуванням можливих масштабів втрат ***(М)*** та таких показників, як розмір людських втрат, економічних втрат, втрат безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку ***(В)***. Однією із найпростіших формул для її обчислення буде така:

$$\boldsymbol{H = M \times B}$$

У цій формулі чим більшою є величина ***(Н),*** тим більшого захисту потребує об'єкт КІ.

Таке обчислення є більш характерним для організації

[113] Словник української мови: академічний тлумачний словник (1970-1980): в 11 т. Том 5, 1974. С. 192.

захисту об'єктів від кіберзагроз, терористичних загроз та на даний час активно досліджується і впроваджується фахівцями АТЦ при СБ України.

Отже, визначення наслідків покладається в основу *віднесення об'єкта КІ до певної категорії.*

Аналіз вітчизняних нормативно-правових актів свідчить про те, що законодавець в Концепції створення державної системи захисту критичної інфраструктури започаткував перші кроки у зазначеному напрямку, виокремивши та визначивши зміст чотирьох категорій об'єктів КІ як: критично важливі, життєво важливі, важливі й необхідні, та закріпивши положення про те, що «для визначення необхідного рівня захисту об’єктів критичної інфраструктури, повноважень, завдань та відповідальності суб’єктів здійснюється категоризація об’єктів інфраструктури». Хоча вищеописаний автором можливий механізм ранжирування об'єктів наразі ще залишається нерозробленим.

У ряді європейських держав обов'язком об’єктів КІ є вжиття належних заходів для виявлення на ранній стадії загроз, недопущення ризиків від їх дії та подальшого постійного контролю за ними для забезпечення сталого функціонування об’єктів КІ, надання відповідних послуг та сприяння стабільності в регіоні та в цілому у державі. До таких несприятливих чинників, поряд із ризиковими операціями, порушеннями вимог законодавчих актів у сфері фінансово-господарської діяльності та вчиненням правопорушень, пе-

редбачених адміністративним чи кримінальним законодавством (охоплюються ризик-менеджментом), також включають загрози стихійних явищ, терактів, кіберінцидентів, шпигунства, конкурентної розвідки тощо, котрі можуть значно впливати на подальшу діяльність та навіть існування об'єкта.

Отже, запровадження системи захисту критичної інфраструктури передбачає цілий ряд необхідних заходів, обов'язкових для кожного об'єкта КІ, за таким алгоритмом:

– визначення виду притаманних загроз (стихійні явища, технічні поломки і недбалість персоналу, теракти, злочини тощо) та їх можливої інтенсивності;

– оцінка уразливих місць;

– аналіз стійкості;

– визначення ризиків;

– визначення категорії об'єкта, його рівня захисту (від наявних та потенційних загроз);

– прогнозування розвитку ситуації залежно від наслідків та загроз;

– формування мети захисту та визначення заходів, необхідних для її досягнення;

– реалізація заходів та спільних заходів держави і приватних партнерів;

– на основі аналізу та з урахуванням розвитку ситуації постійне внесення коректив у спільні дії та регулятивні нормативно-правові акти.

Зазначені заходи мають бути чітко визначені та передбачені як обов'язковий алгоритм дій для операторів КІ та інших учасників. Доцільно розглянути можливість закріплення подібного алгоритму, наприклад у *Вимогах щодо захисту об'єктів КІ* (далі – Вимоги). Ці Вимоги, у свою чергу, мають бути передбачені Програмою захисту та розроблятися органом у сфері захисту КІ, СБ України, зацікавленими відомствами та представниками приватного сектору.

Водночас ефективність заходів щодо захисту КІ покращується за умов застосовування ризик-менеджменту та планування розвитку господарської діяльності. Впровадження та злагодженість дій у зазначеному процесі зростає за умов належного законодавчого закріплення відповідних обов'язків всіх учасників процесу захисту КІ.

5. ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Позиція держав – лідерів ЄС за розвитком економіки та за можливістю впливати на геополітичну ситуацію у світі свідчить про усвідомлення ними прямої залежності національного благополуччя від безпечної та стійкої критичної інфраструктури за умов досить глибокої інтегрованої взаємодії державного та приватного сектору, їх партнерства, заснованого на двосторонній вигоді[114].

Партнерство починається з прямих вигод, пов'язаних з чітким та спільним інтересом у забезпеченні безпеки та стійкості критичної інфраструктури нації.

У контексті цього **«партнерство»** визначається як тісна співпраця між сторонами, які мають спільні інтереси у досягненні єдиної мети. З огляду на різні завдання, ролі та відповідальність партнерів у сфері функціонування крити-

[114] Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав // Актуальні проблеми вдосконалення чинного законодавства України. Івано-Франківськ, 2017. № XLIV. С. 224-235; Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США // Науковий вісник ДДУВС. 2017. № 3. С. 135-140.

чної інфраструктури необхідними є гнучкі, активні та всеохоплюючі партнерські стосунки, спрямовані на підвищення надійності та стійкості критичної інфраструктури.

Директивою ЄС від 08.12.2008 № 114 «Про визначення та зміст європейської критичної інфраструктури та про оцінку необхідності підвищення рівня її захисту» закладено основи для реалізації політики щодо заохочення повноцінної участі приватного сектору у захисті критичної інфраструктури. На думку авторів документа, вказані норми обумовлені значною участю приватного сектору у здійсненні оцінки ризиків, плануванні безперервності процесів надання послуг та швидкого відновлення функціонування після ураження загрозами[115].

Згідно із зазначеною директивою на національних рівнях у різних країнах відповідні норми закріплюються переважно у стратегіях національної безпеки, стратегіях захисту різних сфер та інших базових розпорядчих актах, що стосуються функціонування критичної інфраструктури, зокрема і в планах її захисту.

Посиленню партнерства та формуванню злагоджених дій на європейському просторі між учасниками від держави й приватного сектору, а також міждержавного характеру сприяла «Попереджувальна інформаційна мережа кри-

[115] Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/114/EC).

тичної інфраструктури» (CIWIN). Це захищена, інформаційна, комунікаційна і попереджувальна система для обміну інформацією між членами ЄС про спільні загрози, ризики, уразливість та відповідні заходи зі зменшення ризиків. Для цього в державах – членах ЄС створено конкретні контактні місця. За їх допомогою існує можливість на форумі обмінюватись інформацією щодо захисту критичної інфраструктури. Також наявною є функція своєчасного попередження учасників про загрози. Окрім уповноважених державних службовців доступ до системи мають оператори критичної інфраструктури[116].

У Німеччині основні положення щодо доцільності зміцнення державно-приватного партнерства при ЗКІ закріплені у Стратегії кібербезпеки від 2011 р. та Концепції основних заходів захисту критичної інфраструктури від 2006 р. З метою поглиблення державно-приватної співпраці та підтримки надання послуг операторами критичної інфраструктури (KRITIS) між ними, їх асоціаціями та відповідними державними установами, такими як Федеральне відомство інформаційної безпеки (BSI), у більшості секторів критичної інфраструктури запроваджено взаємодію UP KRITIS (державно-приватне партнерство). Іншим прикла-

[116] Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: ВШБ – Технический университет Острава, 2014/2015. 60 с. (текст для курсов, подготавливаемых в рамках сотрудничества Чешская республика – Молдавия).

