НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Аналітична доповідь

КИЇВ - 2012

***Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні.* - К.: НІСД, 2012. - 57 с**.

Автори:
Бірюков Д.С. – старший консультант відділу екологічної та техногенної безпеки, кандидат технічних наук
Кондратов С.І. – старший науковий співробітник відділу екологічної та техногенної безпеки

Вступ

Останніми десятиліттями в світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різноманітної природи. Щодня світові ЗМІ повідомляють про природні та техногенні катастрофи, збройні конфлікти, терористичні акти, важкі злочини, вчинені як злочинними організаціями, так і окремими особами, акти піратства на морі тощо. І все частіше в результаті таких надзвичайних подій жертвами стає велика кількість людей, а життєво важливим для існування держав системам, об’єктам і ресурсам завдається серйозна шкода.

З огляду на такі тенденції в більшості провідних країн світу з метою систематизації об’єктів, втрата або порушення нормального функціонування яких призведе до значних або навіть непоправних негативних наслідків для національної безпеки, введено термін «критична інфраструктура». До критичної інфраструктури прийнято відносити транспортні та енергетичні мережі, системи міжбанківських розрахунків і телекомунікації, а також об’єкти, необхідні для функціонування органів державної влади, служби реагування на надзвичайні ситуації та екстреної допомоги населенню, системи життєзабезпечення мегаполісів.

Проблема запровадження системного підходу до розв’язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише введення відповідного терміну. На перше місце тут виходить завдання створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди ключовим (вузловим) елементам критичної інфраструктури внаслідок дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа.

Було б невірно сказати, що в Україні не приділяється увага захисту важливих об’єктів, систем та ресурсів, які, зазвичай, відносять до критичної інфраструктури. Навпаки, в Україні діє ціла низка законодавчих актів, що визначають особливості забезпечення захисту критичної інфраструктури.

Проте в державі досі відсутній загальний механізм управління захистом та безпекою цих об’єктів, спостерігаються непоодинокі випадки дублювання функцій та ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу. До того ж загрози таким об’єктам розглядаються в суто «відомчому» розрізі.

Все це спонукає нас говорити про необхідність впровадження низки суттєвих заходів на державному, регіональному та галузевому рівнях з правового та організаційно-методичного забезпечення, координації та консолідованого забезпечення ресурсами систем безпеки, спільного використання засобів безпеки, які знаходяться в підпорядкуванні окремих відомств.

Зважаючи на сприятливі умови, що створюються в ході модернізації безпекового сектору в Україні, впровадження концепції захисту критичної інфраструктури може стати серйозним внеском у зміцнення національної безпеки нашої держави.

1. Міжнародний досвід створення та функціонування системи захисту критичної інфраструктури

З середини 90-х років XX століття поняття «критична інфраструктура» було введено в нормативно-правові документи та практику міжнародного спілкування на дипломатичному рівні, в науковому та діловому колах. Значення цього терміну дещо відрізняється від країни до країни, але ці відмінності не є суттєвими. Зокрема, згідно з чинним законодавчим актом Сполучених Штатів, під критичною інфраструктурою розуміються: «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»[1].

Як правило, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Слід зауважити, що у США критичну інфраструктуру розглядають у більш широкому розумінні, включаючи до неї національні символи (пам'ятки культурної спадщини).

На сьогодні захист критичної інфраструктури ствердився як важливий напрям політики в сфері безпеки країн-членів НАТО та ЄС. До двох основних чинників, що сформували концепцію захисту критичної інфраструктури, слід віднести: по-перше, посилення боротьби з міжнародним тероризмом (система захисту критичної інфраструктури вдосконалювалася як відповідь на вчинені терористичні акти в США в 2001 р., Іспанії в 2004 р. та Великій Британії в 2005 р.) та, по-друге, забезпечення безпеки у процесі розробки та реалізації основних проектів в області інфраструктури для транспортування нафти, нафтопродуктів, газу та інших стратегічних сировинних матеріалів. Останнє ще було підтверджено заявою, зробленою за результатами саміту країн НАТО (пункт 52[2]), що відбувся 20-21 травня 2012 р. в м. Чикаго (США).

На особливу роль критичної інфраструктури звертають увагу і експерти Всесвітнього банку. Вони підкреслюють, що хоча необхідно якісно проектувати та будувати будь яку інфраструктуру, але виокремлення категорії критичних об'єктів інфраструктури дозволяє урядам приділяти їм особливу увагу, і тим самим зменшити наслідки, спричинені природними

[1] *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
[2] *Chicago* Summit Declaration [Електронний ресурс]. – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. – Режим доступу: http://www.nato.int/

лихами і техногенними аваріями[3].

Аналіз міжнародного досвіду показує, що в основі забезпечення захищеності і безпеки критичної інфраструктури лежить вирішення низки питань, серед яких ключовими є:

– координація та взаємодія силових відомств та обмін інформацією про загрози;

– організація державно-приватного партнерства в сфері безпеки;

– використання ризик-орієнтованого підходу при попередженні загроз критичній інфраструктурі.

Становлення нормативно-правової бази в сфері захисту критичної інфраструктури є тривалим процесом. Напевно найбільших успіхів в даній сфері досягли США. Адміністративний наказ Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних та фізичних загроз» (липень 1996 р.), а згодом Директива Президента США № 63 (травень 1998 р.)[4] започаткували в США національну програму «Захист критичної інфраструктури». Продовження роботи з підсилення захисту критичної інформаційної інфраструктури відобразилося в Національному плані з захисту інформаційних систем (січень 2000 р.). Але переломним моментом у становленні концепції захисту критичної інфраструктури стала необхідність реагувати на терористичні акти, вчинені 11 вересня 2001 р. у Нью-Йорку. Після цієї екстраординарної події уряд США кардинально переглянув підходи щодо забезпечення внутрішньої безпеки держави (як в технічному, так і в організаційному плані). Важливим висновком з трагедії стало прийняття нормативно-правового документу, абревіатура назви якого перекладається як «Акт про патріотизм» (*USA PATRIOT ACT*[5]), в ньому термін критична інфраструктура набув свого

---

[3] *Стихийные* бедствия и техногенные катастрофы: Превентивные меры / Всемирный банк и Организация Объединенных Наций; пер. с англ. - М.: Альпина Паблишер, 2012.- 312 с.

[4] *PDD-63*, May, 1998: Critical Infrastructure Protection [Електронний ресурс]. – Federation of American Scientists. – Режим доступу: http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf

[5] *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

сучасного вигляду.

Саме після 11 вересня 2001 р. США постійно приділяють найсерйознішу увагу зусиллям, спрямованим на захист критичної інфраструктури, що знайшло своє відображення, зокрема, і в останніх стратегічних документах із забезпечення національної безпеки (Стратегії національної безпеки, 2010 р.), і в оновленому плані захисту національної інфраструктури (2009 р.).

Щоб проілюструвати пріоритетну увагу політичного керівництва США цій проблематиці достатньо лише навести короткий перелік основних документів, прийнятих після 11 вересня 2001 р.: Адміністративний наказ Президента США № 13228 «Організація захисту США від терористичних загроз» та № 13231 «Про захист національних критичних інформаційних систем» (жовтень 2001 р.); Стратегія національної безпеки (липень 2002 р.); Національна стратегія захисту критичної інфраструктури і ключових фондів (лютий 2003 р.); Директива Президента США з національної безпеки № 7 (грудень 2003 р.)[6]; План захисту національної інфраструктури (жовтень 2006 р.); План захисту національної інфраструктури (жовтень 2009 р.); Політика у сфері кіберпростору (2009 р.)[7]; Стратегія національної безпеки (березень 2010 р.)[8].

Про значимість захисту критичної інфраструктури свідчить рівень фінансування даного сегменту забезпечення національної безпеки. На захист критичної інфраструктури в США витрачається більша частина коштів, які виділяються у федеральному бюджеті на забезпечення внутрішньої безпеки (у 2012 р. – близько 67,9 млрд дол. та у проекті бюджету на 2013 р. – 68,9 млрд дол. США)[9]. При цьому у 2012 р. розподіл бюджетних коштів на

---

[6] *Homeland* Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/homeland-security-presidential-directive-7

[7] *Cyber* space policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure [Електронний ресурс]. – Washington: The White House, 2009. – Режим доступу: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[8] *National* Security Strategy. – Washington: The White House, May, 2010 [Електронний ресурс]. – Режим доступу: www.whitehouse.gov/.

[9] *Defining* Homeland Security: Analysis and Congressional Considerations / Congressional Research Service: Report for Congress R42462, April 3. – 2012. – 15 p.

зазначені цілі відбувався таким чином: Міністерство внутрішньої безпеки – 52 %, Міністерство оборони – 26 %, 29 інших суб'єктів (міністерств, агентств та установ) – 22 %.

У США керівні документи з організації захисту та реагування на загрози критичній інфраструктурі постійно вдосконалюються, відповідні плани реагування та евакуації населення при надзвичайних ситуаціях періодично переглядаються. Відбувається оновлення технічних засобів попередження та реагування на надзвичайні ситуації, удосконалення способів та засобів інформування населення.

В директиві Президента США з національної безпеки № 7 (грудень 2003 р.)[10] визначено відповідальність Міністерства внутрішньої безпеки, інших міністерств та федеральних агентств, які є відповідальними за окремі сектори критичної інфраструктури. На Міністерство внутрішньої безпеки покладено обов'язок формувати Національний план захисту критичної інфраструктури. Аналізуючи національні плани захисту критичної інфраструктури США (останній розроблений у 2009 р. та попередній – 2006 р.), можна зробити висновки про те, що зміни та вдосконалення були здійснені на таких головних напрямах: планування регіонального захисту, вдосконалення загального підходу до управління ризиком, вдосконалення методики оцінок безпеки за секторами[11].

На відміну від США, де було створено єдиний орган виконавчої влади (Міністерство внутрішньої безпеки), на який покладено функції координації захисту критичної інфраструктури США, в ЄС такого органу немає, а функції захисту критичної інфраструктури виконують відповідні органи окремих країн-членів ЄС.

В ЄС загальноєвропейський підхід до захисту критичної інфраструктури задекларовано в Директиві Європейської Комісії № 786

[10] *Homeland* Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/homeland-security-presidential-directive-7

[11] *National* Infrastructure Protection Plan: Partnering to enhance protection and resiliency. – US Dep. Homeland Security. – 2009. – 188 p.

2006 р.[12]. До загальноєвропейської критичної інфраструктури відносять ті елементи національних критичних інфраструктур країн-членів ЄС, відмова, інцидент або атака на які може мати значний вплив як на країну, в який ця подія відбудеться, так і хоча б на одну іншу країну-члена ЄС. Згадана директива започаткувала Європейську програму з захисту критичної інфраструктури, яка розроблена з метою підвищення рівня захищеності критичної інфраструктури шляхом створення спільного підходу до її захисту в країнах-членах ЄС і гармонізації національних законодавств в даній сфері.

Слід відзначити, що провідні країни світу здійснюють захист своїх національних інтересів, не обмежуючись національними кордонами[13]. Окрім національних критичних інфраструктур, розглядаються зарубіжні об'єкти, безпека яких має важливе значення для тієї чи іншої держави. На підтвердження цього можна згадати, зокрема, той факт, що на веб-сайті WikiLeaks був оприлюднений список компаній і установ, який нібито був створений дипломатичними місіями на запит Державного департаменту США у 2009 р. До цього списку потрапили такі величезні об'єкти інфраструктури як Панамський канал, шахти та мінеральні ресурси в Африці (зокрема шахти з видобутку кобальту в Демократичній Республіці Конго), Азії та Південній Америці, підводні нафто- та газопроводи, трансатлантичні кабелі, морські порти в Китаї та Японії, французькі медичні та фармацевтичні компанії та вантажні термінали, заводи з нафтопереробки на Близькому Сході, об'єкти гідроенергетики в Канаді, мережа транзитних газопроводів, яка проходить через Надим у російському Сибіру, а також багато менш масштабних об'єктів, такі як, наприклад, датський завод з виробництва інсуліну та фабрика, яка виробляє антидот від зміїної отрути в Австралії. В Європі серед таких об'єктів названі: завод у місті Людвігшафен німецького гіганта хімічної промисловості BASF (найбільший у світі інтегрований комплекс хімічної промисловості); завод у місті Ерланген

[12] *European* programme for critical infrastructure protection (COM/2006/786 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[13] *Morag, N.,* Does Homeland Security Exist Outside the United States?. – Homeland Security Affairs. – Vol. 7. – 2011. – 27 – 31.

компанії Siemens AG (виготовлення хімічних речовин).

Тому природно, враховуючи сучасні геополітичні реалії, що, наприклад, газотранспортна система України може розглядатися європейськими та трансатлантичними партнерами як елемент критичної інфраструктури, що має загальноєвропейське значення. Цей аспект, безперечно, заслуговує на увагу при розгляді проблем захисту національної критичної інфраструктури, вирішенні питання власності на об'єкти національної газотранспортної системи, що матиме безпосередній вплив на процес формування ціни на газ для України.

Для України може бути корисним досвід імплементації концепції захисту критичної інфраструктури в законодавствах деяких східноєвропейських країн. Наприклад, в нормативно-правовій базі Республіки Польща введено термін «захист критичної інфраструктури», під яким розуміються всі «зусилля, спрямовані на забезпечення функціональності, неперервності та цілісності критично важливих об'єктів інфраструктури в цілях запобігання загрозам, ризикам і вразливості та обмеження, а також нейтралізації їх наслідків і швидкого оновлення інфраструктури у випадку відмов, атак та інших випадків, що порушують її належне функціонування»[14].

Подібна ж ситуація спостерігається у нормативно-правовій базі Словацької Республіки, де в 2007 р. уряд ухвалив «Концепцію критичної інфраструктури в Словацькій Республіці, її захисту та оборони»[15]. На основі даної концепції в 2008 р. була розроблена «Національна програма захисту та оборони критичної інфраструктури»[16]. Проте обидва документи надають лише загальні (концептуальні) характеристики стратегії захисту критичної

[14] *Act* of 26 April 2007 on Crisis Management. – Пер. англ. мовою [Електронний ресурс]. – Веб-сайт Урядового центру з питань безпеки, Республіки Польщі. – Режим доступу: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf

[15] *Koncepcia* kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany [Електронний ресурс]. – Веб-сайт Міністерства внутрішніх справ Республіки Словаччина. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691.

[16] *Národný* program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [Електронний ресурс]. – Веб-сайт Міністерства внутрішніх справ Республіки Словаччина. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10692

інфраструктури в Словацькій Республіці, але не надають детальний опис заходів з її здійснення.

Інша країна-сусід України – Угорщина, будучі країною-членом ЄС з 2004 р., рішенням уряду в 2008 р. ввела в дію Програму захисту національної критичної інфраструктури[17], згідно з якою в Угорщині визначено 11 секторів критичної інфраструктури.

В законодавстві Хорватії термін «критична інфраструктура» визначено таким чином: «діяльність, мережі, послуги, матеріальні блага та інформаційні технології, вихід з ладу або знищення яких значно би вплинуло на здоров'я та безпеку громадян, або на діяльність державної влади»[18]. Термін було введено у в дію законодавчим актом, призначеним для регулювання охоронної діяльності в цій країні.

В законодавстві Республіки Болгарії визначення «критична інфраструктура» надано в Законі «Про управління в умовах кризи» (на мові оригіналу, болгарською: «Закон за управление на кризи»)[19], введений в дію в березні 2005 р. Проте даний закон втратив чинність вже у травні 2009 р[20]. Саме визначення терміну було аналогічним прийнятому в законодавстві США.

Ситуація, подібна до української, спостерігається в Румунії, де існує біля 15 переліків об'єктів, що відповідають терміну критична інфраструктура, але вони рознесені по різноманітним законодавчим актам[21].

Концепція захисту критичної інфраструктури достатньо активно впроваджується і розвивається в Російській Федерації (РФ). На сьогодні ця

---

[17] *Special* underground facilities (UGF-s) serving for the critical infrastructure [Електронний ресурс]. – New challenges in the field of military science international scientific conference, 7-8 november, 2006. – Режим доступу: http://hadmernok.hu/kulonszamok/newchallenges/szalai.html#12

[18] *Zakon* o privatnoj zaštiti [Електронний ресурс]. – Zakon HR. – Режим доступу: http://www.zakon.hr/z/291/Zakon-o-privatnoj-za%20titi

[19] *Tagarev T., Pavlov N.*, Planning Measures and Capabilities for Protection of Critical Infrastructures // Information & security. – 2007. – Vol. 22. - P. 38 – 48. [Електронний ресурс]. – Режим доступу: http://infosec.procon.bg/v22/Tagarev_Pavlov_CIP.pdf

[20] *Закон* за управление на кризи [Електронний ресурс]. – Българският правен портал. – Режим доступу: http://www.lex.bg/forum/viewtopic.php?t=38583

[21] *L.Muresan, S.Caceu,* Critical infrastructures protection a Romanian perspective [Електронний ресурс]. – Risk and security in the global world. Summer school, 2010. – Режим доступу: http://bsu.ase.ro/oldbsu/anexe/lectures2010/

концепція, є складовим елементом внутрішньої та зовнішньої політики РФ в безпековій сфері, а в законодавстві визначено термін «критично важливі об'єкти інфраструктури» – це «об'єкти, порушення (або припинення) функціонування яких призводить до втрати управління, руйнуванню інфраструктури, незворотнім негативним змінам (або руйнуванню) економіки країни, суб'єкту або адміністративно-територіальної одиниці, або суттєвому погіршенню безпеки життєдіяльності населення, що мешкає на цих територіях, на тривалий період часу»[22].

Початком цілеспрямованої роботи в даній галузі можна вважати рішення спільного засідання Ради Безпеки Російської Федерації і президії Державної ради Російської Федерації (13 листопада 2003 р.), у відповідності до якого було заплановано і виконано комплекс заходів, спрямованих на забезпечення безпеки населення і захищеності потенційно небезпечних об'єктів від загроз техногенного, природного характеру та терористичних актів. З огляду на те, що у зонах можливого впливу вражаючих факторів при аваріях на критично важливих і потенційно небезпечних об'єктах мешкає понад 90 мільйонів осіб (60 відсотків населення РФ), була прийнята Федеральна цільова програма «Зниження ризиків та пом'якшення наслідків надзвичайних ситуацій природного та техногенного характеру в Російській Федерації». В рамках даної програми був створений і успішно функціонує Національний центр управління в кризових ситуаціях МНС РФ та Загальноросійська комплексна система інформування та оповіщення населення в місцях масового перебування.

До нормативно-законодавчих документів, які регламентують захист критично важливих об'єктів в РФ слід віднести: «Основи державної політики в галузі забезпечення безпеки населення Російської Федерації і захищеності критично важливих та потенційно небезпечних об'єктів від загроз

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

техногенного, природного характеру та терористичних актів»[23], «Перелік критично важливих об’єктів Російської Федерації», а також «Концепцію Федеральної системи моніторингу критично важливих, потенційно небезпечних об’єктів та вантажів»[24].

Перший з названих документів розвиває та конкретизує основні положення Стратегії національної безпеки Російської Федерації до 2020 року, що стосуються забезпечення безпеки населення і захищеності критично важливих і потенційно небезпечних об’єктів від загроз різного характеру.

В останньому документі формулюються основи створення Федеральної системи моніторингу критично важливих об'єктів та/або потенційно небезпечних об’єктів інфраструктури РФ та небезпечних вантажів як функціональної складової єдиної системи попередження і ліквідації надзвичайних ситуацій. Створення системи моніторингу обумовлено необхідністю вдосконалення організації робіт в галузі своєчасного виявлення та попередження загроз техногенного та природного характеру, а також викликано проявами тероризму по відношенню до критично важливих об’єктів у РФ. Система моніторингу створюється для федеральних органів виконавчої влади, органів виконавчої влади суб’єктів РФ, органів місцевого самоврядування, які відповідають за питання функціонування критично важливих та/або потенційно небезпечних об’єктів інфраструктури РФ.

В Стратегії національної безпеки Російської Федерації до 2020 року[25] вказується на необхідність подолання технологічного відставання РФ в галузі

---

[23] *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 (утв. Президентом РФ 15 ноября 2011 г. № Пр-3400) [Електронний ресурс]. – http://www.garant.ru/products/ipo/prime/doc/70041358/

[24] *Распоряжение* Правительства Российской Федерации от 27 августа 2005 г. №1314-р «Концепция Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов» [Електронний ресурс]. – http://www.garant.ru/hotlaw/federal/124379/

[25] *Указ* Президента Российской Федерации от 12 мая 2009 г. № 537 «Об утверждении Стратегии национальной безопасности Российской Федерации до 2020 года» [Електронний ресурс]. – http://www.scrf.gov.ru/news/436.html

інформатизації, телекомунікації та зв’язку, забезпечення інформаційної безпеки критично важливих об’єктів. Загрози інформаційній безпеці передбачається запобігати шляхом удосконалення безпеки функціонування інформаційних та телекомунікаційних систем критично важливих об’єктів та об’єктів підвищеної небезпеки в РФ, підвищення захищеності корпоративних та індивідуальних інформаційних систем, створення єдиної інформаційно-телекомунікаційної підтримки в системі забезпечення національної безпеки.

З метою реалізації основних положень Стратегії національної безпеки Російської Федерації до 2020 року, відповідно до якої одним із шляхів запобігання загрозам інформаційній безпеці Російської Федерації є вдосконалення безпеки функціонування інформаційних і телекомунікаційних систем критично важливих об’єктів інфраструктури та об’єктів підвищеної небезпеки, Радою безпеки РФ було розроблено Основні напрями державної політики в галузі забезпечення безпеки автоматизованих систем управління виробничими і технологічними процесами критично важливих об’єктів інфраструктури Російської Федерації (липень 2012 р.). В документі йдеться про єдину державну систему виявлення і попередження комп’ютерних атак на критичну інформаційну інфраструктуру та оцінки рівня реальної захищеності її елементів, що включає сили та засоби виявлення і попередження комп’ютерних атак, а також органи управління різних рівнів, до повноваження яких віднесено питання забезпечення безпеки автоматизованих систем управління критично важливих об’єктів та інших елементів критичної інформаційної інфраструктури.

В названому документі Ради безпеки РФ визнається, зокрема, наявність практики здійснення іноземними фірмами технічного обслуговування і віддаленого налаштування автоматизованих систем управління критично важливих об’єктів в цілому або їх складових частин, а також телекомунікаційного обладнання, що входить до складу критичної інформаційної інфраструктури, а також прагнення організацій-розробників програмного забезпечення автоматизованих систем управління до зниження

витрат і, як наслідок, використання типових рішень та запозиченого програмного забезпечення.

Особлива увага в РФ приділяється безпеці критично важливих об’єктів, стабільне функціонування яких визначає економічне зростання країни. В жовтні 2011 р. було введено в дію Федеральний закон «Про безпеку паливно-енергетичного комплексу»[26], положення якого спрямовані на недопущення вчинення терористичних та інших зловмисних діянь, спрямованих на завдання шкоди об’єктам паливно-енергетичного комплексу.

Цей документ є важливим тому, що в ньому виокремлюються такі крупномасштабні лінійні об’єкти як трубопроводи та магістральні ЛЕП, які мають суттєві особливості щодо організації охорони.

Термін «критично важливі об’єкти» застосовуються і в оновлених підходах до функціонування цивільного захисту в Російській Федерації. Зокрема, в стратегічному документі щодо розвитку цивільної оборони критично важливі об’єкти згадуються у зв’язку із[27]:

– визначенням терористичних загроз серед основних факторів, що визначають напрями єдиної державної політики Російської Федерації в галузі цивільної оборони;

– удосконаленням методів і способів захисту населення, матеріальних і культурних цінностей від небезпек, що виникають при веденні військових дій або внаслідок цих дій, а також при виникненні надзвичайних ситуацій;

– збереженням об’єктів, необхідних для сталого функціонування економіки та виживання населення у воєнний час.

Аналізуючи тенденції розвитку законодавчої бази РФ щодо захисту критично важливих об’єктів, слід наголосити на тому, що введення категорії «критично важливі об’єкти» не повинно бути зведено до створення ще

---

[26] *Федеральный* закон Российской Федерации от 21 июля 2011 г. №256-ФЗ «О безопасности объектов топливно-энергетического комплекса» – ИПС «Закон». [Електронний ресурс]. – Режим доступу: http://ntc.duma.gov.ru/

[27] *Основы* единой государственной политики Российской Федерации в области гражданской обороны на период до 2020 года (утв. Президентом РФ 3 сентября 2011 г. № Пр-2613) http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=125214

одного різновиду, переліку об’єктів, до яких здійснюються функції нагляду та контролю з боку уповноважених органів.

Окрім створення нормативно-правової основи для функціонування систем захисту критично важливих об’єктів в РФ, активно здійснюються та фінансуються наукові дослідження в галузі розвитку методів оцінки зовнішніх і внутрішніх небезпечних для критично важливих об’єктів процесів, аналізу ризику та вразливості систем фізичного захисту цих об’єктів[28], а також створення ефективної системи підготовки керівних кадрів та спеціалістів в даній галузі[29].

2. Основні складники досягнення мети та цілей стратегії захисту критичної інфраструктури

Забезпечення безпеки критичної інфраструктури є складною проблемою для кожної держави і, спираючись на думку американського дослідника Теда Льюіса[30], до головних викликів на цьому напрямі слід віднести:

– величезність кожного з секторів критичної інфраструктури та її самої в цілому;

– управління безпекою за умов взаємозалежності діяльності урядових органів, державного та приватного секторів, а також регулюючих та економічних факторів;

– обмін інформацією, який вже на стадії збору та співставлення необхідних даних виявляється величезною проблемою, оскільки державні органи являють собою, здебільшого вертикально-орієнтовні структури, які переважно накопичують інформацію, у той час, як елементи критичної інфраструктури розпорошені між державою та великою кількістю приватних

[28] *Идентификация* определяющих параметров угроз, уязвимости и защищенности критически важных объектов по отношению к превалирующим угрозам природного, техногенного и террористического характера / Н.А. Махутов и др. // Проблемы безопасности и чрезвычайных ситуаций. - 2008. - N 2. - С. 34-41.
[29] *Разработка* программ подготовки и переподготовки специалистов по системным исследованиям проблем безопасности, снижения рисков чрезвычайных ситуаций и защищенности критически важных объектов / Я.Д. Вишняков и др. // Проблемы безопасности и чрезвычайных ситуаций. – 2007. – №2. – С. 87 – 102.
[30] *Lewis T.G.,* Critical infrastructure protection in homeland security: defending a networked nation. – New Jersey: John Wiley & Sons, 2006. – 474 p.

компаній;

– взаємозалежність елементів та секторів критичної інфраструктури внаслідок притаманним їм комплексних різнорівневих взаємодій та взаємозв'язків.

Крім того, враховуючи, що більшість систем критичної інфраструктури мають мережеву архітектуру, Т. Льюіс вважає, що захищати, у першу чергу, слід ключові «вузли» цих систем[31]. Саме у такий спосіб з'являється можливість слідувати так званому «правилу 80-20 %», коли 80 % ресурсів мають витрачатися на 20 % території країни, а також використовувати теорію мереж для організаційних і фізичних структур, призначених для організації захисту критичної інфраструктури.

Аналізуючи «вибоїни» та можливі «об'їзди» на шляху до побудови ефективної політики захисту критичної інфраструктури, Тед Льюіс та Руді Даркін звертають увагу на такі проблеми[32]:

– розподіл повноважень із захисту критичної інфраструктури між федеральною та місцевою (влада штату) владою;

– відсутність загальної методологічної бази для визначення ризику та вразливості об'єктів;

– необхідність активної участі компаній-операторів (власників) у забезпеченні захисту критичної інфраструктури.

Дослідження механізмів захисту критично важливих для життєдіяльності держави об'єктів, систем та мереж (критичної інфраструктури), включає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися в якості критичної інфраструктури. Як показує досвід розвинутих країн, в яких функціонують нормативно-правові та організаційні механізми захисту критичної інфраструктури, здійснення етапу ідентифікації дозволяє систематизувати множину елементів критичної

---

[31] *Lewis T.G.,* Critical infrastructure protection in homeland security: defending a networked nation. – New Jersey: John Wiley & Sons, 2006. – 474 p.

[32] *Potholes* and Detours in the Road to Critical Infrastructure Protection Policy / T.G. Lewis, R.Darken // Homeland Security Affairs. – 2005. – Vol.1, Issue 2.

інфраструктури, визначити основні її сектори (галузі).

2.1. Оцінка загроз критичній інфраструктурі. Серед загроз критичній інфраструктурі називають: пандемії, промислові аварії, терористичну та злочинну діяльність, кібератаки, стихійні лиха тощо[33]. Держава повинна забезпечувати захист об'єктів критичної інфраструктури від усіх суттєвих загроз, які можна віднести до трьох категорій: техногенні, природного характеру та соціально-політичні.

У підходах до захисту об'єктів критичної інфраструктури поступово відбувалися зміни під впливом тих чи інших подій. Найважливішою можна вважати тенденцію, яка проявилась у США після урагану Катріна (наприкінці серпня 2005 р.), визнаного найбільш руйнівним в історії країни (територія, що постраждала від стихійного лиха, становила близько 200 тис. кв. км – за розміром приблизно третина території України). В результаті аналізу подій у планах захисту критичної інфраструктури значно більше уваги стали приділяти підходу до оцінки ризиків, що враховує увесь комплекс загроз (англ. all-hazard approach).

Серед техногенних загроз особлива увага приділяється спробам втручання в роботу автоматизованих систем управління технологічним процесом на підприємствах та об'єктах інфраструктури. Хоча ще не повідомлялося про факти матеріальних ушкоджень (руйнувань) внаслідок кібератак на критичну інфраструктуру, однак були зафіксовані численні (за оцінками експертів – на 45 тис. об'єктах по всьому світу) випадки зараження автоматизованих систем управління технологічним процесом (перепрограмування контролерів) вірусом Stuxnet[34], а серед останніх подій – спроби втручання в роботу автоматизованих систем управління об'єктів газотранспортних систем США[35].

Кібербезпека залишається пріоритетним напрямком для Адміністрації

---

[33] *Critical* Infrastructure Resilience Strategy – Australian Government [Електронний ресурс]. – Режим доступу: http://www.tisn.gov.au/

[34] *Stuxnet* Dossier // Symantec Security Response. – February. – 2011. – 68 p.

[35] *ICS-CERT* Monthly Monitor – April. – 2012 [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf

Президента Обами[36]. Для забезпечення безпеки найбільш життєво важливих систем, уряд США надає громадськості та приватним компаніям (установам) можливість отримувати оперативну та ефективну допомогу з кібербезпеки.

В Сполучених Штатах Міністерство оборони виступає головним ідеологом розробки не тільки технічних засобів розвідки, а й розвитку інформаційних і телекомунікаційних технологій, ключовим елементом якого є застосування глибоко-ешелонованого захисту (англ., defense-in-depth). Цей підхід передбачає використання інформаційних систем, що складаються з багатошарових систем безпеки і процедур, які використовують активні та пасивні заходи щодо захисту інформаційних ресурсів і запобігають неправомірному доступу до інформації. Захист національної інформаційної інфраструктури віднесено також до компетенції «розвідувального співтовариства» США, яке займається збиранням відповідної інформації щодо усунення загроз та попередженням злочинів, спрямованих проти національних інформаційних систем.

Серед технічних засобів захисту, які нині використовуються в США необхідно виділити концептуальну модель ешелонованої багатошарової системи інформаційної безпеки (безпеки інформації), стандарту ISO/IEC 15408, яка містить в собі набір компонентів, що реалізують функції моніторингу, захисту й адаптації інформаційних ресурсів, а разом – дозволяють поетапно запобігти проникненню, визначити факт порушення, локалізувати об’єкт впливу, нейтралізувати і видворити порушника, відновити втрачені функції системи.

Зважаючи на зростання негативних наслідків для держави, які завдаються кібер-атаками на інформаційну інфраструктуру органів державної влади, та небезпеки, пов’язані з можливими атаками на промислові об’єкти, все частіше лунають заклики посилити відповідальність за вчинення кібер-злочинів. Так, один з членів Ради Федерації РФ, нещодавно запропонував

[36] *Presidential* Proclamation – Critical Infrastructure Protection Month [Електронний ресурс]. – The White House, November 30, 2011. – Режим доступу: http://www.whitehouse.gov/the-press-office/2011/11/30/presidential-proclamation-critical-infrastructure-protection-month-2011

прирівняти злам державних веб-сайтів до захоплення органів влади, обґрунтовуючи свою пропозицію тим, що через такі сайти надаються різного роду держпослуги[37].

Слід відзначити, що терористичні акти, скоєні у вересні 2001 р. у США, березні 2004 р. в Іспанії та у липні 2005 р. у Великій Британії відіграли роль прискорювача процесу впровадження концепції критичної інфраструктури не тільки у Сполучених Штатах, але і в ЄС.

Серед останніх терористичних актів, які були спрямовані на руйнування інфраструктурних мереж, привернули увагу вибухи, скоєні в Туреччині. Протягом двох тижнів в липні-серпні 2012 р. було здійснено два вибухи на турецьких ділянках нафтопроводу Кіркук-Джейхан, через який транспортується іракська нафта до середземноморських портів. Перший вибух було здійснено 21 липня, а другий – 6 серпня в провінції Мардін. В результаті першого теракту одну з двох паралельних труб нафтопроводу було сильно пошкоджено, а функціонування іншої з міркувань безпеки призупинено. В здійсненні терактів підозрюють бойовиків сепаратистського групування «Робітнича партія Курдистану», організації, яка визнана ООН та ЄС терористичною[38].

На жаль, загроза вчинення терактів залишається вкрай актуальною і для європейських країн, про що свідчить, зокрема, скоєний 22 червня 2011 р. в Норвегії подвійний теракт: вибух в урядовому кварталі (радіокерована бомба потужністю близько 500 кг у тротиловому еквіваленті була виготовлена із сільськогосподарських добрив на основі аміачної селітри та дизельного палива) забрав життя 8 осіб та спричинив поранення 92 особам (15 тяжкі), постраждали найближчі будівлі (в т.ч. міністерство нафтової промисловості), а в результаті злочину, вчиненого терористом на острові Утейа, загинули 69 осіб (учасники молодіжного літнього табору, що організовує щорічно правляча Робітнича партія Норвегії).

---

[37] *Информационное* агентство «Оружие России» [Електронний ресурс]. – Режим доступу: http://www.arms-expo.ru/055057052124050056053052056.html

[38] *В Турции* взорван участок нефтепровода [Електронний ресурс]. – Коммерсант.ua. – Режим доступу: http://www.kommersant.ua/news/1996486

Ще один теракт – вибух у мінському метрополітені (скоєний 11 березня 2011 р.) демонструє, наскільки вразливими є об'єкти масового скупчення людей (у США вони віднесені до критичної інфраструктури). В результаті вибуху загинули 11 осіб, понад 100 осіб постраждали. До безпеки таких об'єктів як метрополітен, стадіони, виставкові центри, вищі навчальні заклади висуваються підвищені вимоги з безпеки, проте забезпечити їх стовідсоткову захищеність від терористичних загроз неможливо. Теракт у мінському метрополітені привертає увагу ще й тим, що на відміну від Великої Британії та Іспанії, Білорусь не бере участь в операціях проти «світового» тероризму в Афганістані, у країні відсутні сепаратистські чи екстремістські організації, але це не гарантувало уникнення від терактів.

В серпні 2012 р. в Сполучених Штатах була розкрита терористична організація з найменуванням FEAR (абревіатура від «Forever Enduring Always Ready» (англ., «Вічно стійкий, завжди готовий»), яка планувала скоєння низки терактів в штаті Джорджія та в столиці США, Вашингтоні[39]. Члени цієї організації планували вибухи автомобілів державних діячів та суддів, вибухи в місцях масового скупчення людей та, навіть, вбивство Президента країни.

Що стосується України, то лише протягом 2011 р. сім злочинів було класифіковано як терористичний акт[40] (п. 3.8, с. 191 – вчинення або підготовка підриву саморобного вибухового пристрою). Гучного резонансу набула серія вибухів, вчинених у Дніпропетровську 27 квітня 2012 р. (постраждало 29 осіб). Прокурором Дніпропетровської області порушено кримінальну справу за ч. 2 ст. 258 КК (терористичний акт).

Терористичні акти завжди мають значний резонанс. Але при цьому не слід забувати про те, що техногенні аварії можуть часто мати наслідки важчі, ніж у випадку деяких терактів. Наприклад, вибух природного газу в

---

[39] *'Anarchists'* accused of murder; broader plot against government [Електронний ресурс]. – CNN. – Режим доступу: http://edition.cnn.com/2012/08/28/justice/georgia-soldiers-plot/index.html

[40] *Національна* доповідь про стан техногенної та природної безпеки в Україні у 2011 році / Міністерство з надзвичайних ситуацій [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/nasdopovid2011.htm

10-поверховому будинку, що стався 13 жовтня 2007 р. в тому ж Дніпропетровську, забрав життя 23 людей (в т.ч. 7 дітей). Кримінальну справу було порушено за ст. 367 КК (службова халатність), а на лаві підсудних опинилися три представника ВАТ «Дніпрогаз» – генеральний директор, його перший заступник і головний інженер.

Проблема створення ефективної системи фізичного захисту великомасштабних (за площею, протяжністю тощо) об'єктів (підприємств, нафто- та газопроводів, заповідників) залишається не розв'язаною не тільки в Україні а й в інших країнах. Наприклад, у жовтні 2011 року в Німеччині була здійснена спроба підпалу (вибуху) на залізниці: 18 саморобних вибухових пристроїв (ємності з підпалювальною суміщу) були знайдені у комунікаційних шахтах, в яких прокладені кабелі, що з'єднують центральний комп'ютер зі стрілками та семафорами. Внаслідок було призупинено рух понад 200 електричок. Якби теракт відбувся – наслідки були б жахливими.

Цей приклад свідчить про об'єктивну вразливість великомасштабних систем, через їх природу (територіально-просторову розтягненість) та необхідність забезпечення всіх можливих заходів і засобів забезпечення безпеки, наприклад, дублювання комунікаційних каналів, та фізичного захисту, наприклад, відеоспостереження.

Суттєвою частиною аналізу та оцінки загроз є вивчення взаємозв'язку між елементами критичної інфраструктури як усередині секторів, так і між елементами критичної інфраструктури різних секторів. Одним із прикладів реалізації такого взаємозв'язку є каскадна аварія, що виникла внаслідок відмови мережі енергопостачання в північно-східних штатах США та східних провінціях Канади у 2003 р.[41]. Внаслідок даної аварії: 10 млн осіб у провінції Онтаріо та 45 млн осіб, що мешкають у 8 штатах США, зіткнулися з перебоями в забезпеченні електроенергією, водою, зв'язком, послугами муніципального транспорту; зупинилися виробничі лінії на підприємствах;

[41] *Final* Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations / U.S.-Canada Power System Outage Task Force, April, 2004 [Електронний ресурс]. – Режим доступу: https://reports.energy.gov/BlackoutFinal-Web.pdf

зросла кількість випадків хуліганства та здійснення пограбувань; спостерігалися відмови систем контролю за перетином державного кордону; систем освітлення злітно-посадкових смуг аеродромів; систем фізичного захисту об’єктів.

Інший приклад крупномасштабної аварії, що привертає увагу з огляду на каскадні наслідки, – це події з масовим відключення електроживлення в Індії, які відбулися наприкінці липня 2012 р. Перша аварія викликала майже повний колапс на півночі країни (30 липня), охопивши дев’ять регіонів з загальною чисельністю населення 390 млн осіб. Відновити електроживлення для життєво важливої інфраструктури (аеропорти, залізниця, метро) вдалося тільки після 5 годин після відключення. Повне відновлення електроживлення було досягнуто через 16,5 годин після аварії. Повторна аварія (31 липня) охопила ще більший регіон (окрім північних регіонів були охоплені частини східних та північно-східних регіонів Індії). Енергетична корпорація Індії (Power Grid Corporation of India Ltd) відновила енергоживлення життєво важливих об’єктів після 2,5 годин, в той же час населенню (в т.ч. 16,5 млн осіб, що мешкають в столиці – м. Делі) довелося чекати понад 8,5 годин. Повне відновлення функціонування енергетичної мережі було досягнуто лише 1 серпня (через 32,5 години після повторної аварії).

За оцінками аналітиків під час аварії біля 600 млн осіб були позбавлені електропостачання та можливості користуватися пасажирським електротранспортом. Вже за попередніми оцінками наслідки даних аварій для промисловості та підприємництва складають величину в сотні мільйонів дол. США. Також, відмічається, що інформування населення про інцидент не було здійснено на належному рівні як з боку державних відомств, так й Енергетичної корпорації Індії[42].

Аварія мала й політичні наслідки – було призначено нового керівника Міністерства енергетики Індії.

---

[42] *Blackout* a wake-up call for India [Електронний ресурс]. – World nuclear news. – Режим доступу: http://www.world-nuclear-news.org/

За словами генерального директора Конфедерації промисловців Індії Чандраджіт Банерджі (Chandrajit Banerjee): «для Індії як однієї з найбільш швидко зростаючих економік світу, країни, в якій проживає шоста частина світового населення, імперативом має стати те, що базова інфраструктура повинна відповідати намаганням держави». В то же час в Індії розподільні компанії постійно борються з боржниками та стикаються зі значними (в середньому по країні – 27 %) втратами електроенергії.

На думку експертів Центру стратегічних та міжнародних досліджень (Вашингтон, США), важко справитися з недоліками енергетичної інфраструктури, які на сьогодні присутні в Індії, не розв'язавши складні політичні проблеми, які простягаються від питання права на земельну власність до непосильних для держави соціальних субсидій[43].

Цікавим є аналіз причин даної аварії. Експерти вказують на погодні умови (засуху викликану слабким сезоном мусонів – приблизно на 20 % менше за середні показники), високу температуру повітря. Відповідно, підвищилося використання кліматичного обладнання (кондиціонерів) в офісах та житлових будинках, а також використання систем іригації (насосів для накачування води для поливів) сільськогосподарських посівів. В той же час відсутність дощів спричинила зниження рівня води в водоймах та, відповідно, зниження потужності гідроенергетичних станцій.

Наслідки руйнівних впливів на критичну інфраструктуру можуть виникати далеко за межами її географічно-територіального розміщення. Так, після здійснення терактів у вересні 2001 р. у США попит на пасажирські авіаперевезення в Європі впав на 15-30 %, відповідно, втрати авіакомпаній за останній квартал 2001 р. досягли 3,6 млрд євро, а 17 тис. осіб, тобто близько 5 % працівників європейських авіакомпаній, опинилися під загрозою звільнення[44].

Необхідно також відмітити, що розбудова критичної інфраструктури

[43] *India* in the dark [Електронний ресурс]. – Centre for Strategic & International Studies, Washington. – Режим доступу: http://csis.org/publication/india-dark

[44] *The repercussions* of the terrorist attacks in the United States on the air transport industry (COM/2001/574 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

може викликати міжнародні суперечності. Показовим є приклад протидії впровадженню європейської супутникової системи позиціонування Галілео з боку урядових кіл Сполучених Штатів (заступник міністра оборони США Пол Вольфовіц у грудні 2001 р. надіслав лист 15 міністрам оборони країн-членів ЄС, у якому наводив аргументи проти створення Галілео), які усвідомлювали, що Галілео створюється як альтернатива, що витіснить американську Глобальну систему позиціонування[45].

2.2. Ідентифікація елементів критичної інфраструктури. Розробка методології ідентифікації об'єктів критичної інфраструктури потребує окремого дослідження. Світовий досвід показує, що навіть для такого потужного відомства як Міністерство внутрішньої безпеки США завдання розробки єдиної методології ідентифікації об'єктів, систем і сервісів, які є критичними на національному рівні, а також створення всеосяжної бази даних для ведення їх реєстру, виявилося складним[46].

Його складність полягає у значній неоднорідності самих об'єктів і систем, що належать до різних секторів критичної інфраструктури, їх величезній кількості, а також необхідності враховувати різноманітні характеристики об'єктів та систем з огляду на всі типи загроз. Зокрема, в США остаточний список об'єктів, які розглядалися як критичні на національному рівні, містив 1700 позицій з бази даних, в якій було внесено близько 33 тис. об'єктів (запропоновані як критичні на регіональному або місцевому рівнях державними агентствами у відповідних секторах критичної інфраструктури)[47].

На території РФ функціонує біля 5 тис. критично важливих об'єктів (КВО), порушення (або припинення) функціонування яких призведе до втрати управління, руйнування інфраструктури, незворотних негативних змін в економіці країни або адміністративно-територіальної одиниці,

---

[45] *Tanner, J. C.*, Galileo is go, despite Pentagon pressure - First Mile - Brief Article // Telecom Asia, 31 May, 2012 [Електронний ресурс]. – Режим доступу: http://findarticles.com/p/articles/mi_m0FGI/is_5_13/ai_86827056/

[46] *Critical* infrastructure and key assets: definition and identification. - Congressional research service, RL32631, October, 2004. – 19 p.

[47] Там само.

суттєвого погіршення безпеки життєдіяльності населення, що проживає на цих територіях, на тривалий період часу[48].

Критична інфраструктура містить величезну кількість об'єктів, які прийнято групувати за секторами. Кількість секторів та принцип групування різняться в залежності від країни (див. табл. 1). В США визначено 18 секторів: аграрний та продовольчий, банківська система та фінанси, хімічна промисловість, комерційні об'єкти (музеї, виставки та інші місця масового зібрання людей), критичне виробництво, дамби, оборонно-промисловий комплекс, сервіси допомоги (пожежна, медична швидка допомога, т.ін.) енергетика, урядові об'єкти, охорона здоров'я, інформаційні технології, зв'язок, національні пам'ятки та символи, пошта та доставка, транспортні системи, водопостачання. В Канаді до критичної інфраструктури віднесено 10 секторів: харчова промисловість, фінанси, промисловість, безпека, енергетика, уряд, охорона здоров'я, інформаційні технології та зв'язок, транспорт, водопостачання.

[48] *В Москве* состоится круглый стол на тему «Комплексные решения противодействия терроризму на критически важных объектах» [Електронний ресурс]. – Новости ВПК. – Режим доступу: http://vpk.name [Електронний ресурс]. – Информационное агентство «Оружие России». – Режим доступу: http://www.arms-expo.ru

Таблиця 1

Порівняльна таблиця: сектори критичної інфраструктури

Держава / Сектор критичної інфраструктури	Австралія	Австрія [49]	Велика Британія [50]	Канада	Італія	Нідерланди	Німеччина	Нова Зеландія	Норвегія [51][52]	Польща	РФ	США	Фінляндія	Франція	Швеція
Банки та фінанси	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Водопостачання	X	X	X	X	X	X	X		X	X		X	X	X	
Дамби												X			
Енергетика	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Комунальні мережі	X	X					X		X				X		
Національні символи	X			X								X			
Небезпечні матеріали (ХБРЯ)			X	X						X		X			
Оборонно-промисловий комплекс	X			X							X	X	X	X	
Органи виконавчої влади	X		X	X		X	X	X	X	X		X			X
Органи правосуддя			X			X	X	X				X			
Охорона здоров'я	X	X	X	X	X	X	X		X	X		X	X	X	
Паливно-енергетичний комплекс	X		X	X	X	X	X	X	X	X	X	X			
Поштові служби		X										X			
Сільське господарство	X		X	X		X	X			X		X	X		
Система управління повітряним рухом															X
Служби охорони громадського порядку	X	X	X	X	X	X			X					X	
Служби екстреної допомоги та реагування на надзвичайні ситуації	X	X	X	X	X		X	X	X			X			
Телекомунікації	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Транспорт	X	X	X	X	X	X		X	X	X	X	X	X	X	
Управління відходами	X		X	X	X				X						

Спроба визначити критичну інфраструктуру на рівні ЄС була здійснена в 2005 р., шляхом підготовки так званої «зеленої книги» щодо цієї проблеми. До списку об'єктів критичної інфраструктури відповідно до

[49] *Critical* Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29-30 Sept. 2003)

[50] *Sector* Resilience Plan for Critical Infrastructure 2010 [Електронний ресурс]. – Cabinet Office. – Режим доступу: http://www.cabinetoffice.gov.uk/resource-library/sector-resilience-plan-critical-infrastructure-2010

[51] *K.O. Nystuen, J.M. Hagen,* Critical Information Infrastructure Protection in Norway / Critical Infrastructure Protection (CIP) Workshop in September 2003 in Frankfurt

[52] *Protection* of critical infrastructures and critical societal functions in Norway / Report NOU 2006:6 Submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006

Зеленої книги ЄС[53] було включено 11 секторів: харчова промисловість, фінанси, хімічна промисловість, енергетика, охорона здоров'я, інформаційні технології та зв'язок, ядерна промисловість, транспорт, водопостачання, космічні дослідження, науково-дослідні установи. Але у найближчій перспективі Директивою ЄС[54] лише два сектори – енергетика і транспорт були визнані пріоритетними. До сектору енергетики були включені такі системи та об'єкти: електромережі та об'єкти із генерування та передачі електроенергії; нафтовидобувна та нафтопереробна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали зрідженого газу. До сектору транспорт віднесли такі його види та об'єкти: автодорожній транспорт; залізничний транспорт; авіаційний транспорт; річковий флот; океанічний і морський флот; порти.

Треба зазначити, що суттєвих відмінностей між списками секторів і переліками об'єктів, що визначаються критичною інфраструктурою в США, Канаді та ЄС майже немає. Лише, як вже згадувалося вище, в США до цих списків були внесені національні пам'ятки та символи, а також комерційні об'єкти (музеї, виставки та інші місця масового зібрання людей), натомість, в ЄС – науково-дослідні установи.

При визначенні елементів критичної інфраструктури (віднесенні об'єктів до критичної інфраструктури) будується ієрархія критеріїв, які охоплює такі основні групи: економічна безпека (значна частка продукції на ринку, велика кількість зайнятих співробітників, крупний платник податків); безпека життєдіяльності та здоров'я населення (забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню; недопущення техногенних аварій регіонального або національного масштабів); державна безпека і оборона (недопущення порушення керованості державою, зниження боєздатності збройних сил, розголошення таємної інформації); національна

[53] *Green paper* on a European programme for critical infrastructure protection (COM/2005/576 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[54] *Council* Directive 2008/114/EC «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

самоповага та імідж держави (збереження культурних цінностей, авторитету держави).

При визначенні потенційних елементів критичної інфраструктури враховують такі фактори та характеристики[55]:

– масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду) – міжнародний, національний, регіональний або територіальний;

– важкість можливих наслідків за такими показниками:

а) вплив на населення (число постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення);

б) економічна шкода (вплив на ВВП, розмір економічних втрат як прямих, так і непрямих);

в) екологічна шкода (вплив на населення та навколишнє природне середовище);

г) взаємозв'язок з іншими елементами критичної інфраструктури;

д) політичний ефект (втрата впевненості в дієздатності влади);

е) тривалість впливу (як саме і коли проявлятимуться збитки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

Ще одним прикладом такої категоризації є побудова критеріїв для визначення критично важливих об'єктів паливно-енергетичного комплексу РФ. При цьому враховується[56]:

– критична важливість об'єкту для інфраструктури та життєзабезпечення паливно-енергетичного комплексу;

– масштаби можливих соціально-економічних наслідків, що виникнуть внаслідок аварії на об'єкті;

– наявність критичних елементів, потенційно небезпечних ділянок та

[55] *Council* Directive 2008/114/EC «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

[56] *Федеральный* закон Российской Федерации от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» – ИПС «Закон». [Електронний ресурс]. – Режим доступу: http://ntc.duma.gov.ru/

уразливих місць на об’єкті.

Здійснення категоризації об’єктів критичної інфраструктури дозволяє встановити диференційовані вимоги до забезпечення безпеки цих об’єктів з врахуванням зокрема ступеня потенційної небезпеки здійснення акту незаконного втручання або теракту і його можливих наслідків.

З огляду на складний безпековий стан на Близькому Сході, значний інтерес являють принципи ідентифікації критичної інфраструктури в Ізраїлі.

Відповідно до підходів, що використовуються в Ізраїлі, при ідентифікації критичної інфраструктури, враховуються три ознаки для класифікації[57]:

– символічна значимість об’єктів;

– залежність ключових процесів життєзабезпечення суспільства від тої чи іншої інфраструктури;

– наявність складних взаємозв’язків та залежностей між інфраструктурами.

Згідно з таким підходом об’єкти культурної спадщини (музеї, архіви, культові споруди та інші пам’ятки) віднесені до числа об’єктів, які повинні бути захищені в першу чергу. Також до систем, що мають високе символічне значення ізраїльські експерти відносять ті, що забезпечують здатність держави контролювати ситуацію (сайти органів влади, центральні ЗМІ і т.п.), і втрата яких нанесе іміджу держави значної шкоди.

За другою ознакою до критичної інфраструктури відносять ЛЕП, системи водопостачання, каналізаційні мережі, загальні телекомунікаційні мережі, з якими пов’язані процеси управління інфраструктурами.

Відносно третьої ознаки, спеціалісти вказують на каскадні ефекти у відмовах інфраструктурних елементів. Слід зазначити, що в більшості випадків взаємозалежність інфраструктур не до кінця встановлена, і, відповідно, оцінка можливих наслідків не проведена.

---

[57] *Гриняев С.,* О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль [Електронний ресурс]. – Центр стратегических оценок и прогнозов. – Режим доступу: http://www.csef.ru/

2.3. Державно-приватне партнерство у сфері захисту критичної інфраструктури. У провідних країнах світу цьому питанню приділяють дуже велику увагу. Наприклад, у Національній стратегії захисту критичної інфраструктури Канади[58] зазначається, що відповідальність за забезпечення захисту критичної інфраструктури країни мають нести як усі державні органи, так і приватний сектор, а також усі канадці як члени канадського суспільства. Перед останніми поставлено завдання бути готовими до протистояння надзвичайним ситуаціям щонайменше упродовж перших 72 годин з моменту тієї чи іншої події.

Участь уряду Канади в державно-приватному партнерстві розглядається з точки зору[59]:

– надання операторам і власникам об'єктів і систем критичної інфраструктури вчасної й точної інформації щодо загроз і ризиків;

– забезпечення місцевої влади та операторів об'єктів і систем критичної інфраструктури планами реагування на надзвичайні ситуації;

– спільної роботи з усіма заінтересованими суб'єктами процесу, спрямованої на розробку пріоритетів та ключових заходів у кожному із секторів у сфері зменшення загроз критичній інфраструктурі.

Що стосується Європейської програми захисту критичної інфраструктури[60], то відповідальність за захист об'єктів критичної інфраструктури покладається як на їх власників (операторів), так і на уряд відповідної держави-члена ЄС.

2.4. Інформаційний обмін щодо загроз критичній інфраструктурі. Обмін інформацією про можливі загрози та наслідки їх реалізації, а також про уразливість критичної інфраструктури відіграє ключову роль у процесі аналізу загроз критичній інфраструктурі. Усвідомлюючи необхідність створення з цією метою мережі відповідної системи, Європейська Комісія

---

[58] *National Strategy* for Critical Infrastructure– Public Safety Canada [Електронний ресурс]. – Режим доступу [веб-сайт]: http://www.publicsafety.gc.ca/prg/em/ci/ntnl-eng.aspx

[59] *Там само.*

[60] *European* programme for critical infrastructure protection (COM/2006/786 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

прийняла рішення про створення Європейської інформаційної мережі попередження (англ., European Critical Infrastructure Warning Information Network, CIWIN).

Основним завданням CIWIN є створення засобів для координації дій та інформаційного обміну щодо критичної інфраструктури на загальноєвропейському рівні. CIWIN характеризується високими вимогами до забезпечення інформаційної безпеки, оскільки в мережі обробляється інформація, яка є чутливою з точки зору забезпечення безпеки об'єктів критичної інфраструктури. Вартість підтримки функціонування програмно-апаратної частини CIWIN щорічно складає понад 600 тис. євро[61].

Іншим прикладом реалізації подібного підходу є мережа з обміну інформацією (англ., Trusted Information Sharing Network, TISN), яка була створена урядом Австралії в квітні 2003 р. TISN функціонує як форум, на якому власники та оператори критичної інфраструктури можуть обмінюватися інформацією про загрози, вразливості та способи зниження ризиків. TISN складається із семи секторальних груп і двох експертно-консультативних груп, до яких входять представники уряду, власників та операторів критичної інфраструктури, органів місцевої влади.

3. Проблеми та перспективи імплементації світового досвіду захисту критичної інфраструктури в Україні

Де-факто в Україні присутні всі сектори та елементи, які прийнято відносити до критично важливих об'єктів та критичної інфраструктури. До них можна віднести складні великомасштабні промислові комплекси, наприклад, АЕС та об'єкти ядерної промисловості, підприємства хімічної промисловості, ГЕС, греблі/дамби, інформаційні та платіжні банківські системи, транспортні мережі, нафто- і газопроводи, мережі зв'язку та передачі інформації тощо.

---

[61] *Accompanying* document to the proposal for a Council decision on creating a Critical Infrastructure Warning Information Network (CIWIN) – Impact assessment (SEC/2008/2702). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

Базуючись на визначенні терміну «національні інтереси», що дається в Законі України «Про основи національної безпеки»[62], можна стверджувати, що критична інфраструктура включає ті матеріальні чи віртуальні (інформація, що зберігається в реєстрах, базах даних, інформаційних системах органів влади, або передається засобами Національної системи конфіденційного зв'язку) об'єкти та системи, від стабільного функціонування яких залежить можливість досягнення національних інтересів держави.

В національному законодавстві України діє низка нормативно-законодавчих актів, що встановлюють особливий характер функціонування об'єктів, які в світовій практиці прийнято відносити до критичної інфраструктури. Проте сам термін «критична інфраструктура», або його аналог – «критично важливі об'єкти», в законодавстві України відсутні.

Перше згадування про критичну інфраструктуру (з точки зору інформаційних мереж) в офіційних документах України прозвучало у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства[63], однак, на жаль, робота з впровадження цих рекомендацій, у т.ч. стосовно захисту критичної інфраструктури від широкого кола загроз, у подальшому припинилася.

В новій Стратегії національної безпеки[64] в четвертому розділі «Стратегічні цілі та основні завдання політики національної безпеки» серед ключових завдань політики національної безпеки у внутрішній сфері одним із шляхів зміцнення енергетичної безпеки (пункт 4.3.4.) названий: «дієвий захист критичної інфраструктури паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій», а одним із шляхів забезпечення інформаційної безпеки (пункт 4.3.8.): «забезпечення безпеки

---

[62] *Закон* України від 19.06.2003 № 964-IV «Про основи національної безпеки» // ВВР, 2003, №39, ст. 351 [Електронний ресурс]: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15

[63] *Про Рекомендації* парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради України // ВВР. – 2006. – № 15. – ст.131.

[64] *Указ* Президента України від 08.06.2012 № 389/2012 «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/389/2012

інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури». Проте сам термін «критична інфраструктура» так і не отримав свого визначення.

Оцінка важливості об'єктів з точки зору національної та державної безпеки в Україні здійснювалася за окремими типами загроз, наприклад кібер-загроз. Так, Указом Президента України від 10.12.2010 р. № 1119/2010 введено в дію рішення РНБО[65], в якому на Кабінет Міністрів України покладено завдання (п. 4.б абз. 3): «розробити за участю Служби безпеки України та затвердити перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак».

В Проекті Закону України «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» (зареєстрований під № 11125 від 31.08.2012)[66] передбачається внесення змін до Закону України «Про основи національної безпеки України», і, зокрема, введення таких термінів:

– «об'єкти критичної інфраструктури – об'єкти, вплив на які, зокрема через об'єкти критичної інформаційної інфраструктури, може мати наслідки, що безпосередньо зачіпають національну безпеку, включаючи безпеку людини і громадянина, суспільства та держави …»;

– «об'єкти критичної інформаційної інфраструктури – це сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором,

---

[65] *Про виклики* та загрози національній безпеці України у 2011 році: Рішення Ради національної безпеки і оборони України від 17.11.2010 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua

[66] *Проект* Закону про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України [Електронний ресурс]. – Верховна Рада України. Веб-портал. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208

підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави».

На жаль проект закону не враховує, що в нашій державі паралельно вже діють Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджене Постановою Кабінету Міністрів України № 1051 від 15.08.2007), Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру (Положення затверджене постановами Кабінету Міністрів України № 1198 від 03.08.98, зміни – № 1376 від 29.07.99, № 1006 від 09.08.2001, № 717 від 15.05.2003, № 1402 від 04.09.2003, № 1700 від 08.12.2006), Єдина державна система цивільного захисту населення і територій (Закон України «Про правові засади цивільного захисту» від 24.06.2004 р. № 1859-IV).

Перелічені системи створені в тому числі для захисту життєво важливих для держави об'єктів від окремих видів загроз, у зв'язку з чим створюється ситуація, що характеризується домінуванням відомчих підходів до розв'язання безпекових проблем національного масштабу.

За цих умов неможливо уникнути, з одного боку, дублювання функцій та розпорошення ресурсів, а з іншого – прогалин у розподілі відповідальності за захист об'єктів та систем, критично важливих для існування держави, захисту національних інтересів, забезпечення безпеки населення та довкілля. Це також спричиняє слабкість і недостатність існуючих механізмів координації зусиль міністерств і відомств щодо забезпечення захисту об'єктів, що у світі прийнято відносити до критичної інфраструктури.

В національному законодавстві України є низка окремих термінів (переліків об'єктів), що визначають особливий статус об'єктів та систем з

точки зору захисту національних інтересів, стабільного функціонування держави в цілому. Всі вони, відповідно до світового досвіду, в тій чи іншій мірі відповідають за характеристиками категорії об’єктів «критичної інфраструктури». До цієї категорії, очевидно, слід віднести:

а) підприємства, які мають стратегічне значення для економіки та безпеки держави[67];

б) об'єкти, що підлягають обов’язковій охороні підрозділами Державної служби охорони за договорами[68];

в) об’єкти, які включені до Державних реєстрів потенційно небезпечних об'єктів[69] та об’єктів підвищеної небезпеки[70] (в т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров’ю громадян, майну, спорудам, навколишньому природному середовищу[71]);

г) важливі державні об’єкти[72];

д) об’єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період[73];

є) особливо важливі об’єкти електроенергетики[74,75];

---

[67] *Постанова* Кабінету Міністрів України від 23.12.04 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/1734-2004-%D0%BF

[68] *Постанова* Кабінету Міністрів України від 10 серпня 1993 р. № 615 «Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами) [Електронний ресурс]. – Законодавство України. - Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

[69] *Постанова* Кабінету Міністрів України від 29.08.2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів» [Електронний ресурс]: http://zakon3.rada.gov.ua/laws/show/1288-2002-%D0%BF

[70] *Закон* України від 18.01.2001 № 2245-III «Про об’єкти підвищеної небезпеки» [Електронний ресурс]: http://zakon1.rada.gov.ua/laws/show/2245-14

[71] *Перелік* особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу / Затв. Постановою Кабінету Міністрів України від 06.05.2000 № 765 [Електронний ресурс]: http://zakon.nau.ua/doc/?code=765-2000-%EF

[72] *Постанова* Кабінету Міністрів України № 1051 від 15.08.2007 (для службового користування)

[73] *Постанова* Кабінету Міністрів України від 24.04.99 року №675-019 «Щодо затвердження Переліку об’єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»

[74] *Закон* України від 16.10.1997 № 575/97-ВР «Про електроенергетику» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/575/97-%D0%B2%D1%80

[75] *Постанова* Кабінету Міністрів України від 28.07.2003 № 1170 «Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади» [Електронний ресурс]: http://zakon1.rada.gov.ua/laws/show/1170-2003-%D0%BF

ж) особливо важливі об’єкти нафтогазової галузі[76];

з) нерухомі об’єкти культурної спадщини.

Постановою Кабінету Міністрів України від 23.12.04 р. № 1734 було затверджено перелік підприємств, які мають стратегічне значення для економіки та безпеки держави. До переліку віднесені великі промислові об’єкти, комбінати, заводи, науково-дослідні установи, науково-виробничі об’єднання, конструкторські бюро тощо. Даний перелік систематично оновлюється міністерствами та іншими центральними органами виконавчої влади та подається щороку до Мінекономрозвитку України для зведення пропозицій з обґрунтуваннями по кожному об’єкту з метою прийняття Кабінетом Міністрів України рішення про внесення змін до зазначеного переліку. Основною метою даної постанови, очевидно, є обмеження щодо приватизації таких підприємств і установ. В постанові зазначається, що Фонду державного майна у планах розміщення акцій підприємств, що не увійшли до даного переліку підприємств, не передбачати залишення акцій у державній власності, крім випадків, визначених законодавством.

В новій редакції Воєнної доктрини України (ст. 28)[77] як один із напрямів військово-промислової політики держави згадується про необхідність «залишення у державній власності стратегічно важливих для забезпечення обороноздатності держави підприємств».

Не зважаючи на суто економічну спрямованість введення категорії «підприємства, які мають стратегічне значення для економіки та безпеки держави», даний перелік використовується як базовий при визначенні підвищених вимог щодо фізичного захисту тих чи інших об’єктів. Ряд таких об’єктів охороняється Державної службою охорони, відповідно до Постанови Кабінету Міністрів України № 615 від 10 серпня 1993 р. «Про заходи щодо

---

[76] *Розпорядження* Кабінету Міністрів України від 27.05.2009 № 578-р «Про затвердження переліку особливо важливих об'єктів нафтогазової галузі» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/578-2009-%D1%80

[77] *Указ* Президента України від 08.06.2012 № 390/2012 «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Воєнної доктрини України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/390/2012

вдосконалення охорони об’єктів державної та інших форм власності»[78]. Названою постановою затверджений перелік об’єктів, що підлягають обов’язковій охороні підрозділами Державної служби охорони за договорами. До даного переліку віднесені, зокрема, такі об’єкти:

– будинки, в яких розміщуються центральні органи виконавчої влади (крім центральних органів виконавчої влади, що здійснюють керівництво військовими формуваннями, Державної податкової служби та Державної митної служби), будинки та приміщення, в яких розміщуються органи влади Автономної Республіки Крим;

– Національна телекомпанія, Національна радіокомпанія, державні телевізійні центри, будинки радіомовлення та звукозапису;

– державні архіви та їхні сховища, державні музеї, картинні галереї, історико-культурні заповідники, інші важливі об’єкти культури, де зберігаються історичні та культурні цінності загальнодержавного значення;

– Українська фондова біржа та її філії, державні підприємства ювелірної промисловості, бази, склади благородних металів, дорогоцінного каміння та виробів із нього, підприємства, що виробляють цінні державні папери, інспекції пробірного нагляду;

– підприємства, спеціалізовані цехи і дільниці, що виробляють вогнепальну спортивно-мисливську зброю, спеціальні засоби, заряджені речовинами сльозоточивої та дратівної дії, засоби активної оборони, вибухові речовини та об’єкти їх зберігання;

– бази, склади та інші державні об’єкти зберігання матеріальних цінностей на суму понад 20 тисяч мінімальних розмірів заробітної плати; державні універсальні магазини із щоденною виручкою в сумі понад 5 тисяч мінімальних розмірів заробітної плати, їхні склади, центральні каси;

– склади мобілізаційного резерву, центральні й обласні аптечні склади;

---

[78] *Постанова* Кабінету Міністрів України №615 від 10 серпня 1993 р. «Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами) [Електронний ресурс]. – Законодавство України. - Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

– об’єкти водопостачання населених пунктів з резервуарами питної води;

– морські порти;

– особливо важливі мости на залізничних магістралях і автомагістралях державного значення;

– сховища нафти і газу, особливо важливі об’єкти нафтогазової галузі;

– магістральний трубопровід, яким транспортується аміак;

– склади, інші нерухомі об’єкти зберігання (використання) небезпечних речовин; пункти поховання радіоактивних відходів; об’єкти, розташовані в зоні безумовного відселення та відчуження;

– Національний виставочний центр при Кабінеті Міністрів України (м. Київ), Національна бібліотека України імені В.І. Вернадського (м. Київ), Національний спортивний комплекс «Олімпійський», клінічна лікарня «Феофанія» Державного управління справами;

– Український та регіональні центри оцінювання якості освіти, їх об’єкти, пункти тестування, а також місця проведення та перевірки результатів зовнішнього незалежного оцінювання.

Окрім Державної служби охорони, яка функціонує в структурі МВС, інші відомства теж опікуються охороною важливих об’єктів, які належать їх сфері підзвітності. Так, наприклад, відповідно до вимог постанови Кабінету Міністрів України від 24.04.99 р. № 675-019 «Щодо затвердження Переліку об’єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період» та з метою здійснення та вдосконалення системи охорони шлюзів як стратегічно важливих об’єктів України Мінтранспорту (2004 р.) було створено у складі ДП «Укрводшлях» загони для охорони судноплавних шлюзів[79], а для охорони особливо важливих об’єктів підприємств паливно-енергетичного комплексу Міненерговугілля створило в 2007 р. відомчу

[79] *Наказ* Міністерства транспорту України від 16.02.2004 № 89 «Про затвердження Положення про загін відомчої охорони судноплавних шлюзів та Запорізького району гідротехнічних споруд» / Зареєстр. в Мінюсті 02.03.2004 за № 268/8867 [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/z0268-04

воєнізовану охорону[80].

Згідно з розпорядженням Кабінету Міністрів України від 27.05.2009 р. № 578-р Міненерговугілля разом з МВС і МНС повинно забезпечувати згідно з вимогами законодавства організацію охорони, зокрема пожежної, особливо важливих об'єктів нафтогазової галузі, фінансування якої здійснюється за рахунок підприємств, включених до даного переліку.

Привертають увагу декілька випадків судового розгляду справ щодо правомірності укладання договорів про охоронні послуги Державної служби охорони. Господарюючі суб'єкти відмовляються від охорони з боку Державної служби охорони, аргументуючи свою відмову наявністю на об'єктах власних підрозділів охорони та відсутністю чіткої методики визначення переліку об'єктів, які мають підлягати охороні[81,82].

Зокрема, в судовій справі Державної служби охорони проти ДП «Придніпровська залізниця» було встановлено таке. Незважаючи на те, що до Переліку об'єктів, що підлягають обов'язковій охороні підрозділами Державної служби охорони при Міністерстві внутрішніх справ за договорами, віднесені, зокрема, особливо важливі мости на залізничних магістралях і автомагістралях державного значення, конкретного найменування та місцезнаходження таких об'єктів зазначений перелік не містить.

Для умов надзвичайного стану та особливого періоду, відповідно до Постанови Кабінету Міністрів України від 13.12.2000 р. № 1833-034, ряд залізничних мостів підлягають обов'язковій охороні. Втім, в умовах мирного часу зазначені мости не віднесені до особливо важливих мостів на залізничних магістралях і автомагістралях державного значення. Взагалі, категорія мостів визначається тільки по їх вантажопідйомності та довжині

---

[80] *Наказ* Мінпаливенерго України від 08.10.2007 № 480 «Про організацію діяльності відомчої воєнізованої охорони Міністерства палива та енергетики України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z1262-07

[81] *Постанова* Вищого господарського суду України. Справа № 5005/2220/2011, 06.10.2011 [Електронний ресурс]. – Єдиний державний реєстр судових рішень. – Режим доступу: http://reyestr.court.gov.ua/Review/18544529

[82] *Рішення* Господарського суду Донецької області. Справа № 43/271пд, 04.03.2010 [Електронний ресурс]. – Єдиний державний реєстр судових рішень. – Режим доступу: http://reyestr.court.gov.ua/Review/8236600

(наприклад, великий міст – міст повною довжиною понад 100 м, а малий міст – до 25 м)[83], проте, за якими критеріями визначається особлива важливість мосту, ніде не встановлено.

Таким чином, відсутність нормативних документів, що визначають особливо важливі інфраструктурні об'єкти, зокрема на залізниці, для умов мирного часу спричиняє ситуацію, коли важливість об'єкту визначається керівництвом відомства, якому даний об'єкт підпорядковується.

Наприклад, перелік об'єктів залізничного транспорту, що підлягають охороні підрозділами відомчої воєнізованої охорони, затверджується начальником залізниці за погодженням з Управлінням воєнізованої охорони Укрзалізниці[84]. При цьому не розглядається загальнодержавне чи регіональне значення об'єкту.

Однією з основних категорій об'єктів, що визначена в національному законодавстві та може бути використана при визначенні критично важливих об'єктів та інфраструктури в Україні, є потенційно небезпечні об'єкти.

В рамках Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій створено Державний реєстр потенційно небезпечних об'єктів. Реєстрації на безоплатній основі підлягають всі, незалежно від форми власності, розташовані на території України небезпечні об'єкти, на яких існує загроза виникнення надзвичайних ситуацій. Метою створення реєстру було ведення державного обліку потенційно небезпечних об'єктів та інформаційного забезпечення процесів підготовки управлінських рішень і виконання зобов'язань України згідно з міжнародними договорами щодо запобігання та ліквідації наслідків надзвичайних ситуацій, у тому числі транскордонного характеру, пов'язаних з функціонуванням небезпечних об'єктів.

Порядок проведення ідентифікації потенційно небезпечних об'єктів

---

[83] *згідно* Інструкції по утриманню штучних споруд, затвердженої Наказом Укрзалізниці від 27.04.1999 р. № 124-Ц

[84] *відповідно* до п. 1.7 Положення про порядок охорони вантажів і об'єктів на залізницях України, затвердженого наказом Укрзалізниці від 29.12.2008 р. № 570-Ц

встановлено відповідною методикою[85]. Складовим етапом процедури ідентифікації є виявлення за результатами аналізу джерел небезпеки, які при певних умовах (аварії, порушення режиму експлуатації, виникнення природних небезпечних явищ тощо) можуть стати причиною виникнення надзвичайної ситуації, а також оцінка можливих наслідків надзвичайної ситуації для кожного з джерел небезпеки (кількість загиблих, постраждалих, тих, яким порушено умови життєдіяльності, матеріальні збитки) з використанням відповідної методики[86]. При встановленні рівня можливих надзвичайних ситуацій визначається: територіальне поширення імовірних надзвичайних ситуацій; кількість осіб, яким можуть бути порушені умови життєдіяльності у результаті можливої аварії на об’єкті; збитки від наслідків можливих надзвичайних ситуацій.

Таким чином, основною характеристикою, що враховується при визначенні та віднесення об’єктів до категорії «потенційно небезпечні об’єкти» є розмір наслідків можливої аварії на об’єкті. Виходячи із загальноприйнятого визначення критичної інфраструктури, частина переліку потенційно небезпечних об’єктів може увійти й у перелік об’єктів критичної інфраструктури.

Необхідність систематизації та категоризації об’єктів в окремих галузях, з метою визначення переліку таких об’єктів, на яких повинні діяти підвищені вимоги щодо фізичного захисту, знайшла своє відображення в ряді нормативних актів. Зокрема, розпорядженням Кабінету Міністрів України від 27.05.2009 р. № 578-р визначено перелік особливо важливих об’єктів нафтогазової галузі[87]. До названої категорії об’єктів було віднесено:

– об’єкти підприємств нафтогазової галузі, які мають стратегічне

---

[85] *Наказ* МНС України від 23.02.2006 року № 98 «Про затвердження Методики ідентифікації потенційно небезпечних об'єктів» / Зареєстр. в Мінюсті України 20.03.2006 р. за № 286/12160 [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/z0286-06

[86] *Постанова* Кабінету Міністрів України від 15 лютого 2002 р. № 175 «Про затвердження Методики оцінки збитків від наслідків надзвичайних ситуацій техногенного і природного характеру» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/175-2002-%D0%BF

[87] *Розпорядження* Кабінету Міністрів України від 27.05.2009 р. № 578-р «Про затвердження переліку особливо важливих об’єктів нафтогазової галузі» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/578-2009-%D1%80

значення для економіки і безпеки держави (визначені Постановою Кабінету Міністрів України від 23.12.04 р. № 1734);

– об’єкти підприємств нафтогазової галузі, які згідно з встановленими критеріями оцінки підпадають під визначення важливих державних об’єктів та об’єктів державного значення всіх форм власності (відповідно до Постанови Кабінету Міністрів України від 24.04.99 р. № 675-019);

– об’єкти підприємств нафтогазової галузі, які включені до Державних реєстрів потенційно небезпечних об’єктів та об’єктів підвищеної небезпеки і потребують постійного підтримання надійності, безпеки експлуатації та охорони спеціалізованими підрозділами в зв’язку з підвищеною вибухо- та пожежонебезпечністю газу, нафти та продуктів їх переробки.

До даного переліку об’єктів віднесені: магістральні нафтопроводи; відводи магістрального нафтопроводу; нафтоперекачувальні станції; лінійні виробничі диспетчерські станції; кінцеві пункти; морські нафтові термінали; цехи видобування нафти і газу; дільниці підготовки і перекачування нафти в т.ч. з резервуарним парком і наливною естакадою; газліфтні компресорні станції; газопереробні заводи; резервуарні парки газопереробних заводів.

Іншим нормативно-законодавчим документом – Постановою Кабінету Міністрів України від 28.07.2003 р. № 1170, затверджено перелік особливо важливих об’єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади[88]. Охорону об’єктів даної категорії повинні здійснювати узгоджено підрозділи відомчої воєнізованої охорони Міненерговугілля, МВС, Мінінфраструктури.

До даного переліку особливо важливих об’єктів електроенергетики віднесені: диспетчерські пункти оперативно-технологічного управління; електропідстанції напругою понад 330 кВ; теплоелектростанції;

[88] *Постанова* Кабінету Міністрів України від 28.07.2003 № 1170 «Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади» [Електронний ресурс]: http://zakon1.rada.gov.ua/laws/show/1170-2003-%D0%BF

гідроелектростанції; теплоелектроцентралі.

Ще однією категорію, яка визначена в українському законодавстві, і з огляду на можливі терористичні загрози, визначається, наприклад, в США, як елемент критичної інфраструктури, є нерухомі пам'ятки культурної спадщини. До об'єктів культурної спадщини у відповідності до Закону України «Про охорону культурної спадщини»[89] належать визначні місця, споруди (витвори), комплекси (ансамблі), їхні частини, пов'язані з ними рухомі предмети, а також території чи водні об'єкти (об'єкти підводної культурної та археологічної спадщини), інші природні, природно-антропогенні або створені людиною об'єкти незалежно від стану збереженості, що донесли до нашого часу цінність з археологічного, естетичного, етнологічного, історичного, архітектурного, мистецького, наукового чи художнього погляду і зберегли свою автентичність. Пам'ятками культурної спадщини є об'єкти культурної спадщини, які занесені до Державного реєстру нерухомих пам'яток України. Навколо пам'яток культурної спадщини встановлюється охоронна зона, зона регулювання забудови, зона охоронюваного ландшафту, зона охорони археологічного культурного шару, в межах яких діє спеціальний режим їх використання.

Окрім вказаних категорій (переліків об'єктів) в національному законодавстві окремими нормативно-правовими актами регулюється функціонування:

- Національної система конфіденційного зв'язку[90];
- платіжних систем[91];
- Системи екстреної допомоги населенню за єдиним номером 112[92];
- аварійно-рятувальних служб.

---

[89] *Закон* України від 08.06.2000 № 1805-III «Про охорону культурної спадщини» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/1805-14

[90] *Закон* України від 10.01.2002 № 2919-III «Про Національну систему конфіденційного зв'язку» (із змінами) [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/2919-14

[91] *Закон* України від 05.04.2001 № 2346-III «Про платіжні системи та переказ коштів в Україні» http://zakon2.rada.gov.ua/laws/show/2346-14

[92] *Закон* України від 13.03.2012 № 4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» http://zakon2.rada.gov.ua/laws/show/4499-17

Названі системи та служби, з огляду на світовий досвід, належать до критичної інфраструктури.

В галузі зв'язку та інформаційних систем потрібно згадати Національну систему конфіденційного зв'язку та платіжні системи. Перша, згідно Закону України «Про Національну систему конфіденційного зв'язку»[93] являє собою сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану. Держспецзв'язок здійснює управління Національною системою конфіденційного зв'язку, забезпечує її функціонування, розвиток, використання та захист інформації.

Друга група інформаційних систем – це платіжні системи, координацію, створення та контроль над функціонуванням яких, згідно Закону України «Про Національний банк України» (ст. 7), здійснює Національний банк України. На сьогодні створено та забезпечується функціонування Системи електронних платежів (міжбанківські розрахунки) та Національної системи масових електронних платежів (роздрібні платежі). Для визначення основних засад політики щодо здійснення нагляду (оверсайта) за платіжними системами, що функціонують в Україні, схвалив Концепцію запровадження нагляду (оверсайта) за платіжними системами в Україні[94]. Окрім економічних параметрів платіжних систем значна увага приділяється технічному забезпеченню їх надійної роботи, здебільше, інформаційній безпеці.

Важливо відзначити, що до критичної інфраструктури за міжнародним досвідом прийнято, зокрема, відносити аварійно-рятувальні служби та

---

[93] *Закон* України від 10.01.2002 № 2919-III «Про Національну систему конфіденційного зв'язку» (із змінами) [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/2919-14

[94] *Концепція* запровадження нагляду (оверсайта) за платіжними системами в Україні / Постанова Правління Національного банку України від 15.09.2010 № 426 [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/v0426500-10

служби надання екстреної допомоги населенню. В Законі України «Про аварійно-рятувальні служби» вказується, що аварійно-рятувальні служби обслуговують окремі території, а також підприємства, установи та організації незалежно від форми власності, на яких існує небезпека виникнення надзвичайних ситуацій природного чи техногенного характеру. Перелік таких об’єктів визначений Постановою Кабінету Міністрів України[95]. До даного переліку внесені: об’єкти геологорозвідки, вугільної промисловості, гірничорудної та нерудної промисловості, нафтодобувної промисловості, хімічної та нафтохімічної промисловості (в т.ч. магістральні нафтопроводи, нафтопродуктопроводи, аміакопроводи, етиленопроводи), металургійної промисловості, машинобудування, енергетики, транспортно-дорожнього комплексу і т.д.

На виконання Розпорядження Кабінету Міністрів України від 02.10.2003 р. № 589-р МНС був розроблений «Порядок обслуговування об’єктів та окремих територій державними аварійно-рятувальними службами»[96]. Чисельність та професійний склад державної аварійно-рятувальної служби (формування), що обслуговує об’єкт згідно з договором на постійне та обов’язкове обслуговування, залежить від джерела небезпеки та масштабу (рівня) можливої надзвичайної ситуації, статистичних даних фактичної аварійності на цьому об’єкті чи території, а також обсягів профілактичної роботи та визначається керівником державної аварійно-рятувальної служби (формування). Вартість аварійно-рятувального обслуговування об’єктів державними аварійно-рятувальними службами, в тому числі відшкодування витрат, пов’язаних з ліквідацією надзвичайних ситуацій, визначається Порядком визначення розмірів оплати за обслуговування об’єктів та окремих територій державними аварійно-

[95] *Постанова* Кабінету Міністрів України від 04.08.2000 № 1214 «Про затвердження переліку об'єктів та окремих територій, які підлягають постійному та обов'язковому на договірній основі обслуговуванню державними аварійно-рятувальними службами» http://zakon1.rada.gov.ua/laws/show/1214-2000-%D0%BF

[96] *Наказ* Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 17.11.2003 №440 «Про Порядок обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z1125-03

рятувальними службами[97].

Тобто об'єм ресурсів та засобів (організаційних, технічних, інженерних, інформаційних і т.д.), яким забезпечені аварійно-рятувальні служби при обслуговуванні об'єктів, визначається керівництвом відповідного формування даної служби, і немає жодних вимог щодо врахування при цьому загальнодержавної (чи регіональної) значущості об'єкту, розміру та характеру можливих наслідків від аварії на інші об'єкти і т.д.

До того ж, поширення послуг аварійно-рятувальних служб МНС подекуди не охоплює всі потенційно-небезпечні об'єкти. Наприклад, в протоколі засідання (листопад 2011 р.) Комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій при Одеській обласній державній адміністрації зазначається: «аварійно-рятувальним загоном спеціального призначення ГУ МНС України в Одеській області обслуговується лише 202 об'єкта, що складає 33 % та 34 окремі території (місця масового відпочинку людей), що складає 18 % від загальної кількості, які підлягають обов'язковому обслуговуванню»[98].

На жаль, в Україні залишається неефективною система охорони, або взагалі відсутня система фізичного захисту таких об'єктів, де зберігається значний об'єм токсичних речовин (наприклад, території комбінату поблизу м. Калуш), природно-заповідних зон, місць зберігання твердих промислових відходів. Щодо питання поводження з відходами можна, як приклад, згадати, що на території Україні з 60-х років Збройними Силами СРСР були створені могильники для радіоактивних відходів, і на сьогодні на цих об'єктах фізичний захист практично відсутній. В той же час держава зазнає

---

[97] *Наказ* Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерства економіки та з питань європейської інтеграції України від 15.12.2003 № 495/369 «Про затвердження Порядку визначення розмірів оплати за обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1222-03

[98] *Протокол* № 36 позачергового засідання комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій облдержадміністрації від 22 листопада 2011 року [Електронний ресурс]. – Управління з питань надзвичайних ситуацій Одеської обласної державної адміністрації. – Режим доступу: http://guns.odessa.gov.ua/Main.aspx?sect=Page&IDPage=38905&id=113

зовнішнього тиску (критики) у зв'язку з проблемою незаконного обігу радіоактивних матеріалів.

Окремим питанням є спроможність держави виділяти достатні матеріальні ресурси на утримання та модернізацію системи захисту критично важливої інфраструктури.

На сьогодні планування витрат на забезпечення безпеки життєво важливих об'єктів і систем в Україні здійснюється без урахування розміру наслідків від можливих аварій на цих об'єктах та аналізу загроз цим об'єктам. Зокрема, фінансування діяльності з попередження, реагування та ліквідації наслідків надзвичайних ситуацій заплановано в Загальнодержавній цільовій програмі[99]. На фінансування витрат, пов'язаних з надзвичайними ситуаціями також використовується Резервний фонд Кабінету Міністрів України[100].

На жаль, витрати на розвиток систем забезпечення безпеки критичної інфраструктури можуть повністю лягти на плечі користувачів послуг цієї інфраструктури.

Наприклад, комісія, що була утворена Міненерговугілля (Наказ № 365 від 08.07.2008 р.)[101], визнала, що охорона структурних підрозділів ДП «Кримські генеруючі системи» не відповідає вимогам чинного законодавства щодо охорони особливо важливих об'єктів електроенергетики. Ця ж комісія запропонувала вийти з пропозицією до Національної комісії, що здійснює державне регулювання у сфері енергетики, про включення витрат на утримання підрозділу відомчої воєнізованої охорони до тарифу на виробництво електроенергії.

Подібна ж ситуація складається із модернізацією мереж

---

[99] *Закон* України від 07.06.2012 № 4909-VI «Про Загальнодержавну цільову програму захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру на 2013-2017 роки» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/4909-17

[100] *Постанова* Верховної Ради України від 22.02.1996 № 62/96-ВР «Про затвердження Положення про резервний фонд Кабінету Міністрів України»

[101] *Наказ* Міненерговугілля № 365 від 08.07.2008 «Про організацію охорони об'єктів Державного підприємства «Кримські генеруючі системи» [Електронний ресурс]. – офіційний веб-сайт Міненерговугілля. – Режим доступу: http://mpe.kmu.gov.ua/fuel/doccatalog/document?id=136192

життєзабезпечення, які є критично важливими для великих міст. Аномально-високі температури влітку та морози взимку спричиняють аварії на мережах житлового господарства. Втрата теплової енергії в мережах теплопостачання в Україні є досить високою (8-10 % – котельня, 10-13 % – теплотраса, 20-40 % – будинок). Навіть витрачаючи порівняно з європейцями меншу частку від своїх доходів на оплату послуг ЖКГ, українці боляче відчувають збільшення цін.

Низку економічних механізмів запроваджено в Україні для захисту підприємств, що є життєво важливими для забезпечення населення та територій послугами з водопостачання, електроенергії, теплопостачання тощо.

Зокрема, Законом України «Про електроенергетику» вводиться поняття «екологічна броня електропостачання споживача» – мінімальний рівень споживання електричної енергії споживачем (крім населення), який забезпечує передумови для запобігання виникненню надзвичайних ситуацій техногенного та природного характеру. Екологічна броня електропостачання встановлюється з метою запобігання виникненню надзвичайних ситуацій техногенного та природного характеру через припинення електропостачання підприємствам. Кабінет Міністрів України затверджує порядок складання переліку споживачів та їх обладнання, для якого має бути встановлена екологічна броня електропостачання. Фінансування екологічної броні електропостачання при несплаті або неповній оплаті за спожиту електроенергію споживачами, що мають таку броню, здійснюється з державного або місцевих бюджетів. Відповідно до Порядку складання переліку споживачів та їх обладнання, для якого має бути встановлена екологічна броня електропостачання, затвердженого Постановою Кабінету Міністрів України від 26.12.2003 р. № 2052[102], цей перелік складається, з метою запобігання виникненню надзвичайних ситуацій техногенного та

[102] *Постанова* Кабінету Міністрів України від 26.12.2003 № 2052 «Про затвердження Порядку складання переліку споживачів та їх обладнання, для якого має бути встановлена екологічна броня електропостачання, та визнання такою, що втратила чинність, постанови Кабінету Міністрів України від 16 листопада 2002 р. № 1792» [Електронний ресурс]: http://zakon3.rada.gov.ua/laws/show/2052-2003-%D0%BF

природного характеру через обмеження або припинення електропостачання. Також, відповідно до Порядку надання кредитів для оплати екологічної броні електропостачання, затвердженого Постановою Кабінету Міністрів України від 03.08.2005 р. № 702[103], визначається механізм надання кредитів для оплати екологічної броні електропостачання у разі несплати або неповної оплати спожитої електричної енергії споживачами, що мають таку броню.

Станом на 1 травня 2005 року до Переліків споживачів електричної енергії та їх обладнання, для якого має бути встановлена екологічна броня електропостачання за всіма адміністративно-територіальними одиницями України, включено 2307 підприємств (в тому числі 565 підприємств водопровідно-каналізаційного господарства)[104].

Таким чином підприємства, для яких встановлена екологічна броня, розглядаються як критичні з точки зору можливих наслідків при відключенні енергопостачання і теж можуть розглядатися як «кандидати» до переліку об'єктів критичної інфраструктури.

Згідно з Постановою Кабінету Міністрів України від 6 травня 2000 р. № 765[105] низка підприємств вугільної, гірничодобувної, металургійної промисловості, хімічного комплексу, енергетики та оборонної промисловості визначена особливо небезпечними в разі припинення їх діяльності. Відповідно до згаданої постанови діє порядок задоволення вимог щодо відшкодування витрат на заходи для запобігання заподіянню можливої шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу у випадку банкрутства таких підприємств.

Проблему впровадження цілісної концепції захисту критичної інфраструктури в Україні потрібно вирішувати з огляду на процеси

---

[103] *Постанова* Кабінету Міністрів України від 03.08.2005 № 702 «Про затвердження Порядку надання кредитів для оплати екологічної броні електропостачання» [Електронний ресурс]: http://zakon2.rada.gov.ua/laws/show/702-2005-%D0%BF

[104] *Інформація* щодо визначення величини екологічної броні електропостачання споживачів на 01.05.05р. [Електронний ресурс]. – НЕК «Укренерго». – Режим доступу: http://www.ukrenergo.energy.gov.ua/ukrenergo/control/uk/publish/article?art_id=39300&cat_id=35981

[105] *Постанова* Кабінету Міністрів України від 06.05.2000 № 765 «Про реалізацію статей 31 і 43 Закону України «Про відновлення платоспроможності боржника або визнання його банкрутом» [Електронний ресурс]: http://zakon.nau.ua/doc/?code=765-2000-%EF

модернізації системи захисту національної безпеки.

Так, спроба систематизувати правові норми, розпорошені по численних законодавчих актах, що регламентують питання захисту населення і територій від надзвичайних ситуацій природного та техногенного характеру, була здійснена в проекті Кодексу цивільного захисту України (реєстр. № 10294 від 02.04.2012 р.)[106]. Після прийняття цього законопроекту має втратити чинність низка законів, що регулюють дану сферу суспільних відносин, зокрема, Закони України «Про цивільну оборону», «Про пожежну безпеку», «Про загальну структуру і чисельність військ Цивільної оборони», «Про війська Цивільної оборони України», «Про аварійно-рятувальні служби», «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», «Про правові засади цивільного захисту».

Разом з тим, законопроект має ряд суттєвих недоліків. Проект містить положення декларативного характеру, що не забезпечують регулюючого впливу на відповідні суспільні відносини. Так, визначення функцій суб'єктів забезпечення цивільного захисту (ст. 10, 11, 12), мають описовий характер, не дають чіткого уявлення про те, який орган має здійснювати ту чи іншу функцію.

У висновку Головного науково-експертного управління щодо даного законопроекту констатується таке: «У цілому проект не дає чіткого уявлення про повноваження та взаємодію центральних органів виконавчої влади у складі єдиної державної системи цивільного захисту». Це означає, що даний проект кодексу законів не спрямований на розв'язання проблем координації зусиль із захисту критично важливих для життєдіяльності держави об'єктів та інфраструктури.

Ще одним питанням, яке виникне при системному впровадженні концепції захисту критичної інфраструктури в Україні буде залучення

---

[106] *Проект* Кодексу цивільного захисту України [Електронний ресурс]. – Верховна Рада України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?pf3511=43014

Збройних Сил України та регулювання в умовах особливого стану та надзвичайної ситуації. Низка законів України[107,108,109,110,111] містять положення про координацію дій та концентрацію зусиль державних органів у певних умовах, які стосуються або так званого особливого періоду часу (охоплює час мобілізації, воєнний час і частково відбудовний період), або надзвичайного стану, і спрямовані на організацію діяльності державних органів у разі воєнної загрози або захисту від наслідків надзвичайних ситуацій техногенного, екологічного, природного та воєнного характеру. Проте, терористичні загрози у цих законах не згадуються. Аналогічний підхід спостерігається і у законах про транспорт[112] (ст. 15. Організація роботи транспорту у надзвичайних умовах) і трубопровідний транспорт[113] (ст. 18. Організація роботи підприємств, установ та організацій трубопровідного транспорту в умовах надзвичайного стану).

Серед пріоритетних напрямів підготовки держави до збройного захисту національних інтересів в новій редакції Воєнної доктрини України (ст. 23)[114] вказується «розвиток інфраструктури регіонів з урахуванням потреб підготовки території держави до оборони».

На даному етапі все гострішою стає проблема стандартизації процедур оцінки ризиків для великих інфраструктурних об’єктів в Україні. У теперішній час в законодавстві України існує біля 30 визначень поняття «ризик» (зокрема, в законах України «Про об’єкти підвищеної небезпеки»,

---

[107] *Закон* України «Про оборону України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1932-12

[108] *Закон* України «Про цивільну оборону України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2974-12

[109] *Закон* України «Про правовий режим надзвичайного стану» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1550-14

[110] *Закон* України «Про мобілізаційну підготовку та мобілізацію» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3543-12

[111] *Закон* України «Про функціонування єдиної транспортної системи України в особливий період» [Електронний ресурс]. –Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=194-14

[112] *Закон* України «Про транспорт» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=232%2F94-%E2%F0

[113] *Закон* України «Про трубопровідний транспорт». [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=192%2F96-%E2%F0

[114] *Указ* Президента України від 08.06.2012 № 390/2012 «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Воєнної доктрини України» [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/390/2012

«Про основні засади державного нагляду (контролю) у сфері господарської діяльності», «Про стандарти, технічні регламенти та процедури оцінки відповідності» та інших нормативно-правових документах). В той же час для оцінки ризиків критичної інфраструктури потрібно розробити методологію, яка враховує особливості інфраструктурних об'єктів.

На сьогодні провідні країни світу проходять шлях стандартизації термінології та підходів в сфері захисту критичної інфраструктури, зокрема, ці процеси активно відбуваються в Сполучених Штатах[115].

Аналіз показує явну недостатність стандартів з аналізу ризиків в Україні в порівнянні з провідними країнами і, головне, слабку узгодженість понятійного апарату, що використовується. Практичне вирішення проблем стандартизації, сертифікації забезпечення якості та ефективності систем комплексної безпеки в Україні на сьогодні в перспективі гостро затребуване, а у зв'язку з євроінтеграційними намірами буде ще більше затребуване і потребуватиме гармонізації з міжнародними стандартами, в тому числі для забезпечення конкурентоздатності вітчизняної продукції на світовому ринку.

Висновки та пропозиції

1. Дослідження ступеня впровадження концепції захисту критичної інфраструктури в провідних країнах світу, в наших східноєвропейських країнах-сусідах, а також в Російській Федерації показує, що концепція критичної інфраструктури на сьогодні є дієвим інструментом, який використовується як в міжнародній, так і в національних системах безпеки для захисту найбільш важливих систем, об'єктів та ресурсів.

Україна підтвердила свій євроінтеграційний вибір, і це передбачає, зокрема, її наближення до підходів ЄС у безпековій сфері. Також треба зважати на процеси реформування державного апарату в Україні, які закладають сприятливі організаційно-управлінські підвалини для

[115] *Harter A.G.,* Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management // Critical Infrastructure Protection: Elements of Risk. – George Mason University, 2007. – P. 79 – 92.

запровадження концепції захисту критичної інфраструктури в нашій країні.

Зважаючи на це, запровадження в Україні концепції захисту критичної інфраструктури стане важливим кроком на шляху до вдосконалення існуючих державних систем і інституцій в сфері безпеки.

2. Заходи щодо захисту критично важливих об’єктів, систем та ресурсів в Україні, здійснюються низкою відомств в межах їх завдань і компетенції, і мають фрагментарний характер, що відбивається в паралельному функціонуванні систем, призначених для захисту об’єктів та населення від окремих типів загроз (техногенного, природного або соціально-політичного характеру), а саме: Єдиної державної системи запобігання і реагування на надзвичайні ситуації техногенного та природного характеру; Єдиної державної системи цивільного захисту населення і територій; Єдиної державна система запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків.

Таке паралельне існування систем захисту критично важливих об’єктів та інфраструктури створило загрозу «бюрократизації» проблеми, неефективного використання ресурсів на національному рівні.

3. Категоризація критично важливих об’єктів або елементів критичної інфраструктури України здійснюється на основі галузевих (відомчих) підходів, виходячи з міркувань та критеріїв забезпечення безпеки за окремими складовими національної безпеки (економічної, державної, політичної, енергетичної, екологічної, гуманітарної тощо), що мало своїм результатом різні дефініції об’єктів, а саме: підприємства, які мають стратегічне значення для економіки та безпеки держави; важливі державні об’єкти; об’єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період; потенційно небезпечні та об’єкти підвищеної небезпеки; особливо важливі об’єкти електроенергетики, нафтогазової галузі; нерухомі пам’ятки культурної спадщини.

4. Попри істотні досягнення в становленні (формуванні) системи захисту національної безпеки України, існує ціла низка труднощів і проблем,

пов’язаних із захистом критичної інфраструктури, що потребують розв’язання:

– невідповідність національної нормативно-правової бази, положенням міжнародних документів, зокрема в тій частині, що регулює питання захисту критично важливих об’єктів та інфраструктури, на фоні декларування курсу на євроінтеграцію;

– обмеженість механізмів обміну інформацією та інформаційного забезпечення про загрози об’єктам критичної інфраструктури та відсутність механізмів надвідомчого управління та інвентаризації ресурсів, які задіяні для попередження загроз техногенного та природного характеру, в умовах зростання їх рівня, що вимагає кращого забезпечення інженерними засобами, обладнанням, технікою, інформаційними та кадровими ресурсами;

– відсутність нормативних документів, вимог, методологій для оцінки загроз об’єктам, що є критичними для життєдіяльності держави; загальної методології оцінки ризиків для критично важливих об’єктів та інфраструктури, не зважаючи на щільну взаємозалежність критично важливих об’єктів (насамперед інформаційними, енергетичними і транспортними мережами), що створює небезпеку виникнення каскадних аварій;

– відсутність ефективної практики державно-приватного партнерства в сфері безпеки, що вимагає вдосконалення організаційних та правових основ такого партнерства;

– задачі захисту критичної інфраструктури мають міждисциплінарний характер, потребують комплексних наукових досліджень, які через свою складність вимагають значних фінансових інвестицій.

5. На сьогоднішній день інформаційні та телекомунікаційні мережі стають однією з основних та найбільш вразливих складових критичної інфраструктури, але впровадження концепції захисту критичної інфраструктури не повинно обмежуватися заходами щодо захисту тільки від

кібер-загроз.

З метою подолання названих труднощів та проблем, упровадження в Україні підходів до захисту критичної інфраструктури доцільно здійснити такі кроки.

1. Раді національної безпеки і оборони України розглянути можливість ініціювання процесів удосконалення державної системи захисту критично важливих об’єктів та інфраструктури в Україні шляхом:

– створення Робочої групи і організації розробки Стратегії захисту національної критичної інфраструктури;

– сприяння вдосконаленню чинного законодавства в безпековій сфері та його гармонізації з урахуванням кращого зарубіжного досвіду;

– розроблення загальної методології оцінки ризиків для об’єктів критичної інфраструктури.

2. Мінінфраструктури, Міненерговугілля, Міноборони, МНС, АТЦ при СБУ підготувати пропозиції щодо критеріїв віднесення об’єктів до критичної інфраструктури, надіслати їх Робочій групі з розробки Стратегії захисту національної критичної інфраструктури.

3. Мінінфраструктури, Міненерговугілля, Міноборони, МНС, МВС вдосконалити контроль за системами фізичного захисту критично важливих об’єктів та інфраструктури, використовуючи досвід, набутий Міненерговугілля та Держатомрегулювання, з організації та контролю над системами фізичного захисту об’єктів ядерної енергетики.

4. Мінприроди вдосконалити систему управління в сфері поводження з відходами, активізувати роботу із впровадження систем інформаційно-аналітичного супроводження державного контролю в даній сфері.

5. Мінрегіону вдосконалити систему оперативного контролю за станом мереж водо- та теплопостачання, вдосконалити методологію аналізу аварійності та оцінки ризиків аварій на даних мережах, з врахуванням впливу на цінову доступність послуг та платоспроможність населення.

6. ДКАУ підготувати пропозиції щодо вдосконалення системи космічного моніторингу за критично важливими об’єктами та інфраструктурою України.

7. Адміністрації Держспецзв’язку розглянути організаційні та технологічні можливості створення мережі обміну інформацією про загрози критично важливим об’єктам і інфраструктурі в рамках Національної системи конфіденційного зв’язку.

8. Мінекономрозвитку передбачити в Плані національної стандартизації розробку нормативних документів із стандартизації процесів управління ризиками.

9. НАНУ, МОНмолодьспорту передбачити:

– кошти для виконання підпорядкованими науково-дослідними установами та вищими навчальними закладами досліджень з оцінки ризиків для критично важливих об’єктів та інфраструктури в Україні;

– започаткування науково-практичного видання у сфері захисту критичної інфраструктури.

10. НІСД організувати та провести в 2013 році науково-практичну конференцію з проблем упровадження концепції захисту критичної інфраструктури в Україні; забезпечувати аналітичний та науковий супровід Робочої групи з розробки Стратегії захисту національної критичної інфраструктури, залучаючи до цього представників органів виконавчої влади, які є учасниками утвореної при НІСД Міжвідомчої експертної робочої групи з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов’язаних з ними терористичних загроз і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури.