Захист енергетичної інфраструктури: аналіз зарубіжного законодавства

Захист важливої інфраструктури життєдіяльності суспільства стає одним з найважливіших пріоритетів держави. Важливість безпечного функціонування критичної інфраструктури, і зокрема енергетичної інфраструктури, є чинником забезпечення національної безпеки, сталого функціонування економіки, добробуту та захисту населення країни.

Для України важливість захисту інфраструктури була актуалізована російською агресією у 2014 р. У той же час українське законодавство не вимагає створення єдиної державної системи фізичного захисту енергетичної інфраструктури від цілеспрямованих зловмисних дій [1]. Питання захисту об'єктів енергетики врегульовується на галузевому та відомчому рівні без належної координації та узгодження з іншими пріоритетами забезпечення національної безпеки. Виключення з цього становить лише система захисту ядерних установок від загроз ядерного тероризму, у рамках якої розроблена методологія організації системи захисту та запропоновано окремий інструментарій організації та координації зусиль у вигляді «проектної загрози» [2].

Саме тому, використання досвіду країн, які раніше стали приділяти увагу захисту критичної інфраструктури, є важливим при створені єдиної системи фізичного захисту енергетичної інфраструктури в Україні.

1. Зарубіжний досвід правового регулювання у сфері захисту енергетичної інфраструктури

Найбільших успіхів у даній сфері досягли Сполучені Штати Америки (США). Роботу з питань захисту критичної інфраструктури було започатковано ще наприкінці минулого століття. Тим не менш переломним моментом у становленні єдиної концепції захисту критичної інфраструктури стали трагічні події, пов'язані з терористичними актами 11 вересня 2001 р. у Нью-Йорку. США кардинально переглянули підходи щодо забезпечення безпеки держави, що відобразилось у прийнятті «Акта про патріотизм» (USA PATRIOT ACT) [3]. Законом було визначено потребу у захисті критичної інфраструктури життєдіяльності суспільства та дано визначення терміну «критична інфраструктура», а саме: «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище» [4].

Завдання захисту критичної інфраструктури підняло проблему узагальнення та аналізу необхідної інформації, що зумовило прийняття «Акту щодо інформації з критичної інфраструктури» (Critical Infrastructure

Information Act (“CIIA”) [5] у 2002 р. Зазначеним законом регулюється питання щодо обміну інформації з питань оцінки вразливості та загроз інфраструктурі, у тому числі пов’язаних із терористичними загрозами. Закон вводить важливий термін «інформація щодо критичної інфраструктури» як інформації, яка зазвичай не знаходиться у полі уваги суспільства та відноситься до безпеки функціонування критичної інфраструктури чи захищених систем. Акт визначає урядовий орган, Департамент внутрішньої безпеки, відповідальним за збір, аналіз та поширення інформації з метою прийняття необхідних заходів із захисту критичної інфраструктури. Одночасно законом встановлюються вимоги та обмеження щодо використання такої інформації (вводиться режим обмеженого доступу) для недопущення зловживань та захисту суб’єктів господарювання (операторів інфраструктури) від поширення чутливої комерційної інформації.

Цільова Стратегія фізичного захисту критичної інфраструктури США була затверджена у 2003 р. (The Physical Protection of Critical Infrastructures and Key Assets) [6] та охопила організаційні та інституційні питання захисту енергетичної інфраструктури.

Стратегія визначила національні цілі та принципи реалізації державної політики захисту критичної інфраструктури та важливих активів для цілей забезпечення національної безпеки, ефективного врядування, суспільної безпеки, економічного розвитку та соціальної стабільності.

Цілями Стратегії визначено: ідентифікацію важливої для забезпечення національної безпеки критичної інфраструктури та формування системи її захисту; забезпечення випереджуючого інформування та фізичного захисту інфраструктури, у відношенні якої існують (виявлено) безпосередні та специфічні загрози; запровадження спеціальних механізмів захисту критичної інфраструктури від потенційних загроз довгострокового плану (залежно від часу, ринкової ситуації, оцінки ризиків); налагодження механізму взаємодії різних зацікавлених осіб (державних органів влади, суб’єктів господарювання, громадян) у цій сфері.

Стратегія забезпечила: уніфікацію підходів до реалізації заходів окремими штатами (уніфікація законодавства); ідентифікацію окремих спеціальних заходів, які мають суттєвий вплив на загальнонаціональному рівні; встановлення організаційно-інституційних засад координації діяльності та поєднання зусиль зацікавлених осіб для забезпечення захисту критичної інфраструктури у найбільш ефективний спосіб.

Стратегія також визначила загальні вимоги організації діяльності з захисту критичної інфраструктури від зловмисних дій, а саме: забезпечення планування заходів та розподілу ресурсів, обміну інформацією та

попередження щодо можливих загроз, захисту персоналу та підвищення його обізнаності з цих питань, дослідження та розвитку технологій захисту, моделювання ситуацій та аналіз ризиків.

У подальшому, питання захисту критичної інфраструктури знайшло своє відображення у Плані захисту національної інфраструктури (2009 р.) [7], який безпосередньо забезпечував координацію зусиль різних урядових агенцій та реалізацію національної стратегії захисту критичної інфраструктури. Заходи Плану спрямовані на: поглиблення розуміння та поширення інформації щодо теоретичних загроз та інших ризиків критичній інфраструктурі; формування партнерства щодо обміну інформацією і кращим досвідом; впровадження довгострокових програм управління ризиками; забезпечення ефективного використання суспільних ресурсів для захисту, відновлення та подолання можливих наслідків критичній інфраструктурі.

У частині енергетичного сектору планом виділяється три основних блоки уваги, зокрема електроенергетична інфраструктура, нафта та нафтопереробка, а також газова сфера. При цьому відзначається вагомість приватного сектору, оскільки понад 80 % всієї енергетичної інфраструктури США знаходиться у приватній власності, що потребує окремих механізмів узгодження та координації зусиль [8].

Стратегія національної безпеки США 2010 р. [9] додатково звертає увагу на важливість державно-приватного партнерства у забезпеченні стійкості функціонування критичної інфраструктури. Зокрема, наголошується на тому, що приватним власникам (операторам) належить як більшість об’єктів критичної інфраструктури, так і лідерство у розробці новітніх технологій виробництва та технологій їх захисту. Стратегія стимулює як приватних власників, так і уряд створити таку інфраструктуру життєзабезпечення суспільства, яка буде спроможна переборювати надзвичайні ситуації, знижувати ризики та наслідки виникнення таких ситуацій.

В Європейському Союзі питання захисту критичної інфраструктури також розвивалось тривалий час [10]. Формування ж єдиного загальноєвропейського підходу на офіційному рівні було врегульовано Директивою Ради ЄС у 2008 р. [11]. Директива встановила вимоги щодо визначення окремих об’єктів та їх включення до переліку європейської критичної інфраструктури, а також запропонувала загальний підхід щодо захисту критичної інфраструктури та оцінки систем захисту.

Директивою дається визначення «критичної інфраструктури», що розуміється як «активи, системи або їх частина, які розташовані в державах-членах та є важливими для життєзабезпечення суспільства, здоров'я, безпеки, економічного чи соціального благополуччя людей, порушення або

руйнування яких матиме значний вплив в країнах-членах як результат неспроможності виконувати відповідні функції». Дається також визначення «європейської критичної інфраструктури», до якої відносять елементи національних критичних інфраструктур країн-членів ЄС, порушення функціонування яких призведе до негативних наслідків не менш ніж для двох країн ЄС.

Визначаються поняття «аналіз ризиків» як сценарний аналіз можливих загроз з метою оцінки вразливості та потенційних наслідків припинення або руйнування критичної інфраструктури та «захист», як будь-які види діяльності, спрямовані на забезпечення сталого, тривалого та інтегрованого функціонування критичної інфраструктури з метою відвернення, зниження та нейтралізації загроз, ризиків або вразливості інфраструктури.

Від кожної країни вимагається забезпечення постійного перегляду переліку об'єктів критичної інфраструктури, виходячи з наступних критеріїв: можливі фізичні втрати населення (смерті та поранення); економічні втрати (збитки, погіршення функціонування суб'єктів господарювання (економіки), екологічні втрати); величина впливу на життєдіяльність суспільства (суспільне занепокоєння, порушення надання послуг, страждання населення).

У свою чергу відповідно до Директиви власники (оператори) об'єктів інфраструктури мають підготувати «план безпеки» як процедури ідентифікації об'єктів та заходів безпеки щодо їх захисту, а також визначити співробітників, завданням яких буде зв'язок та обмін інформацією з національним органом, відповідальним за захист критичної інфраструктури. При цьому Директива наголошує, що обмін інформацією вимагає довірчих відносин та забезпечення захисту конфіденційних даних залучених компанії та організації.

Необхідний план безпеки оператора має містити визначення критичних об'єктів інфраструктури, проведення ризик-аналізу основних можливих загроз та потенційних наслідків, визначення заходів протидії реалізації загроз та відповідні процедури їх реалізації для різних сценаріїв (звичайні та підвищені заходи безпеки). Відповідні заходи мають охоплювати: технічні заходи, організаційні заходи, контрольні та версифікаційні заходи ефективності системи захисту, програми комунікації, підвищення усвідомленості та навчання персоналу тощо.

У частині енергетичного сектору Директивою виділено наступні критичні об'єкти, порушення роботи яких буде мати серйозні наслідки: інфраструктура та обладнання для генерування та передавання електроенергії; видобувні нафто- та газопромисли; об'єкти переробки та зберігання нафти та газу; трубопроводи, сховища та термінали.

У свою чергу Єврокомісія розробила робочий документ, який формалізує Європейську програму захисту критичної інфраструктури (EPCIP) [12] та встановлює загальні рамки для організації діяльності в усіх державах ЄС та передбачає підтримку шляхом координації зусиль і регулярного обміну інформацією між державами ЄС у цій сфері.

Програма розроблена з метою підвищення рівня захищеності критичної інфраструктури шляхом запровадження узгодженого підходу до її захисту в країнах-членах ЄС та гармонізації національних законодавств. При цьому загрози, яким програма спрямована запобігати, не пов’язуються лише з тероризмом, але також включають злочинну діяльність, стихійні лиха та інше. Окремо програма передбачає створення Мережі попереджувального інформування захисту критичної інфраструктури (CIWIN).

Єврокомісія фінансує окремі заходи у сфері захисту критичної інфраструктури в рамках спеціальної програми фінансування «Попередження, готовність та ліквідація наслідків тероризму та інших пов'язаних з безпекою програми ризиків» [13]. Програма призначена для захисту громадян і критично важливих об'єктів інфраструктури від терористичних атак та інших інцидентів в області безпеки за рахунок поліпшення систем захисту критичної інфраструктури та розробки рішень у рамках кризового управління. Ключовим завданням є підтримка політики захисту критичної інфраструктури шляхом надання експертних знань та розробки наукових засад і методології діяльності у цій сфері на всіх рівнях функціонування системи захисту.

Концепція захисту критичної інфраструктури прийнята також Російською Федерацією (РФ) [14].

Затверджені у 2006 р. «Основи державної політики в галузі забезпечення безпеки населення Російської Федерації і захищеності критично важливих та потенційно небезпечних об’єктів від загроз техногенного, природного характеру та терористичних актів» [15] забезпечили введення необхідної термінології та формулювання загальних підходів до реалізації державної політики у цій сфері.

Зокрема, було визначено термін «критично важливі об’єкти інфраструктури» як «об’єкти, порушення (або припинення) функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін (або руйнування) економіки країни, суб’єкту або адміністративно-територіальної одиниці, або до суттєвого погіршення безпеки життєдіяльності населення, що мешкає на цих територіях, на тривалий період часу».

Серед основних факторів, які визначали державну політику забезпечення захисту населення та захищеності небезпечних об'єктів, відзначались зокрема:

– збільшення кількості потенційно небезпечних об'єктів, які розміщувались у густонаселених районах;

– моральне старіння систем та комплексів захисту, зниження рівня підготовки персоналу, низька виробнича культура;

– посилення загрози міжнародного і внутрішнього тероризму.

Цілями політики визначалось: створення необхідних умов для безпечної життєдіяльності та соціально-економічного розвитку РФ; підвищення рівня безпеки технологій, пов'язаних із експлуатацією потенційно небезпечних об'єктів; мінімізація наслідків надзвичайних подій техногенного, природного характеру та терористичних актів.

У подальшому законодавча база, пов'язана із захистом критичної інфраструктури, удосконалювалась та розширювалась. Затверджено «Основні напрями державної політики в галузі забезпечення безпеки автоматизованих систем управління виробничими і технологічними процесами критично важливих об'єктів інфраструктури Російської Федерації» [16]. Особливістю даного акту є виділення загрози «комп'ютерної атаки» як цілеспрямованого впливу на інформаційно-телекомунікаційні мережі програмно-технічними засобами та необхідності формування сил реагування та реалізації заходів щодо ліквідації наслідків таких атак.

Тривалий час діє та періодично переглядається Федеральна цільова програма «Зниження ризиків і пом'якшення наслідків надзвичайних ситуацій природного і техногенного характеру в Російській Федерації» [17]. Затверджено ряд інших нормативно-правових документів, які регламентують захист критично важливих об'єктів в РФ, зокрема «Федеральний план підвищення захищеності критично важливих об'єктів РФ від загроз технічного, природного характеру і терористичних актів» та «Перелік критично важливих об'єктів Російської Федерації».

Слід відзначити, що поступово удосконалюючи законодавство захисту критичної інфраструктури, все більше акцентується увага на створенні механізму випереджаючого аналізу потенційних загроз.

Так, при перегляді основ державної політики у цій сфері однією із її цілей було визначено «мінімізацію ризиків надзвичайних ситуацій природного, техногенного характеру та терористичних актів». Досягнення цілей політики передбачається забезпечити, серед іншого, через запровадження наукових методів прогнозу ризиків, впровадження технічних регламентів з питань забезпечення безпеки експлуатації (функціонування) і

захищеності об’єктів. Було визначено, що планування заходів забезпечення безпеки населення і захищеності об’єктів має здійснюватись з урахуванням ступеня ризику виникнення можливих загроз. При цьому наголошується на необхідності «здійснити розвиток сил, що забезпечують безпеку об’єктів та оснастити ці сили сучасною технікою і технічними засобами» [18].

Окремо слід відзначити Федеральний закон РФ, що стосується безпосередньо захисту енергетичних об’єктів. Закон «Про безпеку об’єктів паливно-енергетичного комплексу» формує правову базу діяльності щодо недопущення вчинення терористичних та інших зловмисних дій, спрямованих на завдання шкоди об’єктам паливно-енергетичного комплексу [19].

Даним законом чітко виділяється «акт незаконного втручання як протиправна дія (бездіяльність), у тому числі терористичний акт або спроба його здійснення, що загрожує безпечному функціонуванню об’єкта паливно-енергетичного комплексу та спричинила шкоду життю та здоров’ю людей, пошкодження або знищення майна або створила загрозу виникнення таких наслідків».

Закон визначає необхідність існування «антитерористичної захищеності об’єкта енергетики», а також виділяє «критично важливі об’єкти енергетики». Під таким об’єктами розуміються «об’єкти енергетики, порушення або припинення функціонування яких призведе до втрати керованості економікою Російської Федерації, суб’єкта РФ або її адміністративно-територіальної одиниці, її незворотної негативної зміни (руйнування) або істотного зниження безпеки життєдіяльності населення».

У вигляді інструменту організації системи охорони таких об’єктів запроваджується «паспорт безпеки об’єкта», що містить необхідну інформацію та план заходів із забезпечення його антитерористичної захищеності. Паспорт безпеки об’єкта затверджується керівником суб’єкта господарювання за погодженням із колегіальним органом з протидії тероризму у регіоні. Доступ до інформації, наведеній у такому паспорті, обмежується.

Законом встановлюються вимоги до суб’єктів господарювання щодо забезпечення антитерористичної захищеності для різних об’єктів, а для диференціювання відповідних вимог передбачено проведення категоризації об’єктів охорони. На основі категоризації формується реєстр об’єктів енергетичної інфраструктури, відповідно до якого визначається відповідальний орган за забезпечення антитерористичної захищеності.

Для забезпечення фізичного захисту критичних об’єктів, у залежності від категоризації об’єкта, можуть використовуватись підрозділи та

організації федерального органу виконавчої влади, відомча охорона, приватні охоронні організації. При цьому виділяються критичні елементи енергетичної інфраструктури та лінійні об'єкти (трубопроводи та електромережі), які мають суттєві особливості щодо організації охорони.

Фінансування охоронних заходів здійснюється за рахунок власних коштів суб'єктами паливно-енергетичного комплексу, однак ці витрати враховуються у складі цін (тарифів) та регулюються державою. Використання для цих цілей інших джерел фінансування регулюється окремим законодавством. При цьому суб'єкти зобов'язуються ще на етапі проектування та будівництва передбачити заходи щодо безпечного функціонування критичних об'єктів енергетики та зниження наслідків надзвичайних ситуацій.

У квітні 2014 р. до Закону було внесено зміни, якими окремо визначалось створення відомчої охорони окремими суб'єктами господарювання. Зокрема, власник Єдиної системи газопостачання, стратегічні акціонерні товариства, які управляють системою магістральних нафтопроводів і нафтопроводів, які здійснюють діяльність з добування і переробки вуглеводневої сировини, отримали право створити відомчу охорону [20].

Відповідно до Закону РФ «Про відомчу охорону» [21] повноваження відомчої охорони набагато ширші тих, якими володіють приватні охоронні структури. Відомча охорона може: обшукувати людей і автотранспорт; застосовувати зброю не тільки на об'єктах (які захищаються), а й поза ними; використовувати зброю (навіть при значному скупченні людей) у випадку, якщо здійснюється напад на об'єкт їх охорони. Структури відомчої охорони можуть використовувати і бойову автоматичну зброю.

2. Аналіз зарубіжного досвіду та пропозиції до формування системи захисту енергетичної інфраструктури в Україні

Важливість формування системи захисту енергетичної інфраструктури в Україні пов'язується не тільки із загальним підвищенням актуальності захисту критичної інфраструктури, що викликано загальним технологічним та інституційним ускладненням її функціонування, але й з тим, що терористичні акти досі не розглядались інструментом цілеспрямованого підриву спроможності держави забезпечити стале енергозабезпечення суспільства та економіки.

Враховуючи важливість енергетичної інфраструктури для життєдіяльності суспільства, система захисту критичної інфраструктури має координувати дії самих різних зацікавлених осіб. З огляду на те, що сьогодні більшість суб'єктів господарювання в енергетичному секторі є приватними,

відповідальність за забезпечення захисту критичної інфраструктури країни мають нести як відповідні органи державної влади, так і приватний сектор (оператори енергетичної інфраструктури). При цьому інші зацікавлені особи, зокрема місцеві органи влади та населення, мають також залучатись до діяльності у цій сфері.

Органи державної влади мають виконувати ряд важливих функцій загальнодержавного рівня, передусім: законодавче та нормативно-правове регулювання діяльності у сфері захисту енергетичної інфраструктури; координацію та організаційне забезпечення функціонування єдиної державної системи захисту енергетичної інфраструктури; надання операторам інфраструктури вчасної інформації щодо можливих перспективних загроз і ризиків; об'єднання зусиль зацікавлених осіб (операторів, органів влади, громадськості) для визначення стратегічних пріоритетів та методології організації діяльності, а також мінімізації видатків на функціонування системи.

При цьому варто наголосити на необхідності існування окремого центру аналізу та обробки інформації. Даний елемент системи, з одного боку, має забезпечити сценарний аналіз можливих загроз з метою оцінки вразливості та потенційних наслідків припинення або руйнування інфраструктури, з іншого боку, має здійснити «розподіл» завдань та постановку цілей для інших елементів системи забезпечення захисту енергетичної інфраструктури. Важливим при цьому є визначення джерел фінансування діяльності такого центру, а також питання захисту інформації з обмеженим доступом. Дана ситуація вимагає розробки відповідних правил та підготовки персоналу, відповідального за комунікацію та обробку відповідної інформації.

Суб'єкти господарювання – власники об'єктів критичної енергетичної інфраструктури – мають забезпечити: ідентифікацію критичної енергетичної інфраструктури та формування переліку об'єктів фізичного захисту; розроблення, відповідно до встановленої методології, паспорту загроз енергетичній інфраструктурі; формування планів захисту критичної інфраструктури та їх узгодження в рамках єдиної державної системи захисту.

При цьому важливим є чітке врегулювання питань безпосереднього забезпечення фізичного захисту об'єктів критичної енергетичної інфраструктури від зловмисних дій, передусім врегулювання питань: підпорядкованості та повноважень охоронних структур; методів та засобів захисту (у нормальному та надзвичайному режимі функціонування); залучення Збройних Сил України та правоохоронних органів; джерел фінансування.

Загалом, проблему впровадження цілісної концепції та формування дієвої системи захисту критичної інфраструктури в Україні потрібно вирішувати з огляду на загальні процеси модернізації системи забезпечення національної безпеки держави та перспективної системи адміністративного та політичного устрою держави.

Тим не менш у будь-якому випадку доцільним є розроблення, з врахуванням наведеного зарубіжного досвіду, законодавчого акту, який визначить основні засади функціонування системи захисту енергетичної інфраструктури. У відповідному законодавчому акті доцільно відобразити загальні підходи до змісту та напрямів реалізації державної політики у цій сфері, а також коло відповідальності зацікавлених осіб. Пропозиції щодо зазначених питань наведено у Таблиці 1.

Таблиця 1
Засади державної політики захисту енергетичної інфраструктури

Напрями	Відповідальність та інструменти
Формування системи захисту критичної інфраструктури	Уряд відповідальний за законодавче врегулювання діяльності державної системи захисту енергетичної інфраструктури та координацію зусиль різних суб'єктів шляхом встановлення вимог до діяльності системи захисту, інформування та обміну інформацією. Оператори енергетичної інфраструктури відповідальні за організаційно-ресурсне забезпечення функціонування системи захисту енергетичної інфраструктури та обмін інформацією відповідно до встановлених вимог. Уряд/Оператори енергетичної інфраструктури визначають пріоритети своїх дій у своїх стратегічних та програмних документах.
Визначення критичної інфраструктури та ідентифікація критичних елементів (об'єктів)	Уряд відповідальний за розроблення методології ідентифікації критичної інфраструктури (вимоги, стандарти, методологія, методики огляду та оцінки), визначення енергетичної інфраструктури та критичних елементів (перелік критичної інфраструктури). Оператори відповідальні за визначення переліку об'єктів захисту та впровадження доведених вимог щодо захисту в операційну діяльність суб'єктів господарювання.
Оцінка ризиків інфраструктурі: – Оцінка загроз – Оцінка вразливості та наслідків	Уряд відповідальний за здійснення оцінки загроз в контексті загроз національній безпеці, формування методології оцінки ризиків та реагування на загрози. Оператори здійснюють оцінку загроз на технологічному і корпоративному рівні та відповідальні за розробку паспорта загроз енергетичній інфраструктурі. Уряд/Оператори відповідальні за періодичність проведення оцінки в рамках стандартизованих вимог
Визначення та проведення заходів захисту енергетичної інфраструктури	Уряд визначає вимоги до формування плану захисту енергетичної інфраструктури та сприяє операторам у розроблені плану захисту за допомогою затвердження стандартів та керівних принципів діяльності у сфері захисту енергетичної інфраструктури, а також надання інформаційної , технічної та ресурсної підтримки. Оператор розробляє та забезпечує реалізацію плану заходів захисту енергетичної інфраструктури відповідно до встановлених вимог.
Забезпечення фізичного захисту у випадках прояву тероризму	Уряд забезпечує фізичний захист об'єктів енергетики відповідними військовими підрозділами у випадку цілеспрямованих актів (акт тероризму, диверсія). Оператори забезпечують охорону та фізичний захист об'єктів енергетики у звичайний період відповідно до встановлених вимог у рамках планів захисту.
Встановлення джерел фінансування	Уряд визначає принципи розподілу фінансових зобов'язань між державою та операторами. Уряд визначає заходи, які він зобов'язується фінансувати у рамках

	функціонування єдиної системи захисту (забезпечення фізичного захисту від безпосередніх атак, розроблення методології, наукове дослідження та оцінка загроз та методів реагування, розроблення керівних документів тощо). Оператор фінансує виконання плану захисту відповідно до законодавства та визначеної урядом методології покриття видатків.
Перегляд та уточнення стратегії безпеки	Уряд та оператори інфраструктури періодично переглядають загрози безпеки, уточнюють цілі та визначають адекватні засоби реалізації політики шляхом удосконалення методології оцінки загроз, перегляду паспорту загроз та планів захисту

Список літератури

1. *Суходоля О. М.* Захист енергетичної інфраструктури: аналіз української законодавчої бази. Аналітична записка. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1568/.

2. Оцінка загрози ядерного тероризму: проектна загроза: Науково-методологічний посібник / С. І. Кондратов, Ю. М. Скалецький, В. І. Кравцов та ін..; за заг. ред. В. П. Горбуліна. – К.: ДП «НВЦ «Євроатлантикінформ», 2006. – 76 с.

3. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT, 2001) [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.gov.

4. *Бірюков Д. С., Кондратов С. І.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. – К.: НІСД, 2012. – 57 с.

5. Critical Infrastructure Information Act of 2002 (“CIIA”). [Електронний ресурс]. – Режим доступу: https://www.fas.org/sgp/crs/RL31762.pdf.

6. The Physical Protection of Critical Infrastructures and Key Assets. [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets.

7. National Infrastructure Protection Plan (NIPP): Partnering to enhance protection and resiliency. – US Dep. Homeland Security. – 2009. – 188 p. [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/national-infrastructure-protection-plan.

8. Homeland Security. Energy Sector. [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/energy-sector.

9. National Security Strategy. – Washington: The White House, May, 2010 [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

10. European Programme for Critical Infrastructure Protection. [Електронний ресурс]. – Режим доступу: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

11. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

12. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0786:EN:NOT.

13. Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS). http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm.

14. *Бірюков Д. С., Кондратов С. І.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. – К.: НІСД, 2012. – 57 с.

15. Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов. Указ Президента РФ 28 сентября 2006 года ПР-1649. [Електронний ресурс]. – Режим доступу: http://umcpo.ru/files/bezopasnost/rukovod_doc/osnovi_gos_politiki.pdf.

16. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации / Совет Безопасности РФ. [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/113.html.

17. ФЦП «Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в Российской Федерации до 2010 года». [Електронний ресурс]. – Режим доступу: http://www.mchs.gov.ru/activities/fcp/archive_fcp/FCP_Snizhenie_riskov_i_smjagchenie_posle.

18. Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года. Указ Президента РФ 15 ноября 2011 г. № Пр-3400 [Електронний ресурс]. – Режим доступу: http://base.garant.ru/70141358/.

19. Федеральный закон Российской Федерации от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

[Електронний ресурс]. – Режим доступу: http://www.rg.ru/2011/07/26/tek-dok.html.

20. Федеральный закон Российской Федерации от 20 апреля 2014 г. № 75-ФЗ. «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу создания ведомственной охраны для обеспечения безопасности объектов топливно-энергетического комплекса». [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2014/04/23/akty-dok.html.

21. Федеральный закон от 14 апреля 1999 г. № 77-ФЗ «О ведомственной охране» (с изменениями и дополнениями). [Електронний ресурс]. – Режим доступу: http://base.garant.ru/1351707/ ***(Суходоля О. М. Захист енергетичної інфраструктури: аналіз зарубіжного законодавства. Аналітична записка // Національний інститут стратегічних досліджень (http://www.niss.gov.ua/articles/1600/).***