дом державно-приватного партнерства у сфері захисту КІ є CERT-Verbund – групи безпеки і команди реагування на комп'ютерні інциденти (CERT) сприяють обміну інформацією (наприклад, про уразливість або інциденти) та співпраці щодо усунення загроз. Співпраця з ними базується на угодах про нерозголошення інформації та на кодексі поведінки.

Для власників та керівників підприємств з числа об'єктів КІ передбачено економічне обґрунтування щодо забезпечення безпеки. В обґрунтуванні серед переваг для операторів критичної інфраструктури зазначено: збільшення доходів; спрощення обмежень; захист сегмента ринку; ризик-менеджмент; захист технологій та товарних знаків.

У Великобританії основи взаємодії державного та приватного секторів закладені Стратегією національної безпеки, Антитерористичною стратегією, (CONTEST – Counter terrorism strategy), Стратегією захисту кіберпростору (Cyber Security Strategy), а також в урядовому Плані розвитку національної інфраструктури.

Розвитку державно-приватного партнерства активно сприяє Національний центр кібербезпеки (NCSC) як організація Великобританії, яка надає консультативну допомогу і підтримку державному і приватному секторам з питань протидії загрозам комп'ютерної безпеки. В центр включені експерти в галузі безпеки команди з реагування на комп'ю-

терні надзвичайні ситуації CERT-UK та MI-5, що діють з метою покращення кіберзахисту об'єктів КІ, мереж державного та приватного секторів, надання консультацій операторам та громадянам для функціонування і ведення бізнесу з використанням інформаційних мереж та Інтернету[117].

В Іспанії при Національному центрі розвідки (CNI) діють орган сертифікації безпеки інформаційних систем та національна комп'ютерна команда криптологічного центру реагування на комп'ютерні інциденти (CCN-CERT)[118]. Центр реагування на комп'ютерні інциденти (INCE) займається аналізом ризиків та загроз у кіберпросторі, їх прогнозом та організацією протидії.

Загалом, виникнення структури CERT тісно пов'язано з боротьбою проти комп'ютерних вірусів – так званих «мережевих черв'яків«. Для протидії першому виявленому комп'ютерному вірусу у 1988 році на замовлення уряду США в університеті Карнегі-Меллон була сформована «комп'ютерна команда екстреної готовності – computer emergency response team», або «CERT». Після цього створення подібних організацій розпочалось в усьому світі[119]. На відміну від США, на території Європейського союзу більшість груп CERT створювалися університетами і великими IT-компаніями. Загальноєвропейська організація носить назву «TF-CSIRT» (англ. Task force – collaboration

[117] https://www.ncsc.gov.uk/information/about-ncsc.
[118] https://es.wikipedia.org/wiki/Centro_Nacional_de_Inteligencia.
[119] https://www.incibe.es/que-es-incibe/como-trabajamos.

security incident response teams).

Досить активно співпраця в рамках державно-приватного партнерства розвивається і у сфері захисту критичної інфраструктури від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха тощо). Саме для цієї сфери характерною є можливість зростання негативних наслідків від порушення цілісності КІ у геометричній прогресії («каскадні ефекти»).

Тому у деяких країнах, наприклад у Данії, одним з основних координаторів роботи у сфері захисту критичної інфраструктури є Агентство з управління надзвичайними ситуаціями (DEMA). Саме цей орган і очолює контактну групу із захисту критичної інфраструктури, в межах якої організовано міжгалузеву співпрацю, включаючи приватний сектор. Законодавчою основою організації партнерства в Данії є Акт керування діями (Інструкція) у випадку надзвичайної ситуації (англ., the Emergency Management Act). Він визначається як план функціонування суспільства за незвичайних умов. Його основною метою є забезпечення впорядкованого та скоординованого використання ресурсів громадянського суспільства.

Поряд із захистом від кіберзагроз та загроз від надзвичайних ситуацій захист критичної інфраструктури передбачає і захист від загроз у сфері державної безпеки.

Девізом Федерального відомства Німеччини з охорони Конституції (BfV) у сфері захисту економіки є «запобі-

гання загрозам через діалог та обмін інформацією»[120]. Хоча захист КІ та нових розробок є обов'язком операторів, однак BfV надає рекомендації щодо захисту. Вони в першу чергу включають протидію розвіддіяльності, організованої спецслужбами іноземних держав, протидію іншим загрозам у цій сфері.

Обмін інформацією між BfV та бізнесом розпочато з 2008 року, цим займається підрозділ із захисту економіки (нім., Arbeitsgemeinschaft für Sicherheit der Wirtschaft). Крім того, у Німеччині діє цікавий механізм залучення до співпраці зі спецслужбою, і цей процес активно заохочує держава. Так, особам, які сприяють діяльності BfV, надається право платити знижену на 10 відсотків податкову ставку за своїми доходами.

Поряд з UP KRITIS в Німеччині існує спільна інтернет-платформа BSI та BBK (Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих) щодо захисту критичної інфраструктури[121].

У США, згідно з положеннями національного плану (англ., National Infrastructure Protection Plan, NIPP) в частині «Партнерство для забезпечення безпеки та стійкості критично важливої інфраструктури» передбачено необхідність учасників-партнерів колективно визначати націона-

[120] https://www.verfassungsschutz.de.

[121] Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. Bundesministerium des Innern, 2006. URL: www.bmi.bund.de.

льні пріоритети та формулювати чіткі заходи задля пом'якшення ризиків, прогнозувати та аналізувати прогрес і вигоду та відслідковувати зворотній зв'язок[122]. У свою чергу, національний план є формою організації національних зусиль, він сприяє прогресу на основі залучення широкого кола учасників-партнерів з різних рівнів урядової гілки влади, приватних та некомерційних секторів, у тому числі й громадянського суспільства, до розуміння важливості забезпечення безпеки і стійкості критично важливої інфраструктури. Крім того, він слугує консолідуючим фактором, оскільки використовує спільні структури та механізми, що полегшують обмін інформацією та вирішення спільних проблем.

Сьогодні одним з основних нормативно-правових актів, яким унормовано правові та організаційні засади взаємодії державних і приватних партнерів в Україні, є Закон України «Про державно-приватне партнерство України» (від 01.07.2010 № 2404-VI, далі – Закон). Законом сформовано поняття та ознаки державно-приватного партнерства, закріплено його основні принципи та форми, визначено основні сфери застосування державно-приватного партнерства та особливості договірно-правових відносин. Відповідно до статті 1 вказаного Закону державно-

[122] NIPP 2013 Partnering for Critical Infrastructure. Security and Resilience. URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

приватне партнерство – це співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів та органів місцевого самоврядування (державними партнерами) та юридичними особами, крім державних та комунальних підприємств, або фізичними особами-підприємцями (приватними партнерами), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами, та відповідає ознакам державно-приватного партнерства, визначеним цим Законом.

Основними ознаками ДПП відповідно до ст. 1 Закону є:

– надання прав управління (користування, експлуатації) об'єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта державно-приватного партнерства з подальшим управлінням (користуванням, експлуатацією), за умови прийняття та виконання приватним партнером інвестиційних зобов'язань відповідно до договору, укладеного в рамках державно-приватного партнерства;

- тривалість відносин (від 5 до 50 років);

- передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства;

- внесення приватним партнером інвестицій в об'єкти партнерства із джерел, не заборонених законодавством.

Закон України не встановлює вичерпного переліку

форм державно-приватного партнерства, а лише визначає, що основною формою ДПП є цивільно-правовий договір, зокрема про концесію; управління майном (виключно за умови передбачення у договорі, укладеному в рамках державно-приватного партнерства, інвестиційних зобов'язань приватного партнера); спільну діяльність та інші договори.

Поряд із вказаним Законом відносини у сфері державно-приватного партнерства регулюються законами України «Про концесії»[123] та «Про угоди про розподіл продукції»[124]. Відносини у сфері державно-приватного партнерства врегульовано також окремими підзаконними актами.

У контексті обміну інформацією між державними та приватними партнерами, що визначений одним із пріоритетних напрямів розвитку ДПП, слід згадати Постанову Кабінету Міністрів України «Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства».

Порядок визначає процедуру надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства у формі звіту, встановлює строки подання такої інформації у формі звіту та визначає уповноваженого

[123] Закон України "Про концесії" від 16.07.1999 № 997-XIV // ВВР України. 1999. № 41. Ст. 372.

[124] Закон України "Про угоди про розподіл продукції" від 14.09.1999 р. № 1039-XIV // ВВР України. 1999. № 44. Ст. 391.

суб'єкта, який проводить моніторинг, узагальнює та оприлюднює результати здійснення державно-приватного партнерства від імені державного партнера, яким є Мінекономрозвитку[125].

Ще одним нормативно-правовим актом, що регулює питання здійснення ДПП, є постанова Кабінету Міністрів України «Деякі питання організації здійснення державно-приватного партнерства», якою затверджено Порядок проведення конкурсу з визначення приватного партнера для здійснення державно-приватного партнерства щодо об'єктів державної, комунальної власності та об'єктів, які належать Автономній Республіці Крим, та Порядок проведення аналізу ефективності здійснення державно-приватного партнерства[126].

Незважаючи на широке закріплення напрямів державно-приватної взаємодії, реалізація її механізмів у сфері захисту критичної інфраструктури значно ускладняється. Стримуючим фактором для розвитку державно-приватного партнерства в Україні, на думку дослідників, є складність, багаторівневість і забюрократизованість нормативно-правової бази регулювання, що створює ризики для ефек-

[125] Постанова Кабінету Міністрів України "Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства" від 09.02.2011 № 81 // Офіційний вісник України. 2011. № 10. Ст. 458.

[126] Постанова Кабінету Міністрів України "Про деякі питання організації здійснення державно-приватного партнерства" від 11.04.2011 № 384 // Офіційний вісник України. 2011. № 28. Ст. 1168.

тивного використання цього механізму[127].

Разом з тим в Україні на загальнодержавному рівні за останній час прийнято низку документів стратегічного та доктринального характеру, що так чи інакше охоплюють питання захисту критичної інфраструктури. У цих документах приділено увагу розвитку як правового регулювання, так і державно-приватного партнерства у сфері захисту критичної інфраструктури.

Зокрема, в Стратегії національної безпеки України (п. 4.13) одним з основних пріоритетів забезпечення безпеки критичної інфраструктури визначено комплексне вдосконалення правової основи захисту критичної інфраструктури та створення системи державного управління її безпекою. Також пріоритетним визнано налагодження співробітництва між суб'єктами захисту критичної інфраструктури та розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них. Приділено увагу в Стратегії нацбезпеки і необхідності розробки та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту

[127] Щодо розвитку державно-приватного партнерства як механізму активізації інвестиційної діяльності в Україні: аналітична записка. URL: http://www.niss.gov.ua/articles/816.

чутливої інформації у цій сфері[128].

У контексті нашого дослідження слід згадати положення Стратегії кібербезпеки України. Відповідно до п. 1 Стратегії державно-приватне партнерство та широка співпраця з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту визнані одним із ключових принципів забезпечення кібербезпеки України. Пунктом 4.3 аналізованого документа закріплено, що кіберзахист критичної інфраструктури має полягати у налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури та розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період.

У Стратегії кібербезпеки України наголошується на необхідності створення умов «для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до

[128] Указ Президента України від 26 травня 2015 р. № 287/2015. "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. "Про Стратегію національної безпеки України".

вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту»[129].

Авторами Стратегії кібербезпеки України, як і Стратегії національної безпеки України наголошено на необхідності розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

Значну увагу до питань державно-приватного партнерства у сфері захисту КІ приділено в Концепції створення державної системи захисту критичної інфраструктури. По-перше, визнано, що нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури є однією із основних проблем, що потребує розв'язання. По-друге, закріплено, що здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури є одним із основних принципів. В межах створення державної системи захисту критичної інфраструктури на загальнодержавному рівні передбачено формування засад державно-приватного партнерства у сфері захисту критичної інфраструктури. Формування державно-приватного партнерства передбачено реалізовувати на ос-

[129] Указ Президента України про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016 // Офіційний вісник України від 29 березня 2016 року. Ст. 899.

нові взаємної довіри, обміну інформацією, створення стимулів для інвестування у здійснення заходів, спрямованих на захист критичної інфраструктури, запровадження уніфікованих підходів щодо вимог до підвищення рівня захисту.

Враховуючи викладене, можемо констатувати, що державно-приватне партнерство визначено досить важливим елементом захисту критичної інфраструктури та має стати взаємовигідним фактором, що сприятиме взаємним інтеграційним процесам.

Аналіз основних підходів щодо захисту критичної інфраструктури у світі дозволяє виділити декілька сфер, в яких, відповідно, доцільно розвивати партнерство. Поряд із захистом від кіберзагроз захист критичної інфраструктури передбачає і захист від загроз у сфері державної безпеки (протидія диверсіям, розвіддіяльності іноземних спецслужб, тероризму, економічній експансії, економічному та промисловому шпигунству, конкурентній розвідці), захист від внутрішніх загроз та фізичного знищення (хуліганство, підпали, загрози від діяльності організованих злочинних угруповань), захист від надзвичайних ситуацій.

У процесі партнерства держава має бути гарантом захисту та виступати в ролі посередника в інформаційних та комунікаційних процесах, при цьому приватний сектор володіє інформацією щодо актуальних ризиків та загроз їх функціонуванню, що при налагодженому процесі обміну дозволить державі застосовувати ефективні конкретні за-

ходи із захисту[130].

Детальні аспекти взаємодії між партнерами доцільно передбачити в рамках *національного плану захисту критичної інфраструктури*, де мають бути зазначені спільні державно-приватні інтереси у забезпеченні безпеки та стійкості критичної інфраструктури. Крім того, зазначений документ стане консолідуючим фактором, оскільки полегшить та скоординує обмін інформацією, вирішення спільних проблем, забезпечить ефективність роботи органів державної влади, органів безпеки та приватного сектору пліч-о-пліч для досягнення соціально-економічного процвітання нації[131].

На нашу думку, взаємна зацікавленість від партнерства держави та операторів критичної інфраструктури може полягати у такому:

– державні органи можуть надавати доступ до наявної своєчасної, достовірної та найбільш повної інформації про загрози та ризики;

– державні органи можуть надавати дані операторам

[130] Єрменчук О. П. Інформаційно-комунікаційна складова державно-приватного партнерства у захисті критичної інфраструктури як важливий елемент забезпечення державної безпеки // Актуальні проблеми управління інформаційною безпекою держави: IX Всеукраїнська науково-практична конференція (Київ, 30 березня 2018 р.). Київ, 2018. С. 68-70.

[131] Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав // Актуальні проблеми вдосконалення чинного законодавства України. 2017. № XLIV. С. 224-235.

критичної інфраструктури щодо різних варіацій загроз та ризиків та тенденцій розвитку ситуації у певному сегменті внутрішнього чи зовнішнього ринку;

– державні органи можуть надавати детальну інформацію щодо ризиків, чим забезпечують свій вклад у захист об'єктів КІ, що позначиться на інвестиціях в безпеку та стійкість з боку операторів;

– оператори критичної інфраструктури можуть отримувати достовірну інформацію про наявні та потенційні загрози і ризики для вжиття відповідних заходів з підвищення безпеки та стійкості, а також розраховувати на необхідні заходи підтримки відповідних органів та місцевої чи державної влади;

– оператори критичної інфраструктури можуть отримувати достовірну інформацію, важливу для вжиття заходів з покращення інвестиційної діяльності;

– оператори критичної інфраструктури можуть впливати на дієвість та ефективність планів державних органів із забезпечення безпеки та стійкості в їх сферах діяльності;

– оператори критичної інфраструктури, які займаються господарською діяльністю, за умов тісної взаємодії з державними органами у сфері захисту критичної інфраструктури можуть якісно організувати роботу та підвищити прибуток. У свою чергу, збільшення їх прибутку є прямо пропорційним вигоді держави зі сплати ними податку з прибутку.

ВИСНОВКИ

Вибір для України тієї чи іншої організаційної моделі захисту критичної інфраструктури свідчить про доцільність ретельного вивчення наявного зарубіжного досвіду та врахування національних особливостей державотворчих процесів.

Додаткової актуальності цій науковій проблемі надає нагальна необхідність подолання загрозливих явищ у соціально-економічній та інших сферах державного управління, а також створення умов для зростання якості життя громадян, рівня їх захищеності та росту промислового виробництва і новітніх технологій, удосконалення захисту економічного потенціалу держави в умовах гібридної війни, захисту суспільства від різних загроз.

Аналіз європейської практики ЗКІ свідчить, що кожна держава обирає власний шлях побудови системи ЗКІ, зважаючи на загальні світові безпекові тенденції та враховуючи відповідний національний досвід. Захист критичної інфраструктури включає систему скоординованих організаційних, нормативно-правових, адміністративних, пошукових, охоронних, режимних інженерно-технічних, наукових та інших заходів, матеріальних та нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки

критичної інфраструктури. Він усіляко має стимулюватися та підтримуватися різними державними механізмами.

Спільними притаманними рисами систем захисту КІ різних держав є такі:

1) кожна національна модель системи захисту КІ залежить від особливостей безпекової ситуації в державі, згідно з якою формується національне законодавство і політика у сфері національної безпеки;

2) важливе значення для побудови таких моделей відіграє практика застосування в національному законодавстві та сутність основоположних понять, таких як «національна інфраструктура», «критична інфраструктура», «об'єкти національної та критичної інфраструктури», «захист критичної інфраструктури», «безпека об'єкта критичної інфраструктури», «стійкість об'єкта критичної інфраструктури», «загрози», «потенціал загрози», «ризики», «уразливість об'єкта критичної інфраструктури», «важливість об'єкта» та «наслідки»;

3) система захисту КІ має багаторівневу структуру, яка базується на конституції держави і діяльності системи органів влади;

4) особливе значення для ефективності, повноти та дієвості конкретних заходів із захисту КІ відіграє стан державно-приватного партнерства;

5) важливе значення в діяльності системи захисту КІ відіграють координуючі та інформаційні центри, участь

спеціальних правоохоронних органів у захисті критичної інфраструктури;

6) ефективність функціонування та якість прийняття управлінських рішень із захисту КІ залежить від інформаційно-комунікаційної складової цієї системи.

Першопричиною та рушійним механізмом для розбудови системи захисту є необхідність створення можливостей протидії загрозам для КІ. Їх здатність уражати важливі елементи значно впливає на стан економічної безпеки держави та на суспільно-політичні аспекти, зумовлює виникнення складних процесів організаційно-безпекового характеру та залучення до них різних партнерів. Для подальшого злагодженого функціонування в нашій державі цієї системи наразі важливо визначити основні її елементи, їх сутність та зміст і вірно здійснити її побудову.

Принциповим для побудови національної системи захисту КІ є обґрунтування понять «національна інфраструктура» та «критична інфраструктура». Під національною інфраструктурою вбачається взаємопов'язана система державного управління та об'єктів інфраструктури, що є основою функціонування держави, її економіки та суспільства. Критична інфраструктура – це система надзвичайно важливих матеріальних та нематеріальних об’єктів національної інфраструктури (а також їх власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може

призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки. Важливо визначити поняття «об'єкт національної інфраструктури», що може об'єднувати в собі державні та приватні підприємства, організації й установи, а також їх власність і результати діяльності, що є складовими єдиного механізму функціонування держави її економіки та суспільства. Автором не випадково застосовується таке поняття, як власність та результати діяльності. Воно поєднує такі недостатньо вживані у вітчизняному законодавстві складові інфраструктури, як: системи та їх частини, мережі, ресурси, вузли тощо.

Аналіз змісту категорії «загрози» для об’єкта КІ дозволяє розуміти їх як наявні або потенційно можливі явища і чинники, що можуть завдати шкоди такому об’єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України. Доцільно здійснювати їх класифікацію: від характеру походження; мети дій, що їх спричиняють; ступеня поширення; розміру людських втрат та матеріальних збитків; втрат для безпеки життєдіяльності; суспільно-політичних та культурних; втрат для забезпечення державної безпеки та громадського порядку; обсягів ресурсів, необхідних для їх локалізації. Вид загроз та їх можлива інте-

нсивність враховується при визначенні критичності об'єкта для формування переліку об'єктів КІ.

Узагальнення досвіду провідних країн Європи дозволяє виділити основні три сфери, що підлягають захисту. Саме в кожній з цих ключових сфер, як правило, створюються та функціонують один чи декілька підрозділів, що здійснюють ЗКІ від загроз, зокрема:

– у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвіддіяльність іноземних спецслужб, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка). Вони можуть включати внутрішні загрози та фізичне знищення КІ (при хуліганстві, підпалах, діяльності організованих злочинних угруповань, дії чинника «внутрішнього порушника»);

– від кіберзагроз (інформаційні атаки, кібертероризм);

– від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха, пожежі, епідемії та пандемії, застосування засобів ураження або інші небезпечні події).

Разом з цим потрібно констатувати, що за останні кілька років особливо актуальними для України стають загрози у сфері державної безпеки. Серед них науковці виділяють: різке збільшення терористичних актів, розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих груп та осіб на економічний, науково-технічний і оборонний потенціал, диверсії та деструк-

тивну злочинну діяльність, намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації, тощо.

Попередження, своєчасне виявлення та припинення впливу цих загроз має сприяти більш плідній співпраці між операторами критичної інфраструктури, що є ціллю деструктивних устремлінь, та відповідними безпековими відомствами нашої держави. Протидія вищезазначеним загрозам входить до повноважень СБ України, розвідувальних та правоохоронних органів, підрозділів з надзвичайних ситуацій тощо, а тому вимагає підвищення продуктивності та удосконалення спільних дій партнерів у цьому напрямку. Саме побудова системи захисту КІ в Україні може відіграти роль рушійної сили у побудові нової системи безпеки та захисту державно-приватних інтересів, а також стати переломним етапом в ментальності пересічних громадян, у якій укорінилася недовіра до спецслужб та правоохоронців, породжена за радянських часів. Причинами цих позитивних зрушень можуть стати спільні заходи з оцінки ризиків та наслідків, забезпечення стійкості тощо.

З огляду на різні завдання, ролі та відповідальність партнерів у сфері функціонування критичної інфраструктури, необхідними є гнучкі, активні та всеохоплюючі партнерські стосунки, спрямовані на підвищення надійності та стійкості критичної інфраструктури. У процесі партнерства держава має бути гарантом захисту та виступати в ролі

посередника в інформаційних та комунікаційних процесах, при цьому приватний сектор володіє інформацією щодо актуальних ризиків та загроз їх функціонуванню, що при налагодженому процесі обміну дозволить державі застосовувати ефективні конкретні заходи із захисту.

Детальні аспекти взаємодії між партнерами доцільно передбачити в рамках національної Програми захисту критичної інфраструктури, де мають бути зазначені спільні державно-приватні інтереси у забезпеченні безпеки та стійкості критичної інфраструктури. Крім того, зазначений документ стане консолідуючим фактором, оскільки полегшить та скоординує обмін інформацією, вирішення спільних проблем, забезпечить ефективність роботи органів державної влади, органів безпеки та приватного сектору пліч-о-пліч для досягнення соціально-економічного процвітання нації.

Система захисту КІ повинна мати ієрархічну структуру і включати елементи системи управління й координації на різних рівнях. Такими рівням можуть бути:

1) міжнародний рівень, на якому здійснюється співпраця та координація міжнародної політики та заходів у сфері захисту КІ через спеціально створені та уповноважені органи;

2) національний (загальнодержавний) рівень, на якому здійснюється формування, координація та реалізація державної політики у сфері захисту КІ через Верховну Раду

України, Президента України, Кабінет Міністрів України, Раду національної безпеки та оборони;

3) галузевий (відомчий) рівень, на якому здійснюється координація та реалізація державної політики через центральні органи виконавчої влади та інші державні органи, які будуть визначені законом як суб'єкти у сфері захисту КІ;

4) місцевий рівень, на якому здійснюється координація спільних дій та реалізація державної політики у сфері захисту КІ через місцеві органи виконавчої влади, органи місцевого самоврядування та інші державні органи місцевого рівня;

5) об'єктовий рівень, на якому суб'єктами здійснюється реалізація державної політики у сфері захисту КІ.

Водночас модель захисту КІ може бути централізованою чи децентралізованою. Та чи інша її побудова впливає на повноваження залучених органів та потребує детального наукового і фахового аналізу, проведення конференцій та круглих столів за участю спеціалістів для подальшого обговорення та прийняття остаточного рішення.

Захист КІ може мати вигляд централізованої системи, з головним державним органом, який відповідає за забезпечення безпеки КІ. Інші відомства беруть участь у визначених заходах або консультують цей орган, але не мають визначального впливу на регулювання діяльності у цій сфері. Така система запроваджена, наприклад, у Великоб-

ританії та Іспанії, де діють спеціально створені центри CPNI та CNPIC відповідно. При цьому у Великобританії з метою посилення захисту критично важливих об'єктів у Інтернет-сфері і для протидії кіберзагрозам в 2016 р. створено NCSC. Водночас Центр також функціонує у складі органів, що входять до Об'єднаного розвідувального комітету. У Німеччині, хоч і не створено окремий орган щодо ЗКІ, проте всі відповідні основні підрозділи є централізовані та перебувають у межах одного відомства. Також структура організації державного управління у сфері ЗКІ може бути децентралізована, коли декілька різних відомств або координують діяльність із захисту, або несуть відповідальність за безпеку КІ спільно чи окремо, залежно від наявного виду загроз. В цьому випадку захист КІ перебуває у компетенції декількох органів державного управління, які здійснюють взаємодію через міжвідомчий комітет, секретаріат тощо. Така форма організації запроваджена, наприклад, у Франції (організацію захисту КІ здійснює SGDSN, важливі функції виконують CDSN та центри у складі МВС (CIC та COGIC), міністерства здійснюють практичне впровадження рішень щодо захисту КІ в сфері свого впливу) та Данії (DEMA відповідає за збереження та продовження важливих функцій держави та суспільства у разі аварій та катастроф; питання протидії кіберзагрозам, терактам та шпигунству покладені на спецслужби в складі МО та поліції).

Основний орган щодо ЗКІ в більшості європейських країн міститься у складі відомств, підпорядкованих уряду. Існує практика створення підрозділів із захисту КІ в складі органів державної безпеки, наприклад у Великобританії при MI-5. В Іспанії контроль за захистом критичної інфраструктури здійснює Державний секретар з питань безпеки, який контролює діяльність спецслужб. При цьому у переважній більшості випадків саме спецслужби координують заходи із захисту КІ від загроз безпекового характеру та кіберзагроз, наприклад: у Німеччині – BSI, BfV; Великобританії – GCHQ та MI-5; Данії – DDIS та DSIS тощо.

Зазвичай у країнах діють центри захисту від надзвичайних ситуацій, що протидіють загрозам від аварій, катастроф, стихійних лих. В деяких з них, наприклад у Данії, таке агентство (DEMA) є одним з основних органів у сфері захисту критичної інфраструктури, тобто при ньому знаходиться основний контактний центр щодо ЗКІ.

В Україні національна система державного управління у сфері захисту критичної інфраструктури може включати у ролі підсистем визначені законодавством: єдину державну систему цивільного захисту; єдину систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; державну систему фізичного захисту, національну систему кібербезпеки та нову національну систему захисту критичної інфраструктури (має містити повноваження щодо ЗКІ у сфері державної безпеки).

Стосовно загальної координації в Україні діяльності із ЗКІ урахування французького досвіду дозволяє запропонувати створення моделі децентралізованої системи ЗКІ з поєднанням президентської вертикалі, РНБО та урядових структур. Робочим координуючим державним органом управління у сфері захисту КІ, наприклад, може стати Державна комісія з питань безпеки критичної інфраструктури, створена при Кабінеті Міністрів України та очолювана Прем'єр-міністром, оскільки більшість сфер, що можна віднести до критичних, регулюються саме через органи виконавчої влади. До складу комісії доцільно включити зацікавлених керівників міністерств та відомств.

Раціональне поєднання різних взаємозв'язків між елементами національної системи захисту КІ передбачає створення й різних центрів аналізу загроз і ризиків КІ, ситуаційно-аналітичних центрів КІ, координаційних рад (груп) на різних рівнях державної системи управління у сфері захисту КІ. Враховуючи положення Закону України «Про Раду національної безпеки і оборони України», за рішенням РНБО України можуть утворюватися тимчасові міжвідомчі комісії, робочі та консультативні органи для опрацювання і комплексного вирішення проблем міжгалузевого характеру, забезпечення науково-аналітичного та прогнозного супроводження діяльності РНБО України. Саме тому можна розглянути варіанти утворення при РНБО України консультативного органу – Центру з аналі-

зу загроз та ризиків для КІ України із залученням до його діяльності (у різних формах співпраці) провідних фахівців державних органів влади, представників наукової спільноти, організацій та підприємств секторів безпеки КІ, або створення відповідного структурного підрозділу у складі Апарату Ради.

Аналіз європейської практики свідчить про доцільність посилення зв'язків між спецслужбами чи створення спільних комітетів з метою попередження, виявлення та припинення загроз від розвідувально-підривної діяльності іноземних спеціальних служб, диверсій і деструктивної та терористичної злочинної діяльності щодо об’єктів КІ. Основну роль при організації протидії загрозам внутрішнього характеру в європейських країнах відіграють контррозвідувальні органи, наприклад BfV, MI5, DSIS та інші. При них спеціально створені відповідні центри. Аналогом могло б стати створення в СБ України Центру протидії загрозам та ризикам критичній інфраструктурі у сфері державної безпеки.

Важлива роль також повинна бути відведена Національному інституту стратегічних досліджень, Статутом якого (затверджений Указом Президента України від 16 грудня 2002 року № 1158) визначено, що Інститут є базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента України, який готує та подає на розгляд Президентові України проекти програм-

них документів, експертиз нормативно-правових актів, аналітичних довідок та пропозицій щодо основних засад внутрішньої та зовнішньої політики, до яких повинні відноситися й засади державної політики у сфері захисту КІ.

Водночас досвід Великої Британії з побудови централізованої системи ЗКІ у сфері державної безпеки вказує на доцільність розгляду питання зі створення Національного центру захисту критичної інфраструктури. Центр міг би бути утворений як окремий орган або як структурна частина в межах діючого органу влади, який буде визначений відповідальним за координацію діяльності із захисту критичної інфраструктури. Це може бути як орган, підпорядкований Прем'єр-міністру чи РНБО, так і орган у складі СБ України (для прикладу, на базі підрозділів контррозвідувального захисту інтересів держави у сфері економічної безпеки тощо). Подібною є практика створення на базі MI-5 центру CPNI, який є основним державним органом, що надає консультації з питань безпеки національної інфраструктури підприємствам, установам та організаціям. Діяльність CPNI спрямована на забезпечення збереження основних послуг економіки Великобританії, формування напрямів діяльності якого може також здійснюватися за рахунок залучення до роботи з визначення загроз та організації протидії їм представників зацікавлених міністерств та відомств.

Координацію дій учасників та нормативне впрова-

дження рішень доцільно реалізовувати через нормативно-правові акти (рішення) РНБО, введені в дію Указом Президента, чи через акти КМ України стосовно діяльності об'єктів, які перебувають у сфері управління уряду.

Не менш важливим є питання організаційних механізмів функціонування вказаної системи.

Досить ефективним засобом організації захисту КІ є розробка та виконання відповідних програм (планів) захисту. Враховуючи зазначене, вважається за доцільне розглянути питання запровадження в Україні відповідної практики розробки Концепції захисту КІ і Концепції захисту секторів економіки України та відповідних програм на національному та регіональному рівнях. На об'єктах також мають створюватись відповідні програми захисту. СБ України доцільно розробляти Концепцію та програму контррозвідувального захисту КІ, що має містити й консолідовану позицію розвідорганів. Програми повинні бути зв'язані з механізмами державної підтримки та стимулювання розвитку економіки, а тому розроблятися у рамках відповідних державних цільових програм. Це сприятиме їх фінансовому забезпеченню.

Безпосередня діяльність учасників, що здійснюють захист об’єктів КІ, має базуватися на складній системі аналізу та визначення (оцінки) показників «загроз», «ризиків», «уразливості», «стійкості», «наслідків» тощо, що детально розглянуто в цьому дослідженні.

В Україні визначення ризиків настання негативних наслідків від ураження об’єктів національної інфраструктури та критичної інфраструктури загрозами доцільно здійснювати на підставі оцінки загроз і вивчення цих об'єктів та їх характеристик.

Ризик від ураження об’єкта КІ (ризик) – це ймовірність настання максимально негативного наслідку від впливу загроз на цей об’єкт. Він залежить від таких факторів, як стан захисту об’єкта від певної загрози, з урахуванням її потенціалу та тривалості дії, прогнозованого терміну відновлення функціонування об’єкту КІ, а також важливості об'єкта для певного типу суб’єктів (держави, суспільства, бізнесу). Формування переліку об'єктів КІ має здійснюватися на основі оцінки ризику.

Основною метою оцінки негативних наслідків від ураження об’єкта КІ (наслідків) є визначення категорії об'єкта КІ, що у свою чергу дозволяє попередити наявні чи потенційні загрози та забезпечити необхідний рівень захисту об'єкта. Їх обчислення пропонується здійснювати з урахуванням можливих масштабів втрат і таких показників, як розмір людських втрат, економічних втрат, втрат безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку.

Таким чином, негативні наслідки у контексті ЗКІ фактично є втратами.

Завдання щодо визначення ризику від ураження загро-

зами об'єкта, що може бути віднесений до критичної інфраструктури, та подальшої його категоризації для визначення необхідного рівня захисту також доцільно покласти на власників (розпорядників) об’єктів критичної інфраструктури на підставі письмового звернення уповноважених органів у сфері ЗКІ.

У свою чергу, на об'єктах КІ поряд з працівником, який відповідає за забезпечення безпеки, вважається раціональним вводити посаду відповідального на об’єкті КІ за визначення ризиків. Саме вони у взаємодії із зацікавленими державними та від приватного сектору уповноваженими представниками спільно визначають ризики, обґрунтовують необхідність належного захисту їх об'єкта.

Запровадження системи захисту критичної інфраструктури передбачає цілий ряд необхідних заходів, обов'язкових для кожного об'єкта КІ, за таким алгоритмом:

– визначення виду притаманних загроз (стихійні явища, технічні поломки і недбалість персоналу, теракти, злочини тощо) та їх можливої інтенсивності;

– оцінка уразливих місць;

– аналіз стійкості;

– визначення ризиків;

– визначення категорії об'єкта, його рівня захисту (від наявних та потенційних загроз);

– прогнозування розвитку ситуації залежно від нас-

лідків та загроз;

– формування мети захисту та визначення заходів, необхідних для її досягнення;

– реалізація заходів та спільних заходів держави і приватних партнерів;

– на основі аналізу та з урахуванням розвитку ситуації – постійне внесення коректив у спільні дії та регулятивні нормативно-правові акти.

Зазначені заходи мають бути чітко визначені та передбачені як обов'язковий алгоритм дій для операторів КІ та інших учасників. Доцільно розглянути можливість закріплення подібного алгоритму, наприклад у Вимогах щодо захисту об'єктів КІ. Ці Вимоги, у свою чергу, мають бути передбачені Програмою захисту та розроблятися органом у сфері захисту КІ, СБ України, зацікавленими відомствами та представниками приватного сектору.

Організація захисту КІ можлива лише завдяки комплексному підходу, поєднаному зі створенням належної нормативно-правової бази. Важливим етапом у цьому процесі є передбачена керівництвом держави та закріплена в Концепції створення державної системи захисту критичної інфраструктури та відповідному розпорядженні КМ України необхідність розробки Закону України «Про критичну інфраструктуру та її захист», що на даний час триває, а також внесення змін у цілий ряд чинних нормативних актів.

Завдяки вжиттю зазначених заходів вітчизняна система захисту КІ охоплюватиме національний, галузевий, місцевий, об’єктовий і міжнародний рівні та закладе основи нової безпекової політики й зміцнення держави, оскільки сприятиме залученню до захисту в рамках багаторівневого єдиного механізму не лише керівництва держави та відомств, а й органів влади на місцях та безпосередньо об'єктів захисту і партнерів з приватного сектору.

Література

1. BSI-Kritisverordnung (BSI-KritisV). 22.04.2016. URL: http://www.buzer.de.

2. Choate, Pat a Susan Walter. America in ruins: the decaying infrastructure. Durham, N.C.: Duke Press Paperbacks, 1981. ISBN 08-223-0554-2.

3. Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/114/EC).

4. Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress / John D. Moteff, Specialist in Science and Technology Policy. 2013. August, 23. Prepared for Members and Committees of Congress. URL: http://fas.org/sgp/crs/homesec/R42683.pdf.

5. Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency. 2009.

6. Evolutions of Infrastructure: 15,000 Years of History" by Demeter G. Fertis, Anna Fertis. Published by Vantage Press, 1998. ISBN 0533124956.

7. Hoffman F. Onnot-so-newwarfare: political war fare vs hybrid threats. URL: http://warontherocks.com.

8. Infrastructure for the 21st Century Framework for a Research Age. Washington: National Academies Press, 1987. ISBN 978-030-9078-146.

9. National Critical Infrastructure Security and Resilience Research and Development Plan. 2015. URL: http://www.dhs.gov/publication.

10. NIPP 2013 Partnering for Critical Infrastructure. Security and Resilience. URL: http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

11. Public Law 107-56. Oct. 26, 2001. Critical Infrastructure Protection Act of 2001. 42 USC 5195c. URL: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56.

12. Říha, Josef. Urbanismus a územní rozvoj ročník X číslo. 2007. № 4. URL: http://www.uur.cz/5-publikacni-cinnost-a-knihovna/casopis/2007-04/08_kriticka.pdf.

13. Směrnice Rady. 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

14. URL: http://brs.dk.

15. URL: http://brs.dk/eng/inspection/contingency_planning/Pages.

16. URL: http://en.digst.dk/about-us.

17. URL: http://es.wikipedia.org/wiki/Centro_Nacional_de_Inteligencia.

18. URL: http://eur-lex.europa.eu/legal-content/TXT-LEGISSUM:l33260 European Programme for Critical Infrastructure Protection.

19. URL: http://fe-ddis.dk.

20. URL: http://fe-ddis.dk/SiteCollectionDocuments//FE_Beretning_2015_2016_printvenlig.pdf.

21. URL: http://hakpaksak.wordpress.com/2008/09/22/the-

etymology-of-infrastructure-and-the-infrastructure-of-the-internet.

22. URL: http://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx.pol=Civil%20Protection&c1=Poland&c2=Germany.

23. URL: http://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx.

24. URL: http://portal.cor.europa.eu/divisionpowers/Pages/Comparer.aspx.Denmark.

25. URL: http://resilens.eu/about-resilience/critical-infrastructure-resilience.

26. URL: http://security.homeoffice.gov.uk.

27. URL: http://sicherheitswiki.org/wiki/Kritische_Infrastrukturen.

28. URL: http://uk.m.wikipedia.org/wiki/Кібервійна.

29. URL: http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

30. URL: http://www.bbk.bund.de.

31. URL: http://www.bmbf.de.

32. URL: http://www.bmbf.de/sicherheitsforschung-forschung-fuer-die-zivile-sicherheit-150.html.

33. URL: http://www.bmel.de.

34. URL: http://www.bmg.bund.de/EN/Ministerium/ministry_node.html.

35. URL: http://www.bmi.bund.de/DE/startseite/startseite-node.html.

36. URL: http://www.bmvi.de/DE/Home/home.html.
37. URL: http://www.bmwi.de.
38. URL: http://www.bundesfinanzministerium.de/Web/DE/Home/ home.html.
39. URL: http://www.bundesgesundheitsministerium.de.
40. URL: http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.
41. URL: http://www.cnpic.es.
42. URL: http://www.cpni.gov.uk/about-cpni.
43. URL: http://www.cpni.gov.uk/default.aspx.
44. URL: http://www.dhs.gov/critical-infrastructure-vulnerability-assessments.
45. URL: http://www.dhs.gov/infrastructure-visualization-platform.
46. URL: http://www.gchq.gov.uk/topics/our-history.
47. URL: http://www.gesetze-im-internet.de/thw-helfrg/BJN180990.html.
48. URL: http://www.gov.uk/government/organisations/cabinet-office.
49. URL: http://www.homeoffice.gov.uk.
50. URL: http://www.incibe.es/que-es-incibe/como-trabajamos.
51. URL: http://www.intelpage.info/comisaria-general-de-informacion.html.
52. URL: http://www.interieur.gouv.fr/Publications/Nos-infographies/Securite-des-biens-et-des-personnes/Mobilisation-de-l-Etat-en-temps-de-crise/Centre-interministeriel-de-crise-CIC.
53. URL: http://www.interior.gob.es.

54. URL: http://www.mi5.gov.uk/output/uk-home-page.html.

55. URL: http://www.ncsc.gov.uk/information/about-ncsc.

56. URL: http://www.parisinfo.com/musee-monument-paris/71397/Ministere-de-l-economie-de-l-industrie-et-de-l-emploi.

57. URL: http://www.pet.dk/English.aspx.

58. URL: http://www.pet.dk/English/About PET/PETs organisation.aspx.

59. URL: http://www.pet.dk/ForebyggendeAfdeling/media/Forebyggende Afdeling/RASKmarkedsfringsbrevpdf.ashx.

60. URL: http://www.proteccioncivil.es.

61. URL: http://www.sgdsn.gouv.fr.

62. URL: http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf.

63. URL: http://www.soca.gov.uk/index.html.

64. URL: http://www.ssi.gouv.fr.

65. URL: http://www.thw.de.

66. URL: http://www.trm.dk/da/ministeriet.

67. URL: http://www.verfassungsschutz.de.

68. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі // Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.

69. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави // Захист інформації. НАУ. 2017. Т. 19.

70. Єрменчук О.П. Інформаційно-комунікаційна складова державно-приватного партнерства у захисті критичної інфра-

структури як важливий елемент забезпечення державної безпеки // Актуальні проблеми управління інформаційною безпекою держави: IX Всеукраїнська науково-практична конференція: зб. тез наукових доповідей (Київ, 30 березня 2018 р.). Київ, 2018. С. 68-70.

71. Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США // Науковий вісник ДДУВС. Дніпро. 2017. № 3. С. 135-140.

72. Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав // Актуальні проблеми вдосконалення чинного законодавства України. Івано-Франківськ, 2017. № XLIV. С. 224-235.

73. Єрменчук О.П. Поняття «критична інфраструктура» // Інформаційна безпека людини, суспільства, держави. 2018. № 1 (23). С. 20-27.

74. Єрменчук О.П. Складові національної інфраструктури // Науковий вісник ДДУВС. 2017. № 4. С. 109-115.

75. Єрменчук О.П. Сутність та зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури // Бюлетень Міністерства юстиції України. 2017. № 11. С. 35-41.

76. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки): аналітична записка Національного інституту стратегічних досліджень. Березень 2017 р. URL: http://www.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf.

77. Закон Данії «Про надзвичайні ситуації» № 660 від

10.06.2009.

78. Запобігання, готовність та реагування на терористичні напади: повідомлення Комісії Ради та Європейському Парламенту від 20 жовтня 2004 року /COM (2004) 698 final – Official Journal від 20.01.2005. URL: http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0702.

79. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. Bundesministerium des Innern, 2006. URL: http://www.bmi.bund.de.

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

81. Магда Е. Гибридная агрессия России: уроки для Европы. К.: Каламар, 2017. 284 с.

82. Малышева М.А. Теория и методы современного государственного управления: учебно-метод. пособие. СПб.: Отдел оперативной полиграфии НИУ ВШЭ Санкт-Петербург, 2011. 280 с.

83. Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: ВШБ Технический университет Острава, 2014/2015. 60 с. (текст для курсов, подготавливаемых в рамках сотрудничества Чешская республика – Молдавия).

84. Про деякі питання організації здійснення державно-приватного партнерства: Постанова Кабінету Міністрів України

від 11.04.2011 № 384 // Офіційний вісник України. 2011. № 28. Ст. 1168.

85. Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства: Постанова Кабінету Міністрів України від 09.02.2011 № 81 // Офіційний вісник України. 2011. № 10. Ст. 458.

86. Про концесії: Закон України від 16.07.1999 № 97-XIV // Відомості Верховної Ради України. 1999. № 41. Ст. 372.

87. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016 // Офіційний Вісник України від 29 березня 2016 року. № 23. Ст. 899.

88. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015.

89. Про угоди про розподіл продукції: Закон України від 14.09.1999 № 1039-XIV // Відомості Верховної Ради України. 1999. № 44. Ст. 391.

90. Радаев Н. Оценка террористической угрозы для объекта / Н. Радаев, А. Бочков. URL: http://mx1.algoritm.org/arch/77/77_3.pdf.

91. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.

92. Сиденко В.М., Грошко И.М. Основы научных исследований. Харьков: Вища школа, 1970. 200 с.

93. Словник української мови в 11 т. / Академічний тлума-

чний словник (1970-1980). Том 5. К., 1974.

94. Словник української мови в 11 томах / Академічний тлумачний словник (1970-1980). Том 7. К., 1976.

95. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України // Стратегічні пріоритети. Серія: Політика. 2016. № 3 (40). С 65-67.

96. Суходоля О.М. Проблеми захисту енергетичної інфраструктури в умовах гібридної війни: аналіт. зап. URL: http://www.niss.gov.ua/articles/1891.

97. Трактаты о военном исскустве / Сунь-цзы, У-цзы / пер. с китайского; предисловие и коммент. Н.И. Конрада. М.: АСТ; СПб.: Terra Fantastica, 2010. 606 с.

98. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / Бык В.В., Климчук А.А., Панченко В.Н., Петров В.В. К.: Академпресс, 2013. 220 с.

99. Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С. Обеспечение безопасности критических инфраструктур в США (аналитический обзор) // Труды ИСА РАН. 2006. Том 27.

100. Щодо розвитку державно-приватного партнерства як механізму активізації інвестиційної діяльності в Україні: аналітична записка. URL: http://www.niss.gov.ua/articles/816.

Для нотаток

Наукове видання

Єрменчук Олександр Петрович

ОСНОВНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КРАЇНАХ ЄВРОПИ: ДОСВІД ДЛЯ УКРАЇНИ

Монографія

Редактор, оригінал-макет – А.*В. Самотуга*
Редактор *Н.Ю. Веріго*

Підп. до друку 21.09.2018 р. Формат 60х84/16. Друк трафаретний (RISO).
Папір офісний. Гарнітура Times. Ум.-друк. арк. 11,00. Обл.-вид. арк. 11,25.
Тираж 300 прим. Зам. № 06/18-м.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, тел. (056) 370-96-59
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018