means of law-enforcement bodies, and others.

A number of measures have been proposed on the normative and legal support of the activities of the National Police to improve the information and analytical activities of the National Police.

The best practices of the Department of Organizational and Analytical Support and Rapid Response of the National Defense Ministry in the Dnipropetrovsk Oblast concerning the collection, evaluation, analysis of information on the crime situation in the region, resonant criminal offenses, public security and order violations, other emergency events and responses to them have been analyzed. It is proposed to extend this practice to similar units of the National Police throughout Ukraine.

The experience of the information and analytical activity of the police of the EU and the USA has been analyzed and measures have been proposed to improve the mentioned activity in Ukraine.

***Keywords**: National Police, information and analytical support, reform of the Ministry of Internal Affairs of Ukraine.*

Єрменчук О.П. ©
кандидат юридичних наук
(Служба безпеки України)

DOI:10.31733/2078-3566-2018-3-40-46

ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРАВОВИЙ АНАЛІЗ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Здійснено аналіз європейського законодавства у сфері захисту критичної інфраструктури. Викладено основні вимоги до побудови державної системи управління такою системою. Визначено особливості її функціонування, структури, повноваження її суб'єктів управління та завдання цієї системи управління. Обгрунтовано понятійно-категорійний апарат у сфері захисту критичної інфраструктури України, зокрема: „захист критичної інфраструктури", "стійкість об'єкта критичної інфраструктури", "безпека критичної інфраструктури", "ризик", "уразливість об'єкта КІ", "наслідки".

***Ключові слова**: державна система управління у сфері захисту критичної інфраструктури України, національна інфраструктура, критична інфраструктура, захист критичної інфраструктури, стійкість об'єкта критичної інфраструктури, безпека критичної інфраструктури, ризик, уразливість об'єкта КІ, наслідки.*

Постановка проблеми. Кожна національна модель системи захисту критичної інфраструктури в країнах Європи залежить від особливостей безпекової ситуації в державі, згідно з якою формується національне законодавство і політика у сфері національної безпеки.

Бажання належним чином відстояти національні інтереси та при цьому продовжувати вигідний для України рух у військову та політико-економічну співдружність повноцінних гравців європейського простору зумовлюють і необхідність раціонального системного підходу до побудови належної системи захисту об'єктів критичної інфраструктури (далі – КІ).

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Окремі питання, пов'язані із захистом критичної інфраструктури, були порушені в наукових працях Бірюкова Д.С., Брежнєва Є.В., Бобро Д.Г., Величка О.Ф., Дубова Д.В., Горбуліна В.П., Зубарєва В.В. Конах В.К., Кондратова С.І., Мірошника М.В., Насвіт О.І., Ожевана М.А., Панченко В.М., Петрова В.В., Рижова І.М., Скурського П.П., Суходолі О.М., Щербини В.М., Юрченка О.М., 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, що і зумовлює актуальність обраної для дослідження теми.

Виклад основного матеріалу. 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 за-

гроз 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, послабити, нейтралізувати) від впливу загроз, розпочали досить активно досліджувати таку категорію, як "стійкість" [1]. Згідно із словником Мерріам-Вебстер (англ., Merriam-Webster dictionary), стійкість (англ., resilience) визначено як "здатність відновлюватися або легко адаптуватися до небезпеки або зміни".

В нормативних актах різних держав та у працях дослідників існують визначення "стійкості критичної інфраструктури" (англ., critical infrastructure resilience, CIR). Більшість авторів під цим визначенням розуміють миттєве припинення або зниження можливостей виконання функцій об'єктами КІ та подальшу здатність їх адаптуватись до дії деструктивного фактора та відновлення нормальної продуктивності.

Наразі відсутня однозначна позиція і з того 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 надання основних функцій та послуг [2].

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" [3]. 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 [4].

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 більша його стійкість до впливу загрози. Для оцінки стійкості об’єкта КІ використовується також такий показник, як втрата його 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 по недопущенню 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 у деяких державах розглядається не окремо, а як одна із 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 підвищення інформованості персоналу об’єктів КІ та населення щодо можливих загроз та 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" достатньо досліджене та визначене, в 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, 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 та реагування на можливе припинення критичною інфраструктурою виконання своїх функцій [5].

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

На віднесення об'єктів національної інфраструктури до критичної інфраструктури значно впливають функції та послуги, якими вони забезпечують людину, суспільство, бізнес і державу. 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 тією, що заслуговує на увагу є позиція чеського вченого з Остравського університету М. Сметани. Він визначає "*глобальні ризики"*, що в інтерпретованому нами розумінні полягають у ймовірності настання глобальних наслідків, тобто таких, які мають географічне поширення, впливають на стан економіки та на 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 (ті, що не підконтрольні 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 [6; 7].

У країнах ЄС рівень ризику для об'єкта КІ, як правило, формують такі складові: 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, нанесенні шкоди державній (національній) безпеці та дестабілізаційних процесах в 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 та культурним і матеріальним цінностям [8].

В Європі багато в чому запозичили значення цієї категорії з нормативно-правових актів США, де під "ризиком" вбачається потенціал для небажаного результату внаслідок інциденту чи події, що визначається його вірогідністю та пов'язаними з нею наслідками [9].

З урахуванням міжнародних підходів до розуміння суті згаданої категорії понять, для вітчизняного законодавства доцільно запропонувати визначити *"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 терміна "ризик" 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 по оцінці ризику від ураження загрозами об'єкта 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 власника (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 та 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 із зацікавленими державними та від приватного сектора 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-менеджмента.

Шкала 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.

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. В 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 загроз прямо впливає підвищення стійкості, зменшення уразливості, планування на випадок надзвичайних ситуацій тощо. Їх комплексним показ-

ником, 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 формує (прямо впливає на) негативні наслідки, адже включає і оцінку масштабності небезпеки від збоїв у сталому функціонуванні об'єкта та аналіз наявних на ньому небезпечних речовин (приклад: від вибухів чи аварій на підприємстві, де зберігається значна кількість твердого ракетного палива, ймовірна 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 загрозами ("ризик" – *Р*), ми, доопрацювавши їх, спробуємо сформулювати власне його бачення. "Ризик" буде залежати від таких факторів як стан захисту об'єкта *(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 P 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 [10], наприклад: 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.

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, ступені поширення та інтенсивності кожної з них, стану основних виробничих фондів 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 [11].

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 формах відвідування об'єктів для надання консультацій, перевірки безпеки, візуалізації об'єктів КІ, підготовки спеціалістів у сфері безпеки тощо.

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 з їх захисту. У висновках та оцінках стійкості об'єктів КІ можуть міститись конкретні пропозиції з 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 сектора [12].

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 по підняттю рівня захищеності такого об'єкта.

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

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 по тексту – *"наслідки", Н*) у контексті ЗКІ фактично є втратами.

Згідно із словником української мови, термін "наслідки" має значення: "те, що виходить, випливає з чого-небудь; результат" [13].

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 таких, 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".

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 вчинення правопорушень, передбачених 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.

Як **висновки** можна зазначити, що 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 на потенційних загроз);
- прогнозування розвитку ситуації залежно від наслідків та загроз;
- формування мети захисту та визначення заходів, необхідних для її досягнення;
- реалізація спільних заходів держави та приватних партнерів;
- на основі аналізу та з урахуванням розвитку ситуації постійне внесення корективів 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, в свою чергу, мають бути передбачені Програмою захисту та мають розроблятися органом у сфері захисту КІ, СБ України, зацікавленими відомствами та представниками приватного сектора.

Водночас ефективність заходів по захисту КІ покращується за умов застосовування ризик-менеджмента 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.

Бібліографічні посилання

1. 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.
2. URL. http://resilens.eu/about-resilience/critical-infrastructure-resilience/.
3. Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency. 2009. P. 111.
4. 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.
5. Суходоля О. М. Проблеми захисту енергетичної інфраструктури в умовах гібридної війни: аналіт. зап. URL. http://www.niss.gov.ua/articles/1891/.
6. Повідомлення Комісії Раді та Європейському Парламенту від 20 жовтня 2004 року – Запобігання, готовність та реагування на терористичні напади [COM (2004) 698 final – Official Journal C 14 від 20.01.2005]. URL. https://eur-lex.europa.eu/legal-content/GA/TXT/.
7. Зелена книга ЄС. 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.
8. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. – Bundesministerium des Innern, 2006. URL. https://www.bmi.bund.de.
9. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL. https://www.dhs.gov/publication.
10. Малышева М.А. Теория и методы современного государственного управления: учебно-методическое пособие. СПб.: Отдел оперативной полиграфии НИУ ВШЭ - Санкт-Петербург, 2011. 280 с.
11. URL. https://www.dhs.gov/critical-infrastructure-vulnerability-assessments.
12. URL. https://www.dhs.gov/infrastructure-visualization-platform.
13. Словник української мови: в 11 томах. Т. 5, 1974. С. 192. Словник української мови Академічний тлумачний словник (1970–1980).

Надійшла до редакції 17.09.2018

Yermenchuk O.P. European experience in critical infrastructure protection: legal analysis and perspectives of implementation in Ukraine. The analysis of European legislation in the field of critical infrastructure protection is carried out. The basic requirements for construction of a state control system of such a system are stated. The peculiarities of its functioning, structure, powers of its subjects of management and tasks of this control system are determined. The concept-categorical apparatus in the sphere of critical infrastructure protection of Ukraine is substantiated, in particular: "protection of critical infrastructure", "critical infrastructure critical infrastructure", "critical infrastructure security", "risk", "vulnerability of the object of critical infrastructure", " consequences".

In a number of European countries, the responsibility of the critical infrastructure objects is to take appropriate measures to detect, at an early stage, threats, to prevent risks from their actions and to further continuously control them, in order to ensure the continued functioning of critical infrastructures, the provision of appropriate services and the promotion of stability. in the region and in general in the state. To such adverse factors, along with risky operations, violations of the requirements of legislative acts in the sphere of financial and economic activity and the commission of offenses provided for by administrative or criminal legislation (covered by risk management), also include threats of natural disasters, acts of terrorism, cyber incidents, espionage, competitive intelligence, etc., which can have a significant effect on further activities and even the existence of an object.

Keywords*: state system of management in the field of critical infrastructure protection of Ukraine, national infrastructure, critical infrastructure, protection of critical infrastructure, stability of the critical infrastructure, critical infrastructure security, risk, vulnerability of the critical infrastructure facility, consequences.*