НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Аналітична доповідь

Київ – 2012

УДК 504:338.14(477)
Б 24

Автори:

Бірюков Д. С., к. техн. н.;
Кондратов С. І.

Електронна версія: http://www.niss.gov.ua

Б 24 **Бірюков Д. С.** Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 96 с.

ISBN 978-966-554-183-7

Обґрунтовано необхідність формування єдиної державної політики у сфері захисту критично важливих об'єктів та інфраструктури в Україні. Представлено огляд досвіду запровадження концепції критичної інфраструктури у провідних країнах світу. Проаналізовано нормативно-правові акти національного законодавства, що виокремлюють і встановлюють особливі умови захисту низки категорій об'єктів в Україні, які за міжнародними підходами належать до критичної інфраструктури.

У додатку друкуються матеріали засідання «круглого столу» «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні», що відбувся 17 липня 2012 р. у Національному інституті стратегічних досліджень.

ISBN 978-966-554-183-7

Вступ

Останніми десятиріччями у світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різного походження. Щодня світові ЗМІ повідомляють про природні й техногенні катастрофи, збройні конфлікти, терористичні акти, тяжкі злочини, вчинені і злочинними організаціями, і окремими особами, акти піратства на морі тощо. І дедалі 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 зазначені тенденції, у більшості провідних країн світу задля 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 зазвичай належать транспортні й 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.

Запровадження системного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише введення відповідного терміна. На першому місці – створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди вузловим елементам критичної інфраструктури внаслідок дії негативних чинників будь-якого походження: техногенного, природного, соціально-політичного або будь-якої їх комбінації.

Було б неправильно стверджувати, що в Україні не приділяється увага захисту важливих об'єктів, систем і ресурсів, які зазвичай належать до критичної інфраструктури. Навпаки, в Україні діє низка законодавчих актів, що визначають особливості забезпечення захисту вказаної інфраструктури. Проте в державі досі відсутній загальний механізм управління захистом і безпекою названих об'єктів, спостерігаються непоодинокі випадки дублювання функцій і ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу. До того ж загрози таким об'єктам розглядаються в суто відомчому розрізі.

Усе це підтверджує необхідність упровадження низки суттєвих заходів на державному, регіональному й галузевому рівнях із правового й організаційно-методичного забезпечення, координації та консолідова-

ного забезпечення ресурсами систем безпеки, спільного використання засобів безпеки, що знаходяться в підпорядкуванні окремих відомств.

Зважаючи на сприятливі умови, що створюються під час 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

Із середини 90-х років XX ст. поняття «критична інфраструктура» було введено в нормативно-правові документи і практику міжнародного спілкування на дипломатичному рівні, в науковому й діловому колах. Його значення у кожній із країн дещо відрізняється, проте 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 перерахованого вище»[1].

Зазвичай до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства і 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 у сфері безпеки країн-членів ЄС і НАТО. Двома основними чинниками, що сформували концепцію захисту критичної інфраструктури, є такі:

• посилення боротьби з міжнародним тероризмом (система захисту критичної інфраструктури вдосконалювалася як відповідь на вчинені

[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

терористичні акти у США 2001 р., Іспанії – 2004 р. та Великій Британії – 2005 р.);

• забезпечення безпеки у процесі розроблення та реалізації основних проектів у області інфраструктури для транспортування нафти, нафтопродуктів, газу й інших стратегічних сировинних матеріалів. Останнє було підтверджено заявою, зробленою за результатами саміту країн НАТО (п. 52[2]), що відбувся 20–21 травня 2012 р. у м. Чикаго (США).

На особливу роль критичної інфраструктури звертають увагу й експерти Світового банку. Вони підкреслюють, що хоча й необхідно якісно проектувати й будувати будь-яку інфраструктуру, проте виокремлення категорії критичних об'єктів інфраструктури дозволить урядам приділяти останнім особливу увагу, зменшуючи тим самим наслідки, спричинені природними лихами й техногенними аваріями[3].

Аналіз міжнародного досвіду свідчить, що основою забезпечення захищеності й безпеки критичної інфраструктури є вирішення низки питань, з-поміж яких основними є такі:

• координація і взаємодія органів державної влади та обмін інформацією про загрози;

• організація державно-приватного партнерства у сфері безпеки;

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

Становлення нормативно-правової бази у сфері захисту критичної інфраструктури є тривалим процесом. Напевно, найбільших успіхів у цій сфері досягли США: Адміністративний наказ Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» (липень 1996 р.), а згодом Директива Президента США № 63 (травень 1998 р.)[4] започаткували там національну програму «Захист критичної інфраструктури». Продовження роботи з підсилення захисту критичної інформаційної інфраструктури відобразилося в Національному плані із захисту інформаційних систем (січень 2000 р.) Однак переломним

---

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

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

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

моментом у становленні концепції захисту критичної інфраструктури стала необхідність реагування на терористичні акти, вчинені 11 вересня 2001 р. в Нью-Йорку. Після цієї екстраординарної події уряд США кардинально переглянув підходи щодо забезпечення внутрішньої безпеки держави (і в технічному, і в організаційному плані). Важливим висновком із трагедії стало прийняття нормативно-правового документа, абревіатура назви якого *(USA PATRIOT ACT*[5]*)* перекладається як Акт про патріотизм; у ньому термін критична інфраструктура набув свого сучасного вигляду.

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

Аби проілюструвати пріоритетну увагу політичного керівництва США цій проблематиці достатньо лише навести короткий перелік основних документів, прийнятих після 11 вересня 2001 р.: адміністративні накази 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 та основних 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 вказаного сегмента забезпечення національної безпеки. На захист критичної інфраструктури у США витрачається більша частина коштів, що виділяються у федеральному бюджеті на забезпечення

---

[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

[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 / The White House. – Washington, 2009 [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

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

внутрішньої безпеки (у 2012 р. – близько 67,9 млрд дол. США та у проекті бюджету на 2013 р. – 68,9 млрд дол. США)[9]. При цьому у 2012 р. розподіл бюджетних коштів на зазначені цілі був таким: міністерство внутрішньої безпеки – 52%, міністерство оборони – 26%, 29 інших суб'єктів (міністерств, агентств та установ) – 22%.

У США керівні документи з організації захисту й реагування на загрози критичній інфраструктурі постійно вдосконалюються, відповідні плани реагування й евакуації населення під час надзвичайних ситуацій періодично переглядаються. Відбувається оновлення технічних засобів попередження та реагування на надзвичайні ситуації, вдосконалення способів і засобів інформування населення.

У Директиві Президента США з національної безпеки № 7 (грудень 2003 р.)[10] визначено відповідальність міністерства внутрішньої безпеки, інших міністерств і федеральних агентств, відповідальних за окремі сектори критичної інфраструктури. На міністерство внутрішньої безпеки покладено обов'язок формувати Національний план захисту критичної інфраструктури. Аналізуючи ці плани (останній розроблений у 2009 р. і попередній – у 2006 р.), можна дійти висновків про те, що зміни й удосконалення були здійснені в таких головних напрямах: планування регіонального захисту, вдосконалення загального підходу до управління ризиком, удосконалення 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.

У Євросоюзі загальноєвропейський підхід до захисту критичної інфраструктури задекларовано в Повідомленні Європейської Комісії № 786 2006 р.[12] До загальноєвропейської критичної інфраструктури належать ті елементи національних критичних інфраструктур країн-

---

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

[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.

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

членів ЄС, відмова, інцидент або атака на які може мати значний вплив і на країну, в якій ця подія відбудеться, і хоча б на одну з інших країн-членів ЄС. Згаданим Повідомленням започатковано Європейську програму із захисту критичної інфраструктури, розроблену задля підвищення рівня захищеності останньої у спосіб створення спільного підходу до її захисту в країнах-членах ЄС і гармонізації національних законодавств у згаданій сфері.

Варто зазначити, що провідні країни світу здійснюють захист своїх національних інтересів, не обмежуючись національними кордонами[13]. Крім 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 та установ, нібито створений дипломатичними місіями на запит Державного департаменту США у 2009 р. До цього списку потрапили такі масштабні об'єкти інфраструктури: Панамський канал, шахти й мінеральні ресурси в Африці (зокрема, шахти з видобутку кобальту в Демократичній Республіці Конго), Азії та Південній Америці, підводні нафто- й газопроводи, трансатлантичні кабелі, морські порти в Китаї та Японії, французькі медичні й фармацевтичні компанії та вантажні термінали, заводи з нафтопереробки на Близькому Сході, об'єкти гідроенергетики в Канаді, мережа транзитних газопроводів, що проходить через Надим у російському Сибіру, а також багато менш масштабних об'єктів (наприклад, датський завод із виробництва інсуліну та фабрика, де виробляється антидот від зміїної отрути в Австралії). У Європі до вказаного списку також внесено такі об'єкти: завод у м. Людвігшафен німецького гіганта хімічної промисловості *BASF* (найбільший у світі інтегрований комплекс хімічної промисловості); завод у м. Ерланген компанії *Siemens AG* (виготовлення хімічних речовин).

Тому природно (з огляду на сучасні геополітичні реалії), що, наприклад, газотранспортна система України може розглядатися європейськими і трансатлантичними партнерами як елемент критичної інфраструктури, який має загальноєвропейське значення. Цей аспект, безперечно, заслуговує на увагу під час розгляду проблем захисту національної критичної інфраструктури, вирішення питання власності на об'єкти національної газотранспортної системи, що матиме безпосередній вплив на процес формування ціни на газ для України.

---

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

Для нашої держави може бути корисним досвід імплементації концепції захисту критичної інфраструктури в законодавствах деяких східноєвропейських країн.

Так, наприклад, у 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 ситуація спостерігається в нормативно-правовій базі Словацької Республіки. Там 2007 р. уряд ухвалив «Концепцію критичної інфраструктури у Словацькій Республіці, її захисту та оборони»[15], на основі якої у 2008 р. було розроблено Національну програму захисту та оборони критичної інфраструктури[16]. Однак обидва документи надають лише загальні (концептуальні) характеристики стратегії захисту критичної інфраструктури у Словацькій Республіці, проте не надають детального опису заходів щодо її здійснення.

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

У законодавстві Хорватії термін «критична інфраструктура» визначено так: «діяльність, мережі, послуги, матеріальні блага й інформаційні технології, вихід з ладу або знищення яких значно вплинуло б на здоров'я та безпеку громадян або на діяльність державної влади»[18].

---

[14]*Act* of 26 April 2007 on Crisis Management [Електронний ресурс]. – 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]. – 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]. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10692

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

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

Термін було введено в дію законодавчим актом, призначеним регулювати охоронну діяльність у цій країні.

У законодавстві Республіки Болгарія визначення «критична інфраструктура» було введено в Законі «Про управління в умовах кризи» (був чинний з березня 2005 р. по травень 2009 р.)[19] Оновлене визначення було введено в Постанові Ради Міністрів «Про порядок, спосіб та компетентні органи для визначення критичної інфраструктури та об'єктів і оцінки ризиків» (жовтень 2012р.)[20]

Ситуація, подібна до української, спостерігається в Румунії, де існує близько 15 переліків об'єктів, що відповідають терміну «критична інфраструктура», але вони зустрічаються в різних законодавчих актах[21].

У Російській Федерації досить активно впроваджується й сьогодні є складником внутрішньої та зовнішньої політики РФ у безпековій сфері, а в законодавстві визначено термін «критично важливі об'єкти інфраструктури» як «об'єкти, порушення (або припинення) функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін (або руйнування) економіки країни, суб'єкта або адміністративно-територіальної одиниці, або до суттєвого погіршення безпеки життєдіяльності населення, яке мешкає на цих територіях, на тривалий період часу»[22].

Початком цілеспрямованої роботи в даній сфері можна вважати рішення спільного засідання Ради Безпеки Російської Федерації і президії Державної ради Російської Федерації (13 листопада 2003 р.), відповідно до якого було заплановано й виконано комплекс заходів, спрямованих на забезпечення безпеки населення та захищеності потенційно небезпечних об'єктів від загроз техногенного, природного характеру й терористичних актів. З огляду на те, що в зонах можливого впливу

---

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

[20]*Наредба* за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях // Българският правен портал [Електронний ресурс]. – Режим доступу: http://www.lex.bg/bg/mobile/ldoc/2135816878

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

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

вражаючих чинників при аваріях на критично важливих і потенційно небезпечних об'єктах мешкає понад 90 млн осіб (60% населення РФ), була прийнята Федеральна цільова програма «Зниження ризиків і пом'якшення наслідків надзвичайних ситуацій природного й техногенного характеру в Російській Федерації». У межах цієї програми були створені й на сьогодні успішно функціонують Національний центр управління у кризових ситуаціях МНС РФ і Загальноросійська комплексна система інформування та оповіщення населення в місцях масового перебування.

Нормативно-законодавчими документами, що регламентують захист критично важливих об'єктів у РФ, є такі: «Основи державної політики у сфері забезпечення безпеки населення Російської Федерації та захищеності критично важливих і потенційно небезпечних об'єктів від загроз техногенного, природного характеру й терористичних актів»[23], Перелік критично важливих об'єктів РФ, а також Концепція федеральної системи моніторингу критично важливих, потенційно небезпечних об'єктів і вантажів[24].

Перший з названих документів розвиває і конкретизує основні положення Стратегії національної безпеки Російської Федерації до 2020 року, що стосуються забезпечення безпеки населення й 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 і небезпечних вантажів як функціонального складника єдиної системи попередження та ліквідації надзвичайних ситуацій. Створення системи моніторингу обумовлено необхідністю вдосконалення організації робіт у сфері своєчасного виявлення та попередження загроз техногенного і природного характеру, а також викликано проявами тероризму відносно критично важливих об'єктів у РФ. Система моніторингу створюється для феде-

---

[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 [Електронний ресурс]. – Режим доступу: http://www.garant.ru/products/ipo/prime/doc/70041358/

[24]*Концепция* Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов : распоряжение правительства РФ от 27.08.2005 г. № 1314-р [Електронний ресурс]. – Режим доступу: http://www.garant.ru/hotlaw/federal/124379/

ральних 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.

У Стратегії національної безпеки Російської Федерації до 2020 року[25] вказується на необхідність подолання технологічного відставання РФ у сфері інформатизації, телекомунікації та зв'язку, забезпечення інформаційної безпеки критично важливих об'єктів. Загрози інформаційній безпеці передбачається запобігати завдяки вдосконаленню безпеки функціонування інформаційних і телекомунікаційних систем критично важливих об'єктів та об'єктів підвищеної небезпеки в РФ, підвищенню захищеності корпоративних та індивідуальних інформаційних систем, створенню єдиної інформаційно-телекомунікаційної підтримки в системі забезпечення національної безпеки.

Задля реалізації основних положень вказаної Стратегії, відповідно до якої одним зі способів запобігання загрозам інформаційній безпеці РФ є вдосконалення безпеки функціонування інформаційних і телекомунікаційних систем критично важливих об'єктів інфраструктури та об'єктів підвищеної небезпеки, Радою Безпеки Російської Федерації було розроблено Основні напрями державної політики у сфері забезпечення безпеки автоматизованих систем управління виробничими й технологічними процесами критично важливих об'єктів інфраструктури РФ (липень 2012 р.) У документі йдеться про єдину державну систему виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру й оцінки рівня реальної захищеності її елементів, що включає сили та засоби виявлення і попередження комп'ютерних атак, а також органи управління різних рівнів, до повноважень яких належить питання забезпечення безпеки автоматизованих систем управління критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури.

У названому документі визнається, зокрема, наявність практики здійснення іноземними фірмами технічного обслуговування та віддаленого налаштування автоматизованих систем управління критично важливих об'єктів у цілому або їх складників, а також телекомунікаційного обладнання, що належить до критичної інформаційної інфраструктури; прагнення організацій-розробників програмного забезпечення автоматизованих систем управління до зниження витрат і, як

[25] *Об утверждении* Стратегии национальной безопасности Российской Федерации до 2020 года : указ президента Российской Федерации от 12.05.2009 г. № 537 [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/news/436.html

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. У жовтні 2011 р. набув чинності 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, адже в ньому виокремлюються такі крупномасштабні лінійні об'єкти, як трубопроводи й магістральні ЛЕП, що мають суттєві особливості стосовно організації охорони.

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

• визначення терористичних загроз з-поміж основних чинників, що визначають напрями єдиної державної політики Російської Федерації у сфері цивільної оборони;

• удосконалення 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;

• збереження об'єктів, необхідних для сталого функціонування економіки та виживання населення у воєнний час.

Аналізуючи тенденції розвитку законодавчої бази РФ стосовно захисту критично важливих об'єктів, варто наголосити на тому, що введення категорії «критично важливі об'єкти» не має зводитися до створення ще одного переліку об'єктів, які знаходяться під наглядом і контролем з боку уповноважених органів.

Крім створення нормативно-правової основи для функціонування систем захисту критично важливих об'єктів у РФ, активно здійснюються та фінансуються наукові дослідження у сфері розвитку методів оцінки зовнішніх і внутрішніх небезпечних для критично важливих

---

[26]*О безопасности* объектов топливно-энергетического комплекса : федеральный закон Российской Федерации от 21.07.2011 г. № 256-ФЗ [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 3.09.2011 г. № Пр-2613 [Електронний ресурс]. – Режим доступу: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=125214

об'єктів процесів, аналізу ризику та вразливості систем фізичного захисту цих об'єктів[28], а також створення ефективної системи підготовки керівних кадрів і спеціалістів у зазначеній сфері[29].

2. Основні складники досягнення цілей стратегії захисту критичної інфраструктури

Забезпечення безпеки критичної інфраструктури є складною проблемою для кожної держави і, посилаючись на думку американського дослідника Теда Льюіса[30], головними викликами в цьому напрямі варто назвати такі:

• значущість кожного із секторів критичної інфраструктури та її самої в цілому;

• управління безпекою за умов взаємозалежності діяльності урядових органів, державного і приватного секторів, а також регулюючих та економічних чинників;

• обмін інформацією, який уже на стадії збору та співставлення необхідних даних є значною проблемою, оскільки державні органи є здебільшого вертикально орієнтованими структурами, які переважно накопичують інформацію, а елементи критичної інфраструктури розпорошені між державою та чималою кількістю приватних компаній;

• взаємозалежність елементів і секторів критичної інфраструктури внаслідок притаманних їм комплексних різнорівневих взаємодій та взаємозв'язків.

Зважаючи на те, що більшість систем критичної інфраструктури має мережеву архітектуру, Т. Льюіс вважає, що захищати необхідно передусім головні «вузли» цих систем[31]. Саме у такий спосіб з'являється можливість дотримуватися «правила 80–20%», за якого 80% ресурсів мають витрачатися на 20% території країни, а також використовува-

---

[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. – № 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.

[31] Там само.

ти 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 і Руді Даркін звертають увагу на такі проблеми[32]:

• розподіл повноважень із захисту критичної інфраструктури між федеральною та місцевою (влада штату) владами;

• 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 і мереж (критичної інфраструктури) починається з етапу ідентифікації (визначення) елементів, що мають розглядатися як критична інфраструктура. Як свідчить досвід розвинених країн, у яких функціонують нормативно-правові й організаційні механізми захисту критичної інфраструктури, здійснення етапу ідентифікації дозволяє систематизувати сукупність елементів критичної інфраструктури, визначити її основні сектори.

2.1. Оцінка загроз критичній інфраструктурі

З-поміж загроз критичній інфраструктурі називають пандемії, промислові аварії, терористичну та злочинну діяльності, кібератаки, стихійні лиха тощо[33]. Держава має 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, що з'явилася у США після урагану Катріна (наприкінці серпня 2005 р.), визнаного найбільш руйнівним в історії країни (постраждала від стихійного лиха територія становила близько 200 тис. км^2 – за розміром майже третина території України). У результаті аналізу подій у планах захисту критичної інфраструктури значно більше уваги стали приділяти підходу до оцінки ризиків, що враховує весь комплекс загроз (*all-hazard approach*).

---

[32] *Potholes* and Detours in the Road to Critical Infrastructure Protection Policy / T. G. Lewis, R. Darken // Homeland Security Affairs. – 2005. – Vol. 1. – P. 2–15.

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

З-поміж техногенних загроз особлива увага приділяється спробам втручання в роботу автоматизованих систем управління технологічним процесом на підприємствах та об'єктах інфраструктури. Хоча досі не повідомлялося про факти руйнувань унаслідок кібератак на критичну інфраструктуру, однак було зафіксовано 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 напрямом для адміністрації президента Обами[36]. Для забезпечення безпеки найбільш важливих систем уряд США надає громадськості та приватним компаніям (установам) можливість отримувати оперативну й ефективну допомогу з кібербезпеки.

У Сполучених Штатах міністерство оборони є головним ідеологом розроблення не тільки технічних засобів розвідки, а й розвитку інформаційних і телекомунікаційних технологій, головним елементом якого є застосування глибоко ешелонованого захисту (*defense-in-depth*). Цей підхід передбачає використання інформаційних систем, що складаються з багатошарових систем безпеки та процедур, які використовують активні й 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 і попередженням злочинів, спрямованих проти національних інформаційних систем.

З-поміж технічних засобів захисту, використовуваних нині у США, необхідно виділити концептуальну модель ешелонованої багатошарової системи інформаційної безпеки (безпеки інформації) стандарту *ISO/IEC* 15408, яка містить набір компонентів, що реалізують функції моніторингу, захисту й адаптації інформаційних ресурсів, а разом дозволяють поетапно запобігти проникненню, визначити факт порушен-

---

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

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

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

ня, локалізувати об'єкт впливу, нейтралізувати й видворити порушника, відновити втрачені функції системи.

Зважаючи на зростання негативних наслідків для держави, які завдаються кібератаками на інформаційну інфраструктуру органів державної влади, та на небезпеки, пов'язані з можливими атаками на промислові об'єкти, дедалі частіше лунають заклики посилити відповідальність за вчинення кіберзлочинів. Так, один із членів Ради Федерації РФ нещодавно запропонував прирівняти зламування державних вебсайтів до захоплення органів влади, обґрунтовуючи свою пропозицію тим, що через такі сайти надаються різні держпослуги[37].

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

З-поміж останніх терористичних актів, спрямованих на руйнування інфраструктурних мереж, особливу увагу привернули вибухи, скоєні в Туреччині протягом двох тижнів у липні-серпні 2012 р. на ділянках нафтопроводу Кіркук – Джейхан, яким транспортується іракська нафта до середземноморських портів. Перший вибух було здійснено 21 липня, а другий – 6 серпня у провінції Мардін. У результаті першого теракту одну з двох паралельних труб нафтопроводу було сильно пошкоджено, а функціонування іншої з міркувань безпеки призупинено. У здійсненні обох терактів підозрюють бойовиків сепаратистського групування «Робітнича партія Курдистану» – організації, визнаної ООН і ЄС терористичною[38].

На жаль, загроза вчинення терактів залишається украй актуальною і для європейських країн, про що, зокрема, свідчить скоєний 22 червня 2011 р. у 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 й дизельного палива) забрав життя 8 осіб і спричинив поранення 92 осіб (15 із них – тяжкі), постраждали найближчі будівлі (у т.ч. міністерства нафтової промисловості), а також злочин, вчинений терористом на острові Утейа, в результаті якого загинуло 69 осіб (учасники молодіжного літнього табору, який щорічно організовує 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 // Коммерсант.ua [Електронний ресурс]. – 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). У результаті вибуху загинуло 11 і понад 100 осіб постраждало. 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 також відсутні сепаратистські чи екстремістські організації, однак це не гарантувало уникнення терактів.

У серпні 2012 р. у Сполучених Штатах була розкрита терористична організація з найменуванням *FEAR* (абревіатура від *Forever Enduring Always Ready* – «вічно стійкий, завжди готовий»), яка планувала скоєння терактів у штаті Джорджія та у столиці США – Вашингтоні[39]. Її члени планували вибухи автомобілів державних діячів і суддів, вибухи в місцях масового скупчення людей і навіть убивство президента країни.

Стосовно 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 частиною 2 ст. 258 КК (терористичний акт).

Терористичні акти завжди мають значний резонанс. Однак при цьому не слід забувати про те, що техногенні аварії часто можуть мати наслідки тяжчі, ніж у випадку деяких терактів. Наприклад, вибух природного газу в 10-поверховому будинку у Дніпропетровську, що стався 13 жовтня 2007 р., забрав життя 23 людей (у т.ч. семи 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 масштабних (за площею, протяжністю тощо) об'єктів (підприємств, нафтой газопроводів, заповідників) залишається нерозв'язаною не тільки

---

[39] *«Anarchists»* accused of murder; broader plot against government / CNN [Електронний ресурс]. – 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.html

в Україні, а й у інших країнах. Наприклад, у жовтні 2011 р. в Німеччині було здійснено спробу підпалу (вибуху) на залізниці: 18 саморобних вибухових пристроїв (ємності з підпалювальною сумішшю) було знайдено в комунікаційних шахтах, у яких прокладені кабелі, що з'єднують центральний комп'ютер зі стрілками й семафорами. Унаслідок цього було призупинено рух понад 200 електричок. Якби теракт відбувся, наслідки були б жахливими.

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

Суттєвою частиною аналізу й оцінки загроз є вивчення взаємозв'язку між елементами критичної інфраструктури всередині секторів, і між різними секторами. Одним із прикладів реалізації такого взаємозв'язку є каскадна аварія, що сталася внаслідок відмови мережі енергопостачання в північно-східних штатах США та східних провінціях Канади 2003 р.[41], унаслідок чого 10 млн осіб у провінції Онтаріо та 45 млн осіб із восьми штатів США зіткнулися з перебоями в забезпеченні електроенергією, водою, зв'язком, послугами муніципального транспорту. Крім того, зупинилися виробничі лінії на підприємствах, зросла кількість випадків хуліганства та здійснення пограбувань, спостерігалися відмови систем контролю за перетином державного кордону, систем освітлення злітно-посадкових смуг аеродромів і систем фізичного захисту об'єктів.

Іншим прикладом масштабної аварії, що привертає увагу з огляду на каскадні наслідки, є події з масовим відключення електропостачання в Індії наприкінці липня 2012 р. Перша аварія (30 липня) викликала майже повний колапс на півночі країни, охопивши дев'ять регіонів із загальною чисельністю населення 390 млн осіб. Відновити електропостачання для життєво важливої інфраструктури (аеропорти, залізниця, метро) вдалося тільки за 5 год після відключення. Повного відновлення було досягнуто за 16,5 год після аварії. Повторна аварія (31 липня) охопила ще більший регіон (крім північних регіонів, були охоплені частини східних і північно-східних регіонів Індії). Енергетична корпорація Індії *(Power Grid Corporation of India Ltd)* відновила енергопоста-

[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. – 2004. – April [Електронний ресурс]. – Режим доступу: https://reports.energy.gov/BlackoutFinal-Web.pdf

чання життєво важливих об'єктів після 2,5 год, однак населенню (в т.ч. 16,5 млн осіб, що мешкають у столиці – м. Делі) довелося чекати понад 8,5 год. Повне відновлення функціонування енергетичної мережі було досягнуто лише 1 серпня (за 32,5 год після повторної аварії).

За оцінками аналітиків, під час аварії близько 600 млн осіб були позбавлені електропостачання та можливості користуватися пасажирським електротранспортом. Уже за попередніми оцінками наслідки згаданих аварій для промисловості та підприємництва сягають сотні мільйонів доларів США. Також варто зазначити, що інформування населення про інцидент не було здійснено на належному рівні ані з боку державних відомств, ані з боку Енергетичної корпорації Індії[42].

Аварія мала й політичні наслідки: було призначено нового керівника міністерства енергетики Індії. За словами генерального директора Конфедерації промисловців Індії Чандраджіт Банерджі, «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». Водночас у Індії розподільні компанії постійно борються з боржниками і стикаються зі значними (в середньому по країні – 27%) втратами електроенергії. На думку експертів Центру стратегічних і міжнародних досліджень (Вашингтон, США), непросто усунути недоліки енергетичної інфраструктури, які на сьогодні є в Індії, не розв'язавши складні політичні проблеми від питання права на земельну власність до непосильних для держави соціальних субсидій[43].

Цікавим є аналіз причин згаданої аварії. Експерти вказують на погодні умови: засуху, викликану слабким сезоном мусонів (майже на 20% менше за середні показники), та високу температуру повітря. Відповідно, підвищилося використання кліматичного обладнання (кондиціонерів) в офісах і житлових будинках, а також використання систем іригації (насосів для накачування води для поливів) сільськогосподарських посівів. Водночас відсутність дощів спричинила зниження рівня води у водоймах, а отже, 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 па-

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

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

сажирські авіаперевезення у Європі знизився 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 зазначити, що розбудова критичної інфраструктури може викликати міжнародні суперечності. Показовим є приклад протидії упровадженню 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 із аргументами проти створення Галілео). Останні усвідомлювали, що названа система створюється як альтернатива, що витіснить американську Глобальну систему позиціонування[45].

2.2. Ідентифікація елементів критичної інфраструктури

Розроблення методології ідентифікації об'єктів критичної інфраструктури потребує окремого дослідження. Світовий досвід свідчить, що навіть для такого потужного відомства, як міністерство внутрішньої безпеки США, завдання розроблення єдиної методології ідентифікації об'єктів, систем і сервісів, критичних на національному рівні, а також створення всеосяжної бази даних для ведення їх реєстру, виявилося складним[46].

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

---

[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/

[45] *Tanner, J. C.* Galileo is go, despite Pentagon pressure – First Mile : Brief Article // Telecom Asia. – 2012. – 31 May [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. – 2004. – October. – 19 p.

[47] Там само.

На території РФ функціонує майже 5 тис. критично важливих об'єктів, порушення (або припинення) функціонування яких призведе до втрати управління, руйнування інфраструктури, незворотних негативних змін в економіці країни або адміністративно-територіальної одиниці, суттєвого погіршення безпеки життєдіяльності населення, яке проживає на цих територіях, на тривалий період часу[48].

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

Спроба визначити критичну інфраструктуру на рівні ЄС була здійснена у 2005 р. під час підготовки Зеленої книги, присвяченої цій проблемі. До списку об'єктів критичної інфраструктури відповідно до Зеленої книги ЄС[49] 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. Однак у найближчій перспективі Директивою ЄС[50] лише два сектори – енергетика і транспорт – було визнано пріоритетними. До сектору енергетики було включено такі системи та об'єкти: електромережі та об'єкти з генерування й передачі електроенергії; нафтовидобувна та нафтопереробна промисловість, нафтопроводи і сховища; газовидобувна промисловість, газо-

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

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

[50]*On the identification* and designation of European critical infrastructures and the assessment of the need to improve their protection : Council Directive 2008/114/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

проводи, термінали зрідженого газу. До сектору транспорту належать такі його види та об'єкти: автодорожній, залізничний та авіаційний транспорт; річковий флот, океанічний і морський флот; порти.

Таблиця 1

Порівняльна таблиця: сектори критичної інфраструктури

Держава / Сектор критичної інфраструктури	Австралія	Австрія	Велика Британія	Канада	Італія	Нідерланди	Німеччина	Нова Зеландія	Норвегія	Польща	РФ	США	Фінляндія	Франція	Швеція
Банки та фінанси	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х
Водопостачання	х	х	х	х	х	х	х	–	х	х	–	х	х	х	–
Дамби	–	–	–	–	–	–	–	–	–	–	–	х	–	–	–
Енергетика	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х
Комунальні мережі	х	х	–	–	–	–	х	–	х	–	–	–	х	–	–
Національні символи	х	–	–	х	–	–	–	–	–	–	–	х	–	–	–
Небезпечні матеріали (ХБРЯ)	–	–	х	х	–	–	–	–	–	х	–	х	–	–	–
Оборонно-промисловий комплекс	х	–	–	х	–	–	–	–	–	–	х	х	х	х	–
Органи виконавчої влади	х	–	х	х	–	х	х	х	х	х	–	х	–	–	х
Органи правосуддя	–	–	х	–	–	х	х	х	–	–	–	х	–	–	–
Охорона здоров'я	х	х	х	х	х	х	х	–	х	х	–	х	х	х	–
Паливно-енергетичний комплекс	х	–	х	х	х	х	х	х	х	х	х	х	–	–	–
Поштові служби	–	х	–	–	–	–	–	–	–	–	–	х	–	–	–
Сільське господарство	х	–	х	х	–	х	х	–	–	х	–	х	х	–	–
Система управління повітряним рухом	–	–	–	–	–	–	–	–	–	–	–	–	–	–	х

Закінчення табл.

Держава / Сектор критичної інфраструктури	Австралія	Австрія	Велика Британія	Канада	Італія	Нідерланди	Німеччина	Нова Зеландія	Норвегія	Польща	РФ	США	Фінляндія	Франція	Швеція
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	–	–	–	–	–	–

Варто зазначити, що суттєві відмінності між списками секторів і переліками об'єктів, які визначаються критичною інфраструктурою у США, Канаді та ЄС майже відсутні. Як уже згадувалося, лише у Сполучених Штатах Америки до цих списків було внесено національні пам'ятки та символи, а також комерційні об'єкти (музеї, виставки й інші місця масового скупчення людей), натомість у ЄС – науково-дослідні установи.

Під час визначення елементів критичної інфраструктури (віднесення об'єктів до критичної інфраструктури) будується ієрархія критеріїв, що 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 та оборона* (недопущення порушень в управлінні державою, зниження боєздатності збройних сил, розголошення таємної інформації);

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

При визначенні потенційних елементів критичної інфраструктури враховують такі чинники та характеристики[51]:

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

• тяжкість можливих наслідків за такими показниками:

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

– економічна шкода (вплив на ВВП, розмір економічних втрат – і прямих, і непрямих);

– екологічна шкода (вплив на населення і навколишнє середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме й коли виявлятимуться збитки, пов'язані із втратою чи відмовою об'єктів критичної інфраструктури).

Ще одним прикладом категоризації є побудова критеріїв для визначення критично важливих об'єктів паливно-енергетичного комплексу РФ. При цьому враховуються такі показники[52]:

• критична важливість об'єкта для інфраструктури й життєзабезпечення паливно-енергетичного комплексу;

• масштаби можливих соціально-економічних наслідків, що виникнуть унаслідок аварії на об'єкті;

• наявність критичних елементів, потенційно небезпечних ділянок і вразливих місць на об'єкті.

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

З огляду на складний безпековий стан на Близькому Сході, значний інтерес становлять принципи ідентифікації критичної інфраструктури

---

[51] *On the identification* and designation of European critical infrastructures and the assessment of the need to improve their protection : Council Directive 2008/114/ EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[52] *О безопасности* объектов топливно-энергетического комплекса : федеральный закон Российской Федерации от 21.07.2011 г. № 256-ФЗ // ИПС «Закон». [Електронний ресурс]. – Режим доступу: http://ntc.duma.gov.ru/

в Ізраїлі. Відповідно до підходів, використовуваних у цій країні, при ідентифікації критичної інфраструктури враховуються такі ознаки для класифікації[53]:

• символічна значимість об'єктів;

• залежність основних процесів життєзабезпечення суспільства від тієї чи іншої інфраструктури;

• наявність складних взаємозв'язків і залежностей між інфраструктурами.

Згідно з таким підходом об'єкти культурної спадщини (музеї, архіви, культові споруди та інші пам'ятки) віднесені до числа об'єктів, що мають захищатися першочергово. Також до систем з високим символічним значенням ізраїльські експерти відносять ті, що забезпечують здатність держави контролювати ситуацію (сайти органів влади, центральні ЗМІ тощо), а також ті, втрата яких завдасть значної шкоди іміджу держави.

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

Стосовно 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.

2.3. Державно-приватне партнерство у сфері захисту критичної інфраструктури

У провідних країнах світу цьому питанню приділяють значну увагу. Наприклад, у Національній стратегії захисту критичної інфраструктури Канади[54] зазначається, що відповідальність за забезпечення захисту критичної інфраструктури країни мають нести і всі державні органи, і приватний сектор, а також усі канадці як члени канадського суспільства. Останні повинні бути готовими до протистояння надзвичайним ситуаціям щонайменше упродовж перших 72 годин з моменту тієї чи іншої події.

---

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

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

Участь уряду Канади в державно-приватному партнерстві розглядається з погляду[55]:

• надання операторам і власникам об'єктів та систем критичної інфраструктури вчасної і 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 зацікавленими суб'єктами процесу, спрямованої на розроблення пріоритетів та основних заходів зі зменшення загроз у кожному із секторів критичної інфраструктури.

Стосовно Європейської програми захисту критичної інфраструктури[56], то відповідальність за захист її об'єктів покладається і на їх власників (операторів), і на уряд відповідної держави-члена Європейського Союзу.

2.4. Інформаційний обмін щодо загроз критичній інфраструктурі

Обмін інформацією про можливі загрози й наслідки їх реалізації, а також про уразливість критичної інфраструктури відіграє головну роль у процесі аналізу загроз критичній інфраструктурі. Усвідомлюючи необхідність створення мережі відповідної системи, Європейська Комісія ухвалила рішення про створення Європейської інформаційної мережі попередження *(European Critical Infrastructure Warning Information Network, CIWIN)*.

Основним завданням мережі 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 погляду забезпечення безпеки об'єктів критичної інфраструктури. Вартість підтримки функціонування програмно-апаратної частини *CIWIN* щорічно становить понад 600 тис. євро[57].

Іншим прикладом реалізації подібного підходу є мережа з обміну інформацією *(Trusted Information Sharing Network, TISN)*, створена

---

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

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

[57]*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

урядом Австралії у квітні 2003 р. Вона функціонує як форум, на якому власники та оператори критичної інфраструктури можуть обмінюватися інформацією про загрози, вразливості і 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 є всі сектори й елементи, які зазвичай відносять до критично важливих об'єктів і критичної інфраструктури. З-поміж них є такі складні масштабні промислові комплекси, як 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 й передачі інформації тощо.

Беручи за основу визначення терміна «національні інтереси», поданого в Законі України «Про основи національної безпеки»[58], можна стверджувати, що критична інфраструктура включає ті матеріальні чи віртуальні (інформацію, що зберігається в реєстрах, базах даних, інформаційних системах органів влади, або передається засобами Національної системи конфіденційного зв'язку) об'єкти й системи, від стабільного функціонування яких залежить можливість досягнення національних інтересів держави.

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

Уперше в офіційних документах України термін «критична інфраструктура» згадується у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства[59], однак,

---

[58] *Про основи* національної безпеки : закон України від 19.06.2003 р. № 964-IV // ВВР. – 2003. – № 39. – Ст. 351 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15

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

на жаль, робота з упровадження цих рекомендацій, у т.ч. стосовно захисту критичної інфраструктури від широкого кола загроз, у подальшому припинилася.

У новій Стратегії національної безпеки[60] в IV розділі «Стратегічні цілі та основні завдання політики національної безпеки» з-поміж головних завдань політики національної безпеки у внутрішній сфері одним зі способів зміцнення енергетичної безпеки (п. 4.3.4.) названо «дієвий захист критичної інфраструктури паливно-енергетичного комплексу від еколого-техногенних впливів і зловмисних дій», а одним зі способів забезпечення інформаційної безпеки (п. 4.3.8.) «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони й 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 погляду національної та державної безпеки в Україні здійснювалася за окремими типами загроз, наприклад кіберзагроз. Так, Указом Президента України від 10.12.2010 р. № 1119/2010 введено в дію рішення РНБО[61], 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».

У Проекті закону України «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» (від 31.08.2012 р. № 11125, відкликаний 12.12.2012р.)[62] передбачалося внесення змін до Закону України «Про основи національної безпеки України», зокрема введення таких термінів:

• об'єкти критичної інфраструктури – об'єкти, вплив на які, зокрема через об'єкти критичної інформаційної інфраструктури, може мати

---

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

[61]*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

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

наслідки, що безпосередньо зачіпають національну безпеку, у т.ч. безпеку людини і громадянина, суспільства й 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 й місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур і 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 враховував, що в нашій державі паралельно вже діють Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків (Положення затверджене Постановою Кабінету Міністрів України від 15.08.2007 р. № 1051), Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру (Положення затверджене постановами Кабінету Міністрів України від 03.08.1998 р. № 1198, зміни – від 29.07.1999 р. № 1376, від 09.08.2001 р. № 1006, від 15.05.2003 р. № 717, від 04.09.2003 р. № 1402, від 08.12.2006 р. № 1700), Єдина державна система цивільного захисту населення й територій (Закон України «Про правові засади цивільного захисту» від 24.06.2004 р. № 1859-IV).

Перераховані системи створені зокрема і для захисту життєво важливих для держави об'єктів від окремих видів загроз, у зв'язку із 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 і розпорошення ресурсів, а з іншого – прогалин у розподілі відповідальності за захист об'єктів і систем, критично важливих для існування держави, захисту національних інтересів, забезпечення безпеки населення й довкілля. Це також спричиняє слабкість і недостатність існуючих механізмів координації зусиль міністерств і відомств щодо забезпечення захисту об'єктів, які у світі зазвичай відносять до критичної інфраструктури.

У законодавстві України є низка окремих термінів, переліків об'єктів, що визначають особливий статус об'єктів і систем з погляду захисту національних інтересів, стабільного функціонування держави

в цілому. Усі вони за характеристиками категорії об'єктів «критичної інфраструктури» тією чи іншою мірою відповідають світовому досвіду. До цієї категорії, очевидно, варто віднести:

• підприємства, що мають стратегічне значення для економіки й безпеки держави[63];

• об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами[64];

• об'єкти, включені до державних реєстрів потенційно небезпечних об'єктів[65] та об'єктів підвищеної небезпеки[66] (у т.ч. внесені до Переліку особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому середовищу[67]);

• важливі державні об'єкти[68];

• об'єкти, що підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період[69];

• нерухомі об'єкти культурної спадщини;

---

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

[64]*Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності (зі змінами) : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

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

[66]*Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2245-14

[67]*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 [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?code=765-2000-%EF

[68]*Про затвердження* єдиної державної системи запобігання, реагування та припинення терористичних актів та мінімізації їх наслідків : постанова Кабінету Міністрів України від 15.08.2007 р. № 1051 (для службового користування) [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?uid=1136.1049.0

[69]*Щодо затвердження* переліку об'єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період : постанова Кабінету Міністрів України від 24.04.1999 р. № 675-019.

• особливо важливі об'єкти електроенергетики[70];
• особливо важливі об'єкти нафтогазової галузі[71].

Постановою Кабінету Міністрів України від 23.12.2004 р. № 1734 було затверджено перелік підприємств, що мають стратегічне значення для економіки та безпеки держави. До нього увійшли великі промислові об'єкти, комбінати, заводи, науково-дослідні установи, науково-виробничі об'єднання, конструкторські бюро тощо. Цей перелік систематично оновлюється міністерствами та іншими центральними органами виконавчої влади та подається щороку до Мінекономрозвитку України для зведення пропозицій з обґрунтуваннями за кожним об'єктом задля прийняття Кабінетом Міністрів України рішення про внесення змін до зазначеного переліку. Основною метою вказаної Постанови є, напевно, обмеження щодо приватизації таких підприємств і установ. У ній, зокрема, зазначається, що Фонду державного майна у планах розміщення акцій підприємств, які не увійшли до даного переліку підприємств, не передбачати залишення акцій у державній власності, крім випадків, визначених законодавством.

У новій редакції Воєнної доктрини України (ст. 28)[72] як про один із напрямів військово-промислової політики держави згадується необхідність «залишення в 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», вказаний вище перелік використовується як базовий при визначенні підвищених вимог щодо фізичного захисту тих чи інших об'єктів. Низка таких об'єктів охороняється Державною службою охорони відповідно до Постанови Кабінету Міністрів України «Про за-

---

[70]*Про електроенергетику :* закон України від 16.10.1997 р. № 575/97-ВР [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/575/97-%D0%B2%D1%80; *Про затвердження* переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії зі спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 р. № 1170 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1170-2003-%D0%BF

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

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

ходи щодо вдосконалення охорони об'єктів державної та інших форм власності» від 10.08.1993 р. № 615[73]. Нею також затверджено перелік об'єктів, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами, до якого, зокрема, віднесено 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, у яких розміщуються органи влади Автономної Республіки Крим;

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

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

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

• підприємства, спеціалізовані цехи й 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 й інші державні об'єкти зберігання матеріальних цінностей на суму понад 20 тис. мінімальних розмірів заробітної плати; державні універсальні магазини зі щоденною виручкою в сумі понад 5 тис. мінімальних розмірів заробітної плати, їхні склади, центральні каси;

• склади мобілізаційного резерву, центральні та обласні аптечні склади;

• об'єкти водопостачання населених пунктів з резервуарами питної води;

• морські порти;

• особливо важливі мости на залізничних магістралях та автомагістралях державного значення;

• сховища нафти й газу, особливо важливі об'єкти нафтогазової галузі;

---

[73]*Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності (зі змінами) : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

• 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 виставковий 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 і регіональні центри оцінювання якості освіти, їхні об'єкти, пункти тестування, а також місця проведення та перевірки результатів зовнішнього незалежного оцінювання.

Крім Державної служби охорони, що функціонує у структурі МВС, інші відомства теж опікуються охороною важливих об'єктів, які належать сфері їх підзвітності. Так, наприклад, відповідно до вимог Постанови Кабінету Міністрів України «Щодо затвердження переліку об'єктів, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період» від 24.04.1999 р. № 675-019, а також задля здійснення та вдосконалення системи охорони шлюзів як стратегічно важливих об'єктів Мінтранспорту України в 2004 р. у складі ДП «Укрводшлях» було створено загони для охорони судноплавних шлюзів[74], а для охорони особливо важливих об'єктів підприємств паливно-енергетичного комплексу Мінпаливенерго створило в 2007 р. відомчу воєнізовану охорону[75].

Згідно з Розпорядженням Кабінету Міністрів України від 27.05.2009 р. № 578-р Мінпаливенерго разом з МВС і МНС мало забезпечувати відповідно до вимог законодавства організацію охорони (зокрема пожежної) особливо важливих об'єктів нафтогазової галузі, фінансування якої здійснюється за рахунок підприємств, включених до згаданого переліку.

Привертають увагу кілька випадків судового розгляду справ щодо правомірності укладання договорів про послуги Державної служби охорони, від послуг якої господарюючі суб'єкти відмовляються, аргументуючи своє рішення наявністю на об'єктах власних підрозділів охо-

---

[74]*Про затвердження* Положення про загін відомчої охорони судноплавних шлюзів та Запорізького району гідротехнічних споруд : наказ Міністерства транспорту України від 16.02.2004 р. № 89 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0268-04

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

рони та відсутністю чіткої методики визначення переліку об'єктів, що мають підлягати охороні[76].

Зокрема, в судовій справі Державної служби охорони проти ДП «Придніпровська залізниця» було встановлено: незважаючи на те, що до Переліку об'єктів, які 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.

Відповідно до Постанови Кабінету Міністрів України від 13.12.2000 р. № 1833-034 в умовах надзвичайного стану та особливого періоду низка залізничних мостів підлягає обов'язковій охороні. Утім, в умовах мирного часу вони не є особливо важливими мостами на залізничних магістралях і автомагістралях державного значення. Узагалі, категорія мостів визначається тільки за їхньою вантажністю й довжиною (наприклад, великий міст – це міст повною довжиною понад 100 м, а малий – до 25 м)[77], 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), в мирний час спричиняє ситуацію, коли важливість об'єкта визначається керівництвом відомства, якому даний об'єкт підпорядковується.

Наприклад, перелік об'єктів залізничного транспорту, які підлягають охороні підрозділами відомчої воєнізованої охорони, затверджується начальником залізниці за погодженням з Управлінням воєнізованої охорони Укрзалізниці[78]. При цьому не розглядається загальнодержавне чи регіональне значення об'єкта.

Одна з основних категорій об'єктів, визначена в національному законодавстві й така, що може бути використана при визначенні критично важливих об'єктів та інфраструктури в Україні, – це потенційно небез-

---

[76]*Постанова* Вищого господарського суду України / Справа № 5005/2220/2011. – 06.10.2011 р. // Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/18544529; *Рішення* Господарського суду Донецької області / Справа № 43/271пд, 04.03.2010 р. // Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/8236600

[77]Згідно з Інструкцією щодо утримання штучних споруд, затвердженою Наказом Укрзалізниці від 27.04.1999 р. № 124-Ц.

[78]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.

печні об'єкти. У межах 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 введення 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 т.ч. транскордонного характеру, пов'язаних із функціонуванням небезпечних об'єктів.

Порядок проведення ідентифікації потенційно небезпечних об'єктів встановлено відповідною методикою[79]. Одним з етапів процедури ідентифікації є виявлення за результатами аналізу джерел небезпеки, які за певних умов (аварії, порушення режиму експлуатації, виникнення природних небезпечних явищ тощо) можуть спричинити надзвичайну ситуацію, а також оцінка можливих наслідків надзвичайної ситуації для кожного із джерел небезпеки (кількість загиблих, постраждалих, тих, яким порушено умови життєдіяльності, матеріальні збитки) з використанням відповідної методики[80]. При встановленні рівня можливих надзвичайних ситуацій визначається таке:

• територіальне поширення ймовірних надзвичайних ситуацій;

• кількість осіб, умови життєдіяльності яких можуть бути порушені в результаті можливої аварії на об'єкті;

• збитки від наслідків можливих надзвичайних ситуацій.

Таким чином, основною характеристикою, що враховується під час визначення та віднесення об'єктів до категорії «потенційно небезпечні об'єкти» є розмір наслідків можливої аварії на об'єкті. Зважаючи на загальноприйняте визначення критичної інфраструктури, частина переліку потенційно небезпечних об'єктів може увійти й до переліку об'єктів критичної інфраструктури.

Необхідність систематизації та категоризації об'єктів в окремих галузях задля визначення переліку об'єктів, на яких мають діяти підвищені вимоги щодо фізичного захисту, знайшла своє відображення

---

[79]*Про затвердження* Методики ідентифікації потенційно небезпечних об'єктів : наказ МНС України від 23.02.2006 р. № 98 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0286-06

[80]*Про затвердження* Методики оцінки збитків від наслідків надзвичайних ситуацій техногенного і природного характеру : постанова Кабінету Міністрів України від 15.02.2002 р. № 175 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/175-2002-%D0%BF

в низці нормативних актів. Зокрема, Розпорядженням Кабінету Міністрів України від 27.05.2009 р. № 578-р визначено перелік особливо важливих об'єктів нафтогазової галузі[81]:

• об'єкти підприємств нафтогазової галузі, які мають стратегічне значення для економіки і безпеки держави (визначені Постановою Кабінету Міністрів України від 23.12.2004 р. № 1734);

• об'єкти підприємств нафтогазової галузі, які згідно зі 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 24.04.1999 р. № 675-019);

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

У згаданому переліку є такі об'єкти: магістральні нафтопроводи; відводи магістрального нафтопроводу; нафтоперекачувальні станції; лінійні виробничі диспетчерські станції; кінцеві пункти; морські нафтові термінали; цехи видобування нафти й газу; дільниці підготовки та перекачування нафти, у т.ч. із 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 зі спеціалізованими підрозділами інших центральних органів виконавчої влади[82]: диспетчерські пункти оперативно-технологічного управління; електропідстанції напругою понад 330 кВ; теплоелектростанції; гідроелектростанції; теплоелектроцентралі. Охорону об'єктів цієї категорії мають узгоджено здій-

---

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

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

снювати підрозділи відомчої воєнізованої охорони Міненерговугілля, МВС, Мінінфраструктури.

Ще одна категорія, яка за українським законодавством (з огляду на можливі терористичні загрози) є елементом критичної інфраструктури – нерухомі пам'ятки культурної спадщини. До об'єктів культурної спадщини відповідно до Закону України «Про охорону культурної спадщини»[83] 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, занесені до Державного реєстру нерухомих пам'яток України. Довкола них встановлюється охоронна зона, зона регулювання забудови, зона ландшафту, що охороняється, зона охорони археологічного культурного прошарку, в межах яких діє спеціальний режим їх використання.

Крім указаних категорій (переліків об'єктів) у національному законодавстві окремими нормативно-правовими актами регулюється функціонування таких систем і служб:

- Національна система конфіденційного зв'язку[84];
- платіжні системи[85];
- Система екстреної допомоги населенню за єдиним номером 112[86];
- аварійно-рятувальні служби.

З огляду на світовий досвід, вони належать до критичної інфраструктури.

У галузі зв'язку та інформаційних систем потрібно згадати Національну систему конфіденційного зв'язку та платіжні системи. Перша

---

[83]*Про охорону* культурної спадщини : закон України від 08.06.2000 р. № 1805-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1805-14

[84]*Про Національну* систему конфіденційного зв'язку» (зі змінами) : закон України від 10.01.2002 р. № 2919-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2919-14

[85]*Про платіжні* системи та переказ коштів в Україні : закон України від 05.04.2001 р. № 2346-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2346-14

[86]*Про систему* екстреної допомоги населенню за єдиним телефонним номером 112 : закон України від 13.03.2012 р. № 4499-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/4499-17

згідно із Законом України «Про Національну систему конфіденційного зв'язку»[87] є сукупністю 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 в разі введення надзвичайного й воєнного стану. Держспецзв'язок здійснює управління Національною системою конфіденційного зв'язку, забезпечує її функціонування, розвиток, використання та захист інформації.

Друга група інформаційних систем – платіжні, координацію, створення та контроль над функціонуванням яких згідно із Законом України «Про Національний банк України» (ст. 7) здійснює НБУ. 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, Національним банком України розроблено відповідну Концепцію[88]. Крім економічних параметрів платіжних систем, значна увага приділяється й технічному забезпеченню їх надійної роботи, здебільшого інформаційній безпеці.

Важливо зазначити, що до критичної інфраструктури за міжнародним досвідом зазвичай також належать аварійно-рятувальні служби та служби надання екстреної допомоги населенню. У 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 визначено Постановою Кабінету Міністрів України від 04.08.2000 р. № 1214[89]: об'єкти геолого-

---

[87]*Про Національну* систему конфіденційного зв'язку» (зі змінами) : закон України від 10.01.2002 р. № 2919-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2919-14

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

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

розвідки, вугільної промисловості, гірничорудної та нерудної промисловості, нафтодобувної промисловості, хімічної та нафтохімічної промисловості (у т.ч. магістральні нафтопроводи, нафтопродуктопроводи, аміакопроводи, етиленопроводи), металургійної промисловості, машинобудування, енергетики, транспортно-дорожнього комплексу тощо.

На виконання Розпорядження Кабінету Міністрів України від 02.10.2003 р. № 589-р МНС було розроблено Порядок обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами[90]. Чисельність і 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 й визначається керівником державної аварійно-рятувальної служби (формування). Вартість аварійно-рятувального обслуговування об'єктів державними аварійно-рятувальними службами (у т.ч. відшкодування витрат, пов'язаних із ліквідацією надзвичайних ситуацій) встановлюється Порядком визначення розмірів оплати за обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами[91].

Тобто обсяг ресурсів і засобів (організаційних, технічних, інженерних, інформаційних тощо), 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'єкта, розміру й характеру можливих наслідків аварії щодо інших об'єктів тощо.

До того ж поширення послуг аварійно-рятувальних служб МНС подекуди не охоплює всі потенційно-небезпечні об'єкти. Наприклад, у протоколі засідання (листопад 2011 р.) Комісії з питань техногенно-

---

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

[91]*Про затвердження* Порядку визначення розмірів оплати за обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами : 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 р. № 495/369 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1222-03

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'єкти, що складає 33% та 34 окремі території (місця масового відпочинку людей), що складає 18% від загальної кількості, які підлягають обов'язковому обслуговуванню»[92].

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, як приклад можна згадати, що на території України із 60-х років XX ст. Збройними силами СРСР було створено могильники для радіоактивних відходів, і на сьогодні на цих об'єктах фізичний захист майже відсутній. Водночас країна зазнає зовнішнього тиску (критики) у зв'язку із 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 них та аналізу загроз цим об'єктам. Зокрема, фінансування діяльності з попередження, реагування та ліквідації наслідків надзвичайних ситуацій заплановано в Загальнодержавній цільовій програмі[93]. На фінансування витрат, пов'язаних із надзвичайними ситуаціями, також використовується Резервний фонд Кабінету Міністрів України[94].

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

---

[92]*Протокол* № 36 позачергового засідання комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій облдержадміністрації від 22.11.2011 р. / Управління з питань надзвичайних ситуацій Одеської обласної державної адміністрації [Електронний ресурс]. – Режим доступу: http://guns.odessa.gov.ua/Main.aspx?sect=Page&IDPage=38905&id=113

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

[94]*Про затвердження* Положення про резервний фонд Кабінету Міністрів України : постанова Верховної Ради України від 22.02.1996 р. № 62/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/62/96-%D0%B2%D1%80

Наприклад, комісія, утворена Міненерговугілля[95], визнала, що охорона структурних підрозділів ДП «Кримські генеруючі системи» не відповідає вимогам чинного законодавства щодо охорони особливо важливих об'єктів електроенергетики. Вона запропонувала вийти із 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 ситуація складається і з модернізацією мереж життєзабезпечення, критично важливих для великих міст. Аномально високі температури влітку та морози взимку спричиняють аварії на об'єктах житлово-комунального 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 зростання цін.

Низку економічних механізмів запроваджено в Україні для захисту підприємств, життєво важливих для забезпечення населення й територій, послугами з водопостачання, електроенергії, теплопостачання тощо.

Законом України «Про електроенергетику», зокрема, 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. Кабінет Міністрів України затверджує порядок складання переліку споживачів та їх обладнання, для якого має бути встановлена екологічна броня електропостачання, фінансування якої за несплати або неповної оплати 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[96], цей перелік складається

---

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

[96]*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 16.11.2002 р. № 1792 : постанова Кабінету Міністрів України від 26.12.2003 р. № 2052 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2052-2003-%D0%BF

задля запобігання виникненню надзвичайних ситуацій техногенного та 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[97], визначається механізм надання кредитів для оплати екологічної броні електропостачання в разі несплати або неповної оплати спожитої електричної енергії споживачами, що мають таку броню.

Станом на 1 травня 2005 р. 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 (у т.ч. 565 підприємств водопровідно-каналізаційного господарства)[98].

Отже, підприємства, для яких встановлена екологічна броня, розглядаються як критичні з погляду можливих наслідків відключення енергопостачання і теж можуть розглядатися як кандидати до переліку об'єктів критичної інфраструктури.

Згідно з Постановою Кабінету Міністрів України від 6.05.2000 р. № 765[99] низка підприємств вугільної, гірничодобувної, металургійної промисловості, хімічного комплексу, енергетики та оборонної промисловості визначені 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 середовищу у випадку банкрутства таких підприємств.

Проблему впровадження цілісної концепції захисту критичної інфраструктури в Україні потрібно вирішувати з огляду на процеси модернізації системи захисту національної безпеки. Так, законодавчі акти, що регламентують питання захисту населення і територій від надзвичайних ситуацій природного й техногенного характеру, були зведені

---

[97]*Про затвердження* Порядку надання кредитів для оплати екологічної броні електропостачання : постанова Кабінету Міністрів України від 03.08.2005 р. № 702 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/702-2005-%D0%BF

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

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

в Кодексі цивільного захисту України[100]. Після набуття ним чинності (01.07.2013 р.) мають втратити чинність закони, що регулюють дану сферу суспільних відносин: 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».

Ще одне питання, яке виникне за системного впровадження концепції захисту критичної інфраструктури в Україні, – залучення Збройних сил України та регулювання в умовах особливого стану і надзвичайної ситуації. Низка законів України[101] містить положення про координацію дій і концентрацію зусиль державних органів у певних умовах, які стосуються або так званого особливого періоду (охоплює час мобілізації, воєнний 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 в законах «Про транспорт»[102] (ст. 15 «Організація роботи транспорту в надзвичайних умовах») і «Про трубопровідний транспорт»[103] (ст. 18 «Організація роботи підприємств, установ та організацій трубопровідного транспорту в умовах надзвичайного стану»).

---

[100]*Кодекс* цивільного захисту України / Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/5403-17

[101]*Про оборону* України : закон України від 06.12.1991 р. № 1932-XII [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1932-12; *Про цивільну* оборону України : закон України від 03.02.1993 р. № 2974-XII [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2974-12; *Про правовий* режим надзвичайного стану : закон України від 16.03.2000 р. № 1550-III [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1550-14; *Про мобілізаційну* підготовку та мобілізацію : закон України від 21.10.1993 р. № 3543-XII [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3543-12; *Про функціонування* єдиної транспортної системи України в особливий період : закон України від 20.10.1998 р. № 194-XIV [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=194-14

[102]*Про транспорт* : закон України від 10.11.1994 р. № 232/94-ВР [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=232%2F94-%E2%F0

[103]*Про трубопровідний* транспорт : закон України від 15.05.1996 р. № 192/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=192%2F96-%E2%F0

З-поміж пріоритетних напрямів підготовки держави до збройного захисту національних інтересів у новій редакції Воєнної доктрини України (ст. 23)[104] вказується «розвиток інфраструктури регіонів з урахуванням потреб підготовки території держави до оборони».

На сьогодні дедалі гострішою стає проблема стандартизації процедур оцінки ризиків для великих інфраструктурних об'єктів в Україні. Нині в законодавстві України існує близько 30 визначень поняття «ризик» (зокрема, в таких законах України: «Про об'єкти підвищеної небезпеки», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», «Про стандарти, технічні регламенти та процедури оцінки відповідності» та інших нормативно-правових документах). Водночас для оцінки ризиків критичної інфраструктури потрібно розробити методологію, що враховуватиме особливості інфраструктурних об'єктів.

Сьогодні у провідних країнах світу відбувається стандартизація термінології та підходів у сфері захисту критичної інфраструктури (наприклад, у США ці процеси проходять доволі активно)[105].

В Україні, порівняно з провідними країнами, спостерігається недостатність стандартів з аналізу ризиків, і, головне, слабка узгодженість понятійного апарату, що використовується. Практичне вирішення проблем стандартизації, сертифікації забезпечення якості та ефективності систем комплексної безпеки в Україні і на сьогодні, і в перспективі гостро затребуване, а у зв'язку з євроінтеграційними намірами буде дедалі більш затребуваним і потребуватиме гармонізації з міжнародними стандартами, у т.ч. для забезпечення конкурентоспроможності вітчизняної продукції на світовому ринку.

Висновки та пропозиції

1. Дослідження ступеня впровадження концепції захисту критичної інфраструктури у провідних країнах світу, в наших східноєвропейських країнах-сусідах, а також у Російській Федерації свідчить, що на сьогодні концепція критичної інфраструктури є дієвим інструментом,

---

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

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

який використовується і в міжнародній, і в національних системах безпеки для захисту найбільш важливих систем, об'єктів і 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, що закладають сприятливі організаційно-управлінські підвалини для запровадження концепції захисту критичної інфраструктури в нашій країні.

Зважаючи на це, упровадження в Україні концепції захисту критичної інфраструктури стане важливим кроком до вдосконалення існуючих державних систем та інституцій у сфері безпеки.

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

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, з огляду на міркування і критерії забезпечення безпеки за окремими складниками національної безпеки (економічної, державної, політичної, енергетичної, екологічної, гуманітарної тощо), результатом чого стали різні дефініції об'єктів: підприємства, що мають стратегічне значення для економіки та безпеки держави; важливі державні об'єкти; об'єкти, які підлягають охороні та 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 у становленні (формуванні) системи захисту національної безпеки України, існує низка труднощів і проблем, пов'язаних із захистом критичної інфраструктури, що потребують розв'язання:

• невідповідність національної нормативно-правової бази положенням міжнародних документів, зокрема у частині, що регулює питання

захисту критично важливих об'єктів та інфраструктури, на тлі декларування курсу на євроінтеграцію;

• обмеженість механізмів обміну інформацією та інформаційного забезпечення про загрози об'єктам критичної інфраструктури й відсутність механізмів надвідомчого управління та інвентаризації ресурсів, задіяних для попередження загроз техногенного і природного характеру, в умовах зростання їх рівня, що вимагає ліпшого забезпечення інженерними засобами, обладнанням, технікою, інформаційними та кадровими ресурсами;

• відсутність нормативних документів, вимог, методологій для оцінки загроз об'єктам, критичним для життєдіяльності держави; загальної методології оцінки ризиків для критично важливих об'єктів та інфраструктури, не зважаючи на щільну взаємозалежність критично важливих об'єктів (насамперед інформаційних, енергетичних і транспортних мереж), що створює небезпеку виникнення каскадних аварій;

• відсутність ефективної практики державно-приватного партнерства у сфері безпеки, що вимагає вдосконалення організаційних і правових основ такого партнерства;

• міждисциплінарний характер завдань захисту критичної інфраструктури, що потребують комплексних наукових досліджень, які через свою складність вимагають значних фінансових інвестицій.

5. На сьогодні інформаційні й телекомунікаційні мережі стають одним з основних і найбільш вразливих складників критичної інфраструктури, але впровадження концепції захисту критичної інфраструктури не має обмежуватися заходами щодо захисту тільки від кіберзагроз.

Задля подолання названих труднощів і проблем, упровадження в Україні підходів до захисту критичної інфраструктури доцільно здійснити такі кроки:

• *Раді національної безпеки і оборони України* розглянути можливість ініціювання процесів удосконалення державної системи захисту критично важливих об'єктів та інфраструктури в Україні у спосіб:

– створення Робочої групи та організації розроблення Стратегії захисту національної критичної інфраструктури;

– сприяння вдосконаленню чинного законодавства у сфері безпеки та його гармонізації з урахуванням кращого зарубіжного досвіду;

– розроблення і затвердження загальної методології оцінки ризиків для об'єктів критичної інфраструктури;

• *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;

• *Мінінфраструктури, Міненерговугілля, Міноборони, МНС, МВС* удосконалити 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;

• *Мінприроди* вдосконалити систему управління у сфері поводження з відходами, активізувати роботу з упровадження систем інформаційно-аналітичного супроводу державного контролю в зазначеній сфері;

• *Мінрегіону* вдосконалити систему оперативного контролю за станом мереж водо- і теплопостачання, вдосконалити методологію аналізу аварійності та оцінки ризиків аварій на цих мережах, з урахуванням впливу на цінову доступність послуг і платоспроможність населення;

• *ДКАУ* підготувати пропозиції щодо вдосконалення системи космічного моніторингу за критично важливими об'єктами та інфраструктурою України;

• *Адміністрації Держспецзв'язку* розглянути організаційні й технологічні можливості створення мережі обміну інформацією про загрози критично важливим об'єктам та інфраструктурі в межах Національної системи конфіденційного зв'язку;

• *Мінекономрозвитку* передбачити у Плані національної стандартизації розроблення нормативних документів зі стандартизації процесів управління ризиками;

• *НАНУ, МОНмолодьспорту* передбачити:

– виділення коштів для виконання підпорядкованими науково-дослідними установами й 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;

• *НІСД* організувати і провести у 2013 р. науково-практичну конференцію з проблем упровадження концепції захисту критичної інфраструктури в Україні; забезпечити аналітичний і 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 із ними терористичних загроз і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури.

Додаток

МАТЕРІАЛИ ЗАСІДАННЯ «КРУГЛОГО СТОЛУ»

17 липня 2012 року в конференц-залі Національного інституту стратегічних досліджень відбулося засідання «круглого столу» **«Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні».** В обговоренні взяли участь представники органів державної влади, промислових компаній, неурядових організацій, науковці, експерти, представники засобів масової інформації.

В обговоренні взяли участь:

БАКАЛИНСЬКИЙ **Олександр Олегович**	заступник завідувача кафедри Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
БЄГУН **Василь Васильович**	доцент кафедри атомних електричних станцій та інженерної теплофізики теплоенергетичного факультету НТУУ «КПІ»
БІРЮКОВ **Дмитро Сергійович**	старший консультант відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
БОГДАНОВ **Олександр Михайлович**	завідувач кафедри № 2 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
БОЧАРНИКОВ **Віктор Павлович**	провідний науковий співробітник відділу проблем оцінки та прогнозів загроз у воєнній сфері науково-дослідного управління Національного університету оборони України
БРЕЖНЄВ **Євген Віталійович**	старший науковий співробітник науково-технічного центру дослідження й аналізу безпеки інфраструктур
ВАРУС **Василь Іванович**	начальник Науково-дослідного інституту проблем військової медицини Збройних Сил України

ВЕРІЧ **Андрій Андрійович**	начальник відділу Департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
ВОЙТКО **Сергій Васильович**	заступник завідувача кафедри міжнародної економіки факультету менеджменту й маркетингу НТУУ «КПІ»
ГАНГАНОВ **Володимир Миколайович**	директор Департаменту науково-освітнього забезпечення АПВ та розвитку сільських територій
ГОЛОВІНОВ **Олег Валерійович**	начальник управління з охорони важливих державних об'єктів штабу ГУВВ МВС України
ГРИЦУНІК **Олег Дмитрович**	заступник начальника Департаменту Державної служби охорони при МВС
ГУДЗЬ **Юлія Вікторівна**	керівник представництва ДП «Миколаївський морський торговельний порт» у м. Києві
ДМИТРИК **Вадим Володимирович**	заступник начальника відділу Департаменту охорони праці промислової безпеки та надійності транспортування газу і нафти НАК «Нафтогаз України»
ЄСИПЕНКО **Юрій Миколайович**	заступник начальника Управління координації інспекційної діяльності Державної інспекції ядерного регулювання України
ЗАСЛАВСЬКИЙ **Володимир Анатолійович**	професор кафедри математичної інформатики факультету кібернетики Київського національного університету імені Тараса Шевченка
ЗЕЛЬ **Володимир Іванович**	головний інженер КП «Київський метрополітен»
ІНШАКОВ **Сергій Валерійович**	директор Федерації страхових посередників України
КАЗІМІРОВА **Алла Володимирівна**	голова Міжнародної екологічної громадської організації «АКВА ДІМ»

КАЧИНСЬКИЙ **Анатолій Броніславович**	радник директора Національного інституту стратегічних досліджень
КОНДРАТОВ **Сергій Іванович**	старший науковий співробітник відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
КОНДРЮК **Сергій Михайлович**	заступник голови Федерації профспілок України
КОРЖ **Ігор Федорович**	головний консультант Комітету Верховної Ради України з питань національної безпеки та оборони
КОРОБКА **Віктор Петрович**	начальник військ РХБ захисту Збройних Сил України – начальник Центрального управління військ РХБ захисту Головного управління оперативного забезпечення Збройних Сил України
КОТЕНОК **Григорій Михайлович**	директор Департаменту координації загальнодержавних проектів з інформатизації Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації
КРАВЧЕНКО **Ростислав Іванович**	провідний науковий співробітник Українського науково-дослідного інституту цивільного захисту
КУЧЕРУК **Сергій Адамович**	завідувач секретаріату Комітету Верховної Ради України з питань транспорту і зв'язку
ЛИТВИНЕНКО **Олександр Валерійович**	заступник директора Національного інституту стратегічних досліджень
МАХАЄВА **Олена Олександрівна**	начальник Управління нагляду (оверсайта) за платіжними системами та системами розрахунків
МЕЛАЩЕНКО **Андрій Олегович**	науковий співробітник Інституту кібернетики імені В. М. Глушкова НАН України

МЕЛЬНИК **Юрій Миколайович**	головний спеціаліст управління нагляду на виробництвах і об'єктах підвищеної небезпеки Державної служби гірничого нагляду та промислової безпеки України
МЕЛЬНІКОВ **Григорій Іванович**	заступник директора ДП «Центр громадської безпеки 112»
МОХОР **Володимир Володимирович**	завідувач кафедри № 5 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
НОВІКОВ **Олексій Миколайович**	завідувач кафедри інформаційної безпеки фізико-технічного факультету НТУУ «КПІ»
ОМЕЛЬЧЕНКО **Анатолій Петрович**	заступник директора Департаменту інформаційних технологій Національного банку України
ПЕТРОВ **Валентин Володимирович**	заступник начальника Департаменту інформаційної безпеки Служби безпеки України
ПОСМІТНИЙ **Олександр Сергійович**	заступник директора Департаменту екологічної безпеки Міністерства екології та природних ресурсів України
РАБЧУН **Андрій Олександрович**	науковий співробітник Науково-дослідного інституту проблем військової медицини Збройних Сил України
РОСЬ **Анатолій Олександрович**	професор кафедри застосування інформаційних технологій та інформаційної безпеки Інституту інформаційних технологій Національного університету оборони України
САМСОНЕНКО **Вадим Феодосійович**	генеральний директор Концерну радіомовлення, радіозв'язку та телебачення
СЕМЕНОВ **Юрій Георгійович**	заступник ректора з фізичного захисту, обліку та контролю ядерного матеріалу Севастопольського національного університету ядерної енергії та промисловості

СИРОВЕЦЬ **Сергій Васильович**	заступник директора Департаменту спеціальних ІТС Адміністрації Держспецзв'язку
СКАЛЕЦЬКИЙ **Юрій Миколайович**	завідувач відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
СОНКІНА **Галина Леонідівна**	головний спеціаліст відділу аналітичного забезпечення управління надзвичайних ситуацій та антитерористичної діяльності Департаменту цивільного захисту МНС України
СТОЛЯРЕВИЧ **Юрій Анатолійович**	головний спеціаліст Державної служби 2-го управління ВЧ А0515
СТРУКОВА **Віта Дмитрівна**	заступник генерального директора ПАТ «АК «Київводоканал»
СУСЛОВ **Сергій Миколайович**	головний фахівець відділу нагляду з питань техногенної безпеки та контролю за органами виконавчої влади Управління техногенної безпеки Державної інспекції техногенної безпеки України
ТРЕТЬЯКОВА **Галина Миколаївна**	генеральний директор Української федерації убезпечення
ФАСЕНКО **Сергій Володимирович**	провідний інженер Управління воєнізованої охорони Укрзалізниці
ФЕДОТОВ **Ігор Олександрович**	начальник групи цивільного захисту Центрального управління військ РХБ захисту Головного управління оперативного забезпечення Збройних Сил України
ХАРЧЕНКО **В'ячеслав Сергійович**	завідувач кафедри комп'ютерних систем і мереж факультету радіотехнічних систем літальних апаратів Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

ЧЕНЧИК **Андрій Миколайович**	головний фахівець відділу екологічної, пожежної та загальної безпеки Департаменту безпеки Міністерства інфраструктури України
ШОФАРЕНКО **Леонід Васильович**	начальник відділу кооперації та інвестицій Державного космічного агентства України
ЯКОВЛЄВ **Євген Олександрович**	провідний науковий співробітник Національного інституту стратегічних досліджень

ЛИТВИНЕНКО О. В.,
заступник директора
Національного інституту стратегічних досліджень

Шановні колеги!

Нещодавні трагічні події в Росії (затоплення Кримська) вкотре засвідчили важливість підтримання в необхідному стані критичної інфраструктури, зокрема гідротехнічних споруд. Коли ми нехтуємо безпекою таких об'єктів критичної інфраструктури, відповідь природи (стихії) не забариться. На жаль, за таку безпечність ми сплачуємо не просто матеріально, а людськими життями.

Не менш важливим є й те, що на сьогодні в Україні активізувалося питання тероризму. Більш важливо не те, з якою метою і хто влаштував вибухи в м. Дніпропетровську (українські правоохоронні органи та СБУ розслідували цю ситуацію), а те, що в нашому суспільстві з'являються групи, які заради грошей, досягнення власних інтересів готові покласти на карту життя людей, вживаючи украй небезпечні заходи й використовуючи такі само інструменти. За цих умов проблема захисту критичної інфраструктури набуває надзвичайної ваги. Відомо, скільки в Україні таких життєво важливих об'єктів (у т.ч. 15 ядерних енергоблоків, дніпровський гідротехнічний комплекс, розвинена хімічна промисловість), руйнування яких може призвести до великої кількості жертв. Руйнування не самих заводів, а місць, де зберігаються відходи вищих категорій (наприклад, Калуський випадок), може не тільки завдати збитків, шкоди Україні, а і призвести до інцидентів міжнародного масштабу. Ми знаємо, що в разі аварії в Калуші це була б катастрофа для трьох країн. І таких об'єктів на території нашої держави досить багато.

Усі усвідомлюють, що обсяг фінансування, ресурсів, доступний Українській державі, як і будь-якій іншій країні, є обмеженим. Відповідно необхідно виокремити основні об'єкти, мережі, на захист яких має спрямовуватися левова частка коштів і зусиль. Не йдеться про те, що інші об'єкти мають працювати за залишковим принципом, але цілком зрозуміло, що виокремлення основних об'єктів, найбільш серйозних, небезпечних, критичних структур є цілком логічним і принциповим напрямом. Робота нашого Інституту в тісному контакті з МНС, СБУ й іншими структурами ведеться вже не перший рік. І ми досягли достатньо серйозних успіхів: напрацювання, наукові роботи, документи, навіть починаємо працювати над матеріалами нормативно-правового характеру.

Тут у нагоді стає світовий досвід, насамперед Сполучених Штатів Америки, Європейського Союзу та Російської Федерації як провідних партнерів, провідних держав у цій сфері. Ми знаємо, що захист критичної інфраструктури визначено Стратегією національної безпеки США як основний напрям діяльності американської держави, одним з основних завдань міністерства внутрішньої безпеки є діяльність, спрямована на забезпечення захисту й безпеки цієї інфраструктури не лише в інформаційній сфері (дуже актуальній на сьогодні), а й у всіх інших секторах критичної інфраструктури.

Усім відомо, скільки уваги приділяється критичній інфраструктурі у країнах Євросоюзу, які рішення прийнято на рівні Європейської Комісії, які фонди й зусилля спрямовано на вирішення цих питань. Особливу увагу слід звернути на досвід Великої Британії, де створено Центр оцінки ризиків і відповідну структуру у складі міністерства внутрішніх справ. Досить цікавим є досвід нашого сусіда – Польщі. Російський досвід, не зважаючи на події в Кримську, свідчить, що критичній інфраструктурі (насамперед у паливно-енергетичному комплексі) також приділяють значну увагу. На жаль, у нашому законодавстві це питання не може розглядатися як достатньо розроблене.

Проблема захисту критичної інфраструктури має більший вимір – вимір культури безпеки, культури сприйняття ризиків, культури управління останніми. Це перехід від старої радянської культури безпеки до сучасної, орієнтованої на захист людини, суспільства й держави.

Ми повинні чітко усвідомлювати наявність певного парадоксу, присутнього в сучасних ліберальних концепціях, так званої людської безпеки *(human security)*, який полягає в тому, що наявні підходи близькі до безпеки в тоталітарних країнах, де безпекою оголошувалося все – і безпека як така зникала.

Зазначу: безпека – це те, що стосується проблем виживання, життя людей, суспільних груп і держави в цілому. Упевнений, що знаходження балансу, чіткого усвідомлення в даній проблематиці можливо лише завдяки відкритій дискусії фахівців різних напрямів, спеціалістів, шкіл. Наш «круглий стіл» надає унікальну можливість для таких дискусій. Тому закликаю всіх до відвертого, щирого діалогу.

За результатами засідання буде підготовлено й опубліковано аналітичні документи (у т.ч. і для керівництва держави). Усі думки, пропозиції, озвучені сьогодні, буде враховано, опрацьовано при вироблені державної політики в обговорюваній сфері.

СКАЛЕЦЬКИЙ Ю. М.,
завідувач відділу екологічної та техногенної безпеки
Національного інституту стратегічних досліджень

У цьому залі 22 травня відбувся «круглий стіл» щодо проблем цивільного демократичного контролю над Збройними силами в умовах надзвичайних ситуацій. Розглядалися передусім надзвичайні ситуації природного й техногенного характеру. На заході були присутні представники всіх європейських країн, які представляли державні структури з питань реагування на надзвичайні ситуації, представники Збройних сил, військові аташе. У результаті обговорення з'ясувалося, що концепція критичної інфраструктури стала робочим дієвим інструментом забезпечення національної безпеки цих держав. Отже, над проблемами стосовно критичної інфраструктури наш Інститут працює давно.

БІРЮКОВ Д. С.,
старший консультант
відділу екологічної та техногенної безпеки
Національного інституту стратегічних досліджень

Доповідь стосується актуальних проблем та етапів розвитку концепції захисту критичної інфраструктури у провідних країнах світу, а також зв'язку термінології, прийнятої в нормативно-законодавчій базі України, із зарубіжними аналогами. Варто зазначити, що термін «критична інфраструктура» не введено в українське законодавство, незважаючи на євроінтеграційні устремління нашої держави.

У низці країн ЄС (у т.ч. Великій Британії, а також у США, Канаді, Австралії під цим терміном розуміють системи, мережі та об'єкти, вихід із ладу яких може призвести до згубних наслідків для економіки, соціального благополуччя, здоров'я.

Концепція захисту критичної інфраструктури поступово розвивалася з II половини 90-х років: унаслідок поширення інформаційних технологій, підсилення їх значимості для безпеки всіх крупних інфраструктурних і промислових об'єктів, функціонування служб та органів влади у Сполучених Штатах Америки було введено термін «критична інфраструктура» та директивою президента окреслено заходи щодо її захисту. Після терористичних актів 11 вересня, акценти змінилися: терористичні загрози були усвідомлені як найбільш актуальні. Саме це усвідомлення стало причиною найбільших перетворень в органах виконавчої влади США за останні 60 років: було створено міністерство внутрішньої безпеки. Такі зміни знайшли своє

відображення і в прийнятті законодавчих актів у сфері захисту критичної інфраструктури Сполучених Штатів Америки.

На основі проведеного аналізу стратегічних документів у сфері захисту критичної інфраструктури, розроблених у провідних країнах світу, можна виокремити такі *основні складники діяльності* у цій сфері:

- координація діяльності органів влади, силових відомств і служб;
- державно-приватне партнерство;
- організація системи інформування про загрози та експертного обговорення;
- упровадження підходу до врахування загроз усіх трьох типів (техногенних, природного та соціально-політичного характеру).

В українському законодавстві введено низку визначень, за якими ідентифікуються об'єкти, які відповідно до світового досвіду належать до критичної інфраструктури:

- підприємства, що мають стратегічне значення для економіки та безпеки держави;
- об'єкти підвищеної небезпеки; об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період;
- особливо важливі об'єкти електроенергетики; особливо важливі об'єкти нафтогазової галузі;
- система електронних платежів НБУ;
- пам'ятки культурної спадщини;
- системи життєзабезпечення.

Проте зазначені об'єкти ідентифікувалися згідно з внутрішньовідомчими методиками та на основі критеріїв, пов'язаних з окремими аспектами функціонування цих об'єктів у державі.

Насамкінець зауважу, що навіть у провідних країнах світу розвиток системи захисту критичної інфраструктури здійснювався із запізненням – як відповідь на загрози, що вже відбулися.

ТРЕТЬЯКОВА Г. М.,
генеральний директор
Української федерації убезпечення

Безперечно, аби захищати якісь об'єкти, треба спочатку визначитися, чи досить ресурсів на здійснення належного захисту, чи потрібно захищати все, чи ми мусимо захищати окремі об'єкти й системи, критичні для нашої держави.

Я довго працюю у страховій сфері, і в мене виробилася певна «соціальна параноя». Навіть удома в розмові з дітьми я завжди говорю,

що в автомобілі треба пристебнутися, не можна сидіти справа від водія (це найбільш небезпечне місце), коли виходиш із дому, треба вимкнути все, що може спричинити небезпеку. Я вважала, що людей, які опікуються питаннями безпеки, дуже мало. Сьогоднішній захід зібрав спеціалістів, які розуміються на тому, що таке ризики, ідентифікують, оцінюють, вивчають, як управляти певними ризиками та передають свій досвід іншим.

У сучасному світі люди, які ідентифікують ризики, оцінюють, а потім вчаться ними управляти, виживають. Ті, хто цього не робить (а отже, і нації, які цього не роблять), приречені на загибель. Дмитро Сергійович зазначив, що Україна не належить до країн, які на законодавчому рівні визначили критичну інфраструктуру, оцінюють і управляють ризиками для її елементів.

Відомо, що частиною управління ризиками є людина. У нашій країні відсутня методика оцінки вартості життя, а це призводить до недооцінювання власного життя. Науковці з європейських країн давно довели, що людина в капіталізмі насамперед є людиною, яка прагне отримати найбільший прибуток. Починаючи з 60-х років XX ст., коли в західних країнах запровадили методику оцінки вартості життя, останнє оцінили сумою, еквівалентною понад 1 млн євро, зараз же у Сполучених Штатах Америки ця сума становить 3 млн дол. США – людина усвідомлено перетворилася на людину, яка має високу цінність.

Можна сперечатися з приводу того, що є першочерговим: гроші, наявні в домогосподарстві, чи психологічне ставлення до себе як до годувальника, втрата якого еквівалентна значній сумі грошей, але в будь-якому разі методика оцінки вартості і власне оцінка вартості життя призвела до змін у суспільних відносинах. Є методики, за якими вартість життя обраховується за сумарною вартістю виховання (скільки коштує вигодувати, навчити дитину). Якщо провести розрахунки в Україні, то отримаємо суми не менші за 200–300 тис. дол. США. У цьому випадку ми житимемо довше, адже наше життя матиме економічну оцінку.

Є методика, за якою людину оцінюють як виробника частки валового національного продукту. У разі втрати, наприклад, чоловіка 40 років – саме людей переважно цієї вікової категорії ми втрачаємо в дорожньо-транспортних пригодах (5–7 тис. осіб на рік) – втрати бюджету становитимуть аналогічну суму. Отже, втрата частини валового національного продукту теж може бути адекватною оцінкою вартості життя.

Якщо ми отримуємо 200–300 тис. дол. США, то оцінюємо еквівалент вартості впровадження безпечних методів праці. Держави ви-

користовують оцінку вартості життя насамперед для стимулювання підприємств, власників та акціонерів до впровадження безпечних умов праці, а також для того, аби в судах належним чином визначалися втрати того чи іншого домогосподарства.

Деякі гуманітарії вважають, що це не дуже добре – ставитися і розглядати людину як засіб виробництва. Однак ми маємо розуміти: без такої оцінки вартості життя ми будемо надто дрібними кроками просуватися до цивілізації.

Безперечно, оцінка й визначення інфраструктури, найбільш критичної для України, є справою держави, яка має захищати від певних ризиків, що загрожують життю та здоров'ю особи, громадянина, а також функціонуванню юридичних осіб. Водночас держава має стратегічно визначити, чого вона не робитиме через обмеженість ресурсів.

Погоджуюся з колегами в тому, що, розглядаючи складники критичної інфраструктури, можливо, необхідно концентрувати зусилля передусім на транспорті й енергетиці (зокрема атомній, наслідки аварії на об'єкті якої наша країна та нещодавно Японія вже пережили). Можна також погодитися з попередніми доповідачами і в тому, що неможливо вгадати, де трапиться наступна пожежа, аварія, проте ми в змозі створити таку «пожежну команду», інституцію, яка опікуватиметься в режимі он-лайн ризиками, які можуть загрожувати критичній інфраструктурі, та змінювати їх залежно від того, які зовнішні чинники на неї впливають. Ця «пожежна команда» має реагувати так, аби забезпечити нації виживання.

Яке ж місце у цих процесах посідає страхування? Коли ми говоримо про аналіз ризиків, спочатку треба ідентифікувати ризики критичної інфраструктури, створити їх карту, дати оцінки, збагнути розміри можливої шкоди від різних загроз, а далі – навчитися управляти ризиками. На етапі управління ризиками потрібні страховики, які управлятимуть ризиками у три способи.

Передусім ці ризики може брати на себе держава, відповідно, треба планувати в державному чи місцевому бюджетах витрати, які можуть знадобитися для відновлення тих чи інших частин критичної інфраструктури, втрачених унаслідок стихійного лиха або техногенної аварії, інших ризиків, характерних нашому життю. Отже, ми можемо обирати: утримувати ці ризики на державному чи місцевому рівнях (наприклад, у разі повені в Західній Україні збитки, нанесені домогосподарствам, майже 100% утримаються з місцевого й державного бюджетів), або ж запровадити обов'язкове страхування.

Відомо, що на транспорті є обов'язкове страхування цивільної відповідальності власників транспортних засобів. Не зупинятимуся сьо-

годні на існуючих деформаціях у цьому виді страхування (наприклад, у європейських країнах цей вид страхування насамперед захищає людей і домогосподарства, які втратили годувальника). У будь-якому разі Україна впровадила цей вид страхування, хоча й дещо деформований. Отже, наша держава вирішила захищати ризики на транспорті у спосіб введення обов'язкового страхування.

Тепер щодо звичайних продуктів страхування. У ядерній енергетиці, наприклад, на сьогодні створений ядерний пул, що використовується в тому разі, коли не вистачає фінансових ресурсів окремої страхової компанії. У таких ядерних пулах іноземних держав також залучаються механізми перестрахування, завдяки чому також можна управляти ризиком з погляду відновлення інфраструктури, яка може бути втрачена під час якихось надзвичайних ситуацій.

Окремо зазначу, що в разі визначення певних пріоритетів (скажімо, енергетика і транспорт – це частини критичної інфраструктури, які вимагають першочергового захисту), то близьким до цих галузей (з погляду наслідків) буде питання соціального захисту населення та окремої людини, яка стоїть у центрі захисту.

Які загрози можуть виникнути, якщо людина не буде соціально захищеною? Насамперед це революції, демонстрації та інші прояви, що, як ми бачимо, виникають навіть у європейських країнах, де система соціального захисту є досить стабільною, вибудуваною консервативно. Що розуміється під соціальним захистом людини, про що необхідно подумати? Передусім про ризик, що є у домогосподарства – втрату годувальника, у результаті якого сім'ї випадають із того класу доходів, у якому вони були, коли годувальник утримував родину. Має бути вибудувана така система захисту родини, аби остання не відчувала значної матеріальної втрати.

Ще один ризик – це інвалідність, яка може бути результатом або захворювання (професійного), або нещасного випадку (в побуті чи на виробництві). Система захисту родини і безпосередньо самої людини від інвалідності має теж працювати в Україні, з-поміж її складників має бути не лише компенсація медичних витрат, а й витрат, наприклад, з переобладнання будинку людини, яка стала інвалідом. Частиною соціального захисту може бути захист від безробіття та накопичення грошей на відпустку й навчання дітей.

Страхування має допомагати у всіх указаних процесах. Його роль полягає у відновленні юридичних осіб або відновленні доходу домогосподарств для продовження життя на належному рівні.

Великі страхові компанії вивчають і оцінюють різноманітні джерела ризиків. Наприклад, така відома страхова компанія, як *Alianz* ана-

лізує космічні ризики, здійснюючи страхування космічних об'єктів. Група спеціалістів (українська «пожежна команда» з оцінки ризиків критичної інфраструктури) повинна передбачити навіть малоймовірні ризики.

На жаль, не можна сказати, що на сьогодні страхування в Україні є досить розвиненим. Якщо проаналізувати, скільки збирають страхові компанії за рік, то побачимо, що сума прямого страхування становить менше 1,5 млрд грн (для порівняння: у Польщі одна страхова компанія із 20 – *PZU Poland* – збирає понад 3 млрд євро на рік).

Це досить суттєвий чинник, який свідчить про те, що наша держава на сьогодні не стимулює використання страхових інструментів для захисту юридичних і фізичних осіб. Якщо подивитися на сектори критичної інфраструктури (а з-поміж них є й фінансовий), можна стверджувати, що страхова сфера є частиною критичної інфраструктури, необхідною для відновлення інших інфраструктур у разі надзвичайних ситуацій. Тому потрібна увага держави для розбудови сфери страхових послуг.

На мою думку, рішенням сьогоднішнього «круглого столу» мають стати рекомендації, адресовані найвищому керівництву держави, Адміністрації Президента України щодо створення інституції, суспільної організації, яка б мала опікуватися ризиками, наявними в Україні. Можливо, це буде структура з невеликим штатом співробітників, однак у ній мають бути зібрані найліпші фахівці. Якщо в Україні функціонуватиме така «пожежна команда», спроможна реагувати на різноманітні виклики й небезпеки, створювати плани протидії, то частиною такої структури може бути служба спасіння, про яку сьогодні вже згадувалося. Якщо це вдасться зробити, ми виживемо як держава, збережемо свою цілісність.

СКАЛЕЦЬКИЙ Ю. М. :

Зазначу, що навіть загрози із космосу не такі вже й гіпотетичні. Наприклад, професор Качинський у своїй монографії порушував питання космічного сміття. Близько 50 супутників на орбіті, джерелами енергоживлення яких є бортові атомні електростанції, що працюють на урані майже збройового збагачення.

Так, у 1978 р. (зараз мене може хтось виправити) радянський супутник упав на територію Канади. Рівні радіаційного забруднення були значні за площею, а в окремих місцях – навіть небезпечні не лише для здоров'я, а і для життя людини. На жаль, у нашій державній системі попередження та реагування на надзвичайні ситуації така підсистема відсутня.

БЄГУН В. В.,
доцент кафедри атомних електричних станцій
та інженерної теплофізики
теплоенергетичного факультету НТУУ «КПІ»

Представлю доповідь з теми «Використання ризик-орієнтованого підходу при попередженні загроз критичній інфраструктурі». На нашій кафедрі вже не один рік викладаються навчальні дисципліни для студентів і бакалаврів з аналізу ризиків, а також пов'язані з цією тематикою спецкурси для магістрів. Наші випускники вміють розраховувати різноманітні ризики, використовують європейські програми, розроблені у Швеції, та програми, якими користуються у США. За допомогою цих програмних засобів можна прорахувати ризики не тільки для АЕС, а і будь-який ризик, що зустрічається в нашому житті, наприклад ризик розлучення молодого подружжя.

Спочатку зверну увагу на термінологію. Справді, в багатьох розвинених країнах використовується термін «критична інфраструктура». Однак зауважу, що в українській мові поняття «інфраструктура» стосується множини, певної кількості об'єктів. Водночас досить часто критично важливими для безпеки життєдіяльності держави є одиничні об'єкти. Тому, на мій погляд, більш доречно вживати термін «критично важливі об'єкти», введений у законодавстві РФ.

Хочу зазначити, що в Україні на державному рівні питання визначення критично важливих об'єктів та інфраструктури порушується вперше. На жаль, реальна ситуація у нашій країні (і сьогодні про це вже багато говорили) така, що ми звикли до понять знеструмлення, зупинка підприємств, аварії на об'єктах водо- й теплопостачання. Звичними в українському житті стали і такі словосполучення (вони вже увійшли до класики надзвичайних ситуацій), як відключення єдиної лінії, розмерзання мережі теплопостачання, відключення водопроводів, паводки на Закарпатті, перевезення небезпечних вантажів. У засобах масової інформації всього світу демонструють «фосфорну» аварію[106], постійно згадують про наслідки Чорнобильської катастрофи.

Наведу кілька подій, які відбулися нещодавно: вчора через сильний порив вітру знеструмлено 409 населених пунктів у десяти об-

[106]16 липня 2007 р. в Буському районі Львівської області на перегоні Красне – Ожидів зійшли з колії та перекинулися 15 цистерн із жовтим фосфором товарного потяга № 2005, унаслідок чого з однієї цистерни витік фосфор і сталося самозаймання шести цистерн. Під час гасіння пожежі утворилася хмара з продуктів горіння (зона ураження близько 90 км^2), здійснювалася евакуація населення із зони ураження.

ластях; під Харковом 11 липня вибухнула газокомпресорна станція. А також дещо раніше: води залили поля й городи у Свалявському та Ужгородському районах, у м. Мукачево стічні води підійшли до дитячої лікарні. Таке трапляється в кожній країні, однак у нас – частіше.

Чому так відбувається? Напевно, це наслідки ситуації, яку ми маємо. У національному законодавстві просто не існує нормативних актів щодо критично важливих об'єктів. В організаційно-технічних планах МНС, які затверджуються щорічно, відсутні словосполучення і «критично важливі об'єкти», і «критична інфраструктура». Не знайти їх і у планах науково-дослідних робіт, розміщених на сайті МНС. І зрештою, в галузевих стандартах вищої освіти Університету цивільного захисту України, розташованого в м. Харкові, ці терміни також не зустрічаються.

Звертаю увагу на зовсім новий документ – проект оновленої Енергетичної стратегії на період до 2030 року[107]. У ньому є тільки констатація факту: «...на сьогодні більша частина генеруючих активів та електромереж зношена й неефективна», «...станом на кінець 2010 р. 84% блоків теплових електростанцій перевищили межу фізичного зношення у 200 тис. год наробітку й потребують модернізації або заміни».

Крім того, «35% повітряних ліній електропередач напругою 220–330 кВ експлуатуються понад 40 років, 55% основного устаткування трансформаторних підстанцій випрацювали свій розрахунковий технічний ресурс». Якщо в залі присутній Євген Олександрович Яковлєв, він може підтвердити, що мережі водопостачання та каналізації мають ще гірший стан.

Порівняймо з нашими східними сусідами – Російською Федерацією. У 2004 р. була створена Міжвідомча координаційна група з вирішення питань забезпечення захисту населення країни та критично важливих для національної безпеки об'єктів інфраструктури. Тоді само був створений і затверджений перелік критично важливих об'єктів Російської Федерації; роком пізніше – Концепція Федеральної системи моніторингу критично важливих об'єктів та небезпечних вантажів, затверджена урядом. І, зрештою, у 2005 р. затверджені Методичні рекомендації з розроблення планів критично важливих об'єктів. До речі, останні оновлювалися у 2011 р.

---

[107] *Проект* оновленої Енергетичної стратегії України на період до 2030 року / Міністерство енергетики та вугільної промисловості України. – 2012. – 7 червня [Електронний ресурс]. – Режим доступу: *mpe.kmu.gov.ua/fuel/doccatalog/document?id=222032*

Доречно звернути увагу на деякі витяги з постанови уряду РФ щодо впровадження програми захисту критично важливих об'єктів. Перше й головне – мета програми. Вона полягає в забезпеченні мінімального рівня ризиків, впливу на об'єкти, загрози тощо. До функцій моніторингу критично важливих об'єктів належать підготовка інтегральних оцінок та моделей кризових ситуацій, що виникають на критично важливих об'єктах і при транспортуванні небезпечних вантажів, а також оцінка їхніх можливих наслідків. Це одна з головних функцій, необхідних для обрахунку ризиків і подальшого забезпечення запобігання надзвичайних ситуацій.

Треба зауважити, що в Російській Федерації переписали всі європейські стандарти, розроблені Міжнародною організацією зі стандартизації або Міжнародною електротехнічною комісією, також уже діє програма ризик-менеджменту.

Досвід країн НАТО, як уже зазначалося, свідчить, що запроваджуються національні стандарти захисту критично важливих об'єктів. Понад те, Альянс регулярно проводить навчання із захисту таких об'єктів. З-поміж останніх повідомлень привертає увагу таке: Стівен Грегорі, директор компанії, що спеціалізується на захисті критичної інфраструктури й виконує замовлення НАТО (тобто існують цілі підрозділи захисту критичної інфраструктури), пропонує «здійснювати обмін знаннями для вдосконалення методології забезпечення безпеки, заснованої на оцінці ризиків»[108]. Тобто інших методів у світовій практиці, крім оцінки ризиків, не існує.

Які потрібно зробити висновки для України, що має бути розроблено? Має бути створена національна законодавча нормативно-правова база щодо критично важливих об'єктів, упроваджений державний нагляд за безпекою на основі ризик-орієнтованого підходу, розроблені методики оцінки ризиків і державного моніторингу критично важливих об'єктів, а також відповідні плани реагування. Це все, що потрібно, і це є в кожній розвиненій країні.

Якщо йдеться про ризик-орієнтований підхід, хочу сказати про стан і можливості його запровадження в Україні. У нас є законодавча база, насамперед це закони України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру»[109],

---

[108] *Protecting* critical infrastructure: a challenge for NATO and its partners / NATO. – 2012. – 31 May [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/en/SID-E0681B65-F8B7259C/natolive/news_88054.htm

[109] *Про захист* населення і територій від надзвичайних ситуацій техногенного та природного характеру : закон України від 08.06.2000 р. № 1809-III [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1809-14

«Про об'єкти підвищеної небезпеки»[110], «Про основні засади державного нагляду (контролю) у сфері господарської діяльності»[111]. Названі закони цілком відповідають європейським принципам і мають забезпечувати функціонування системи попередження та реагування на надзвичайні ситуації на основі розрахунку ризиків. Понад те, у першому з них чітко визначено поняття «запобігання». Чому ж ці закони не працюють? Напевно, через те, що методичний науковий складник ризик-орієнтованого підходу не впроваджений у діяльність відповідного відомства.

Які можливості ми втрачаємо? Галина Миколаївна, на мою думку, сказала досить правильно про можливості оцінки ризиків. Що можна зробити на основі ризик-орієнтованого підходу? По-перше, визначити ймовірність небажаної події. Далі, якщо відома ймовірність, можна відпрацювати реагування, визначити можливі наслідки, і, що найголовніше, під час створення моделі (а ризик-орієнтований підхід передбачає створення моделі об'єкта) на основі розрахунку останньої можна розробити науково обґрунтовані заходи із запобігання. Ще у 2004 р. ми підготували пропозиції щодо захисту критично важливих об'єктів в Україні (від Інституту державного управління у сфері цивільного захисту її підписував генерал Болотських М. В.), і направили її до МНС. На жаль, вони залишилися без уваги.

Зрештою, про серйозність проблеми у сфері безпеки інфраструктурних об'єктів свідчить і той факт, що Прем'єр-міністр України М. Я. Азаров особисто відвідає станцію водопостачання та огляне її.

Шановні колеги, якщо вам потрібно підрахувати ризики, звертайтеся до нас по допомогу.

ЗАСЛАВСЬКИЙ В. А.,
професор кафедри математичної інформатики факультету кібернетики Київського національного університету імені Тараса Шевченка

Тема виступу – «Оцінка ризиків: проблеми моделювання для критичної інфраструктури». На початку зазначу, що мені довелося брати участь у низці науково-дослідних робіт ще в колишньому Радянському Союзі, а також під час перебування в Інституті прикладного

[110] *Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2245-14

[111] *Про основні* засади державного нагляду (контролю) у сфері господарської діяльності : закон України від 05.04.2007 р. № 877-V [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/877-16

системного аналізу (в Австрії), де досліджувалися та вирішувалися проблеми забезпечення надійності складних систем.

Передусім хочу звернути увагу на те, що забезпечення безпеки усвідомлюється як одна з необхідних передумов сталого розвитку. Якість нашого життя, розвиток економіки й соціальної сфери нерозривно пов'язані із надійністю та безпекою функціонування систем життєзабезпечення. Тому ми повинні досліджувати й упроваджувати певні механізми забезпечення безпеки життєдіяльності.

Якщо розглядати багаторівневу структуру управління безпекою в державі, то потрібно зауважити: чим вищий рівень, на якому виникає відмова функціонування, тим значніші наслідки, причому вартість пошкоджень і витрат на відновлення зростає експоненціально. Це свідчить про те, що проблеми (джерела ризику) потрібно вчасно ідентифікувати. Крім того, необхідно володіти механізмом (організаційним, законодавчо-правовим), технічними засобами, які дозволять усувати, попереджати певні проблеми.

Тому стосовно визначення ризику зазначу, що визначення джерела ризику є фундаментальним питанням, і це важливо усвідомлювати. Отже, для тих чи інших об'єктів, систем, мереж необхідно з'ясовувати небезпечні ситуації, що виникають, причини, через які вони виникають, можливі наслідки, а також шляхи або сценарії розвитку тих чи інших ситуацій. Необхідно виписати характеристики для опису можливих ситуацій і ризиків. Для різних прикладних задач вони суттєво відрізнятимуться. Проте системний підхід, реалізований в узагальненій методології аналізу ризику, є просто необхідним, він дозволяє робити розрахунки, досліджувати складні системи, що складаються з неоднорідних елементів, ідентифікувати небажані події, оцінювати ймовірність або частоту можливих небажаних подій і наслідки, якими вони супроводжуються, обчислювати значення показників ризику, і, відповідно, приймати рішення щодо управління.

Потрібно розуміти, що ймовірність виникнення тієї чи іншої події не означає, що остання протягом деякого періоду часу обов'язково відбудеться. Але незнання, недооцінка або ігнорування небезпек, їх невключення до переліку тих чи інших подій може відіграти фатальну роль. Навіть малоймовірні ситуації, події, що залишилися поза проектними розрахунками (і на це вказує аналіз низки техногенних катастроф), можуть виникати й призводити до значних аварій.

На сьогодні проблеми безпеки та ризиків досліджуються багатьма організаціями і національного, і міжнародного рівнів. Загальновідомими є звіти міжнародних експертних груп при таких установах, як МАГАТЕ і Світовий банк. Міжнародний інститут прикладного сис-

темного аналізу (Австрія) на постійній основі виконує дослідження за напрямом «аналіз ризиків». Публікації МАГАТЕ для спеціалістів з аналізу безпеки та надійності складних систем (і не лише атомних електростанцій) давно стали одним із надійних джерел такої інформації. В Україні останніми роками проводяться міжнародні конференції, присвячені проблемам безпеки критичних інформаційних технологій.

Реальні технічні системи та об'єкти є надскладними для розуміння, вивчення, структурованого (у т.ч. математичного) опису. Це створює складність дослідження ризиків для таких систем. Наприклад, аварія на Чорнобильській АЕС засвідчила, наскільки складно було передбачити й оцінити наслідки, з якими ми досі стикаємося, і ще відчуватимемо в майбутньому.

Наслідки подібних катастроф охоплюють усі сфери життєдіяльності (економіку, охорону здоров'я, політику, соціальну сферу тощо). Нещодавні події в Японії (аварія на АЕС Фукусіма-1) знову привернули увагу світової громадськості до питань безпеки ядерних технологій. Оцінка ризиків, пов'язаних із можливими аваріями на об'єктах атомної енергетики або хімічної промисловості вимагає побудови сценаріїв розвитку зараження територій. Такі дослідження (з оцінювання наслідків і ризиків функціонування великих техногенних об'єктів) є міждисциплінарними, вимагають організації груп експертів, науковців різних напрямів, сфер знань.

У Міжнародному інституті прикладного системного аналізу в 90-х роках було проголошено принцип планування безпеки. Це пов'язано з інвестиціями, витрачанням коштів і ресурсів (проведенням технічного обслуговування, заміною устаткування, введенням резерву, диверсифікацією тощо для зменшення ймовірності відмов) і, відповідно, підвищенням надійності та якості функціонування, досягненням більш високого рівня безпеки.

Вартість заходів, пов'язаних з оновленням систем чи ремонтними роботами, значно менша за обсяг коштів, які витрачатимуться у випадку аварії. Такий підхід розроблявся і використовувався для так званих складних систем із високою ціною відмови (зокрема космічних апаратів, стартових комплексів). І наші українські науковці активно залучалися до науково-дослідних робіт у Красноярську, на Байконурі.

Ідентифікація загроз, що виникають для критично важливих об'єктів та інфраструктури, теж важливе питання. Їх спектр досить широкий, тому для їх ідентифікації потрібно проводити і розвідувальну антитерористичну діяльність, здійснювати постійний моніторинг і збирати статистику про технічний стан інженерних систем, можливі

природні лиха, визначати вразливість інформаційних систем тощо. До того ж загрози інколи мають міжнародний характер, стають транскордонними через масштаби можливих наслідків.

Важливим моментом, на який хочу звернути особливу увагу, є управління ризиками (планування, мінімізація). Вирішення таких завдань потребує розроблення та впровадження математичних методів. Українські вчені мають значні досягнення в цьому напрямі. Загальноприйнятим підходом є побудова математичних моделей об'єкта задля мінімізації показника, що характеризує ризик для даного об'єкта. Це дозволяє визначити оптимальний (в межах припущень моделі) варіант чи вирішення для таких складних систем, як регіон країни, галузь економіки, велике промислове підприємство.

Сьогодні ми говоримо про критичну інфраструктуру, її роль у забезпеченні безпеки держави. Зрозуміло, що до критичної інфраструктури належать найбільш важливі об'єкти, підприємства, установи, але, нагадаю, ще є термін «критичні технології». Напевно, слід враховувати, що до критичної інфраструктури мають також увійти підприємства й установи, де розробляються критичні технології, наприклад підприємства авіаційної промисловості.

Варто зупинитися на кількох специфічних особливостях критичної інфраструктури, які створюють труднощі для моделювання ризиків. По-перше, необхідно враховувати, що моніторинг і здійснення аналізу стану таких об'єктів є необхідним для оцінки ризику. Його здійснюють різні відомства за внутрішніми методиками, через що постає проблема консолідації інформації. По-друге, елементи критичної інфраструктури тісно взаємопов'язані: відмова одного елементу тягне за собою каскад відмов інших елементів. Прикладом каскадної аварії є так зване затемнення 2005 р. – аварія електроенергетичної мережі в Північній Америці, коли наслідки аварії були різноманітними: зупинка муніципального транспорту, відключення світлофорів та освітлення вулиць, освітлення смуг зльоту й посадки літаків, знеструмлення об'єктів прикордонної охорони. По-третє, існує велика кількість різноманітних показників ризику, підходів до його оцінки. Це об'єктивно викликано неоднорідністю елементів критичної інфраструктури.

І, зрештою, хотів би ще раз підкреслити, що в Україні наявний достатній потенціал для вирішення такого складного наукового завдання, як аналіз та управління ризиками критичної інфраструктури. У нас працюють наукові кадри найвищої кваліфікації з цього напряму, кожного року зі стін профільних університетів виходять молоді фахівці, які вміють розв'язувати подібні завдання.

КАЧИНСЬКИЙ А. Б.,
радник директора Національного інституту стратегічних досліджень

Хочу коротко прокоментувати слова щодо оцінки вартості життя в Україні. У нашій з Володимиром Павловичем Горбуліним монографії (опублікованій близько трьох років назад) представлена модель оцінки вартості життя пересічного громадянина України, якою можна скористуватися.

Приватне страхування в історії безпеки – єдиний випадок соціальної угоди щодо проблем безпеки між суспільством і бізнесом. Однак, як свідчить досвід природних лих у Новому Орлеані (ураган Катріна в серпні 2005 р.), а згодом у Японії (цунамі в березні 2011 р.), страхові компанії у цих випадках не лише не спрацювали, вони просто познущалися над людьми. За умов таких масових аварій і надзвичайних ситуацій ані судові позиви, ані інші дії не допомогли: жодної копійки не було відшкодовано.

Я позитивно налаштований щодо страхування, проте дуже сумніваюся, що за такого ставлення при масових катастрофах страхові компанії будуть щось відшкодовувати. У наших українських умовах навіть коли згорає будинок, тебе просять прийти і довести, що рама дверей, які згоріли, не була пошкоджена, і лише після цього відшкодовують збитки.

ЯКОВЛЄВ Є. О.,
провідний науковий співробітник відділу стратегій реформування сектору безпеки Національного інституту стратегічних досліджень

У мене питання до Галини Миколаївни. З огляду на те, що Україна – держава аномальної зношеності усього технологічного обладнання, що, на Вашу думку, є більш ефективним: страхування ризиків чи вихід на нормальний технічний регламент?

ТРЕТЬЯКОВА Г. М. :

На сьогодні страховики дедалі частіше страхують ризик на промислових підприємствах. Проте ми не приймаємо на розгляд об'єкти, які не пройшли аджастингової експертизи. На жаль, нині більше залучаються експерти з-за кордону, оскільки в Україні на сьогодні відсутні приватні структури, які б проводили подібну оцінку ризиків промислових підприємств, що викликала б довіру страхових компаній. Адже на основі такої оцінки можна розраховувати тарифну політику для промислових підприємств. Понад те, є такі страхові покриття промис-

лових підприємств, за якими страховик зобов'язує страхувальника опрацювати план безпечних дій. Якщо страхувальник упродовж терміну, оговореного угодою, не робить цих дій, то страхове покриття або знімається, або підвищується його тариф.

ЯКОВЛЄВ Є. О. :

Є ще питання до Василя Васильовича Бєгуна: в Україні близько 24 тис. потенційно небезпечних об'єктів і до 7 тис. об'єктів підвищеної небезпеки. Яким Ви бачите шлях від визначення «потенційно небезпечні об'єкти» до «критично важливі об'єкти»?

БЄГУН В. В. :

Потрібно скористатися світовим досвідом: створити міжвідомчу групу, визначити об'єкти, методики розрахунку ризиків і розроблення планів реагування тощо.

ЗЕЛЬ В. І.,
головний інженер КП «Київський метрополітен»

Як представник потенційно небезпечного об'єкта хотів звернутися від імені підприємств, основні фонди яких фізично дуже зношені. Яким чином діяти, аби не допустити аварій на таких об'єктах? Метрополітен з погляду пожежної безпеки теж є потенційно небезпечним. Сьогодні слушно зазначали, що за часів СРСР було дещо інше ставлення, інша нормативна база. Наприкінці XX ст. стався випадок у Баку: загорівся вагон метрополітену, дим спрямували не в потрібний бік, унаслідок чого загинуло 300 осіб, адже пластик дуже отруйний.

Із цього випадку зроблено висновки. Тож на сьогодні вже прибрано старі трансформатори, пластик і проводку, які запалюються й виділяють під час горіння токсичні речовини. Тобто намагаємося забезпечити відсутність у метрополітені пожеж, а коли раптом не вдасться, то хоча б щоб запобігти не виділенню отруйних речовин. Це важливий напрям, адже під землею замкнений простір, тому забезпечити пожежну безпеку доволі складно.

На жаль, плата за проїзд, встановлена на сьогодні не дозволяє виконати всі необхідні заходи підвищення безпеки. Те, що вже говорили про мережі водопостачання, теплопостачання, можна сказати і про метрополітен, який теж працює на виживання.

У нас немає можливості оновити основні фонди в повному обсязі, ми лише аналізуємо їхній технічний стан і подовжуємо строки служби (для вагонів встановлений строк експлуатації – 31 рік; у нас деякі з них уже відпрацювали 50 років. Так чинимо з усім: з тунелями, шпалами

тощо. Тому хотів би, щоб нас сьогодні підтримали. Ми бачимо, що можна підвищувати тариф за послуги або фінансувати державні програми. Ми подали проект державної програми розвитку метрополітену, де передбачено і будівництво метрополітенів, і, відповідно, кошти на модернізацію та реконструкцію об'єктів, які знаходяться у критичному стані. Мінінфраструктури нас підтримало. А от Мінфін, Мінекономрозвитку – проти: в держави немає коштів. Крім того, метрополітен – міський транспорт, тому нехай міська влада й вирішує це питання.

Тому хотілося б, аби в рішенні засідання «круглого столу» пролунало, що на підприємствах, які можуть створити критичну ситуацію, мають розроблятися державні програми. Щоб це питання знаходило своє логічне розв'язання. Необхідно не допустити ці підприємства до того критичного стану, коли буде запізно.

Також, як відомо, метрополітен є об'єктом цивільної оборони. Так, Московський метрополітен під час Великої Вітчизняної війни використовувався як об'єкт цивільної оборони (ця доктрина існує ще з радянських часів). Наш метрополітен починав будуватися теж як об'єкт цивільної оборони, підготовлений на особливий період. А тепер, коли грошей не вистачає, усім відомо, як будуються і вводяться станції в експлуатацію.

Цього року теж заявлено про введення двох станцій, на що потрібно 1,8 млрд грн. На сьогодні виділено 15% усієї суми, тобто лише 300 млн грн. Відповідно треба на чомусь заощаджувати ресурси. І що, на вашу думку, прибирається передусім? Звісно, об'єкти цивільної оборони. Тобто об'єкт запускається в експлуатацію в урізаному стані. Тому на сьогодні лише Святошино-Броварська лінія облаштована належним чином: на цій лінії є автономні джерела живлення, система очищення повітря. Інші лінії, які добудовуються сьогодні, як об'єкти цивільної оборони не облаштовані.

Тому прошу записати в рішення перегляд доктрини та порядку дій в особливий період. Адже зазначене теж є критичною ситуацією, яку треба розуміти та обізнано нею управляти.

ЄСИПЕНКО Ю. М.,
заступник начальника Управління координації інспекційної діяльності Державної інспекції ядерного регулювання України

Уже було сказано, наскільки добре розвинена згадана система у країнах Північної Америки, Західної Європи, проте Україна належить до держав іншої фінансової категорії. Хотілося б почути про ситуацію в країнах зі схожими з Україною фінансовими ресурсами. Чи дійсно

потрібно витрачати значні кошти, чи під силу нам будуть такі витрати?

Зовсім незрозуміло, яка система є у нас на сьогодні. Чи взагалі нічого немає? Знаю по своєму відомству (Держатомрегулювання) що є. Можливо, все не так уже й погано? І за ті кошти, що ми маємо, це все, що ми можемо придбати.

ТРЕТЬЯКОВА Г. М. :

Хочу дещо прокоментувати. Безумовно, бюджет, скажімо, Сполучених Штатів Америки, загальний або на душу населення набагато переважає український. Але за пірамідою потреб Маслоу перший рівень – фізичні потреби, тобто потреба виживання. Гарантії безпеки належать до другого рівня цієї піраміди. Вище йдуть рівні, пов'язані із задоволенням соціальних і культурних потреб.

Можна сказати, що ми всі знаходимося на стадії виживання. А людина починає замислюватися про безпеку лише тоді, коли задоволені всі її фізичні потреби. На це слід зважати. Якщо держава почне вкладати кошти в безпеку, то не все населення це оцінить. Частина населення, яка знаходиться на межі виживання запитає, куди передусім витрачати кошти – на їхнє виживання, чи на безпеку.

Ще один коментар щодо того, як у державі мають визначатися пріоритети. Не Міністерство фінансів має визначати стратегічні пріоритети України, воно, навпаки, має виконувати ті стратегічні пріоритети, які йому встановлюють. І якщо ми стратегічним пріоритетом ставимо насамперед соціальні ініціативи виживаність населення, то на другому місці має бути безпека нації. І лише потім усе інше.

Якщо у нас визначатимуть стратегічні пріоритети МНС, Мінсоцполітики, МОЗ, Мінінфраструктури, а не Мінфін, то пріоритети щодо того, куди спрямовувати кошти, мають відповідати названій піраміді потреб.

БІРЮКОВ Д. С. :

Дозвольте сказати кілька слів щодо питань, порушених Юрієм Миколайовичем. По-перше, стосовно витрат на забезпечення захисту критичної інфраструктури у США: на 2012 р. бюджетом заплановано 68 млрд дол. США, і на наступний у плані – 69 млрд дол. США. Так, Україна не володіє такими фінансовими ресурсами, але ми витрачаємо кошти на реагування та ліквідацію наслідків надзвичайних ситуацій.

У нас (і це зазначається в рекомендаціях нашого сьогоднішнього засідання), одночасно функціонує низка державних систем: Єдина

державна система запобігання та реагування на надзвичайні ситуації техногенного і природного характеру; Єдина державна система цивільного захисту населення й територій; Єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їхніх наслідків. За своїм призначенням і функціями вони суттєво перетинаються, проте в організаційному та ресурсному аспектах розділені. Ми бачимо, що є певні способи вдосконалення роботи названих систем.

До того ж у нашому законодавстві є низка категорій об'єктів, виокремлених, зважаючи на їх значимість для економіки, техногенної безпеки, терористичної загрози тощо. З погляду міжнародної практики ці об'єкти, або певна частина списку цих об'єктів, можуть розглядатися як критична інфраструктура.

Ми бачимо проблему не просто у відсутності переліків об'єктів чи самого визначення «критична інфраструктура», а у відсутності взаємозв'язку між цими категоріями, інформаційного взаємозв'язку між відомствами, загальної оцінки на рівні держави ризиків указаних об'єктів, спільного підходу до захисту від усіх груп загроз (техногенного, природного та соціально-політичного характеру). До того ж не існує загальної (спільної) бази ресурсів для реагування та запобігання загрозами, яка б містила інформацію не тільки від МНС, а і, скажімо, від Мінрегіону, де збирається інформація про наявну кількість місць у лікарнях малих міст України та ступінь забезпечення медичним персоналом.

Подібна інформаційна база ресурсів потрібна для оперативного реагування. А на сьогодні не видно, що наші відомства, які опікуються захистом об'єктів критичної інфраструктури, були забезпечені такою інформацією.

СКАЛЕЦЬКИЙ Ю. М. :

Не варто забувати і про те, що безпека – це дохідна справа. Ліпше вкладати гроші в безпеку, ніж ліквідувати наслідки надзвичайних ситуацій, і великі техногенні аварії це неодноразово підтвердили (згадати хоча б Чорнобильську аварію та аварію на нафтодобувній платформі в Мексиканській затоці). Якщо є небезпечні об'єкти, то ними потрібно займатися і забезпечувати відповідний рівень безпеки. Інакше не може бути.

Що стосується концепції критичної інфраструктури, то в Україні вона не впроваджена. На противагу, скажімо, Польщі, де згідно з нею повністю побудований закон, що регулює антикризове реагування.

КОНДРЮК С. М.,
заступник голови Федерації профспілок України

Шановні колеги, спочатку стосовно виживання й безпеки. Спробуймо відповісти на запитання: «Яка частина українського населення позитивно прийняла б бюджетні витрати на додатковий захист від космічного сміття?» Думаю, що три чверті були б категорично проти таких витрат. Як не дивно, і більшість населення була б навіть проти досить значних витрат на добудову нового саркофага на ЧАЕС. Саме тому, як уже зазначалося, на сьогодні для більшості населення важливішими є проблеми не післязавтрашні, а саме сьогодення.

Щодо можливостей держави. На сьогодні, можливо, зовсім не правильно проходить комерціалізація в питаннях безпеки. Скажімо, ми знаємо, що нині приватизовані певні системи енерго-, теплозабезпечення населення тощо. Напевно, це правильно, оскільки держава виявилася нездатною їх фінансувати. Але тоді постає питання щодо фінансової доступності таких критично важливих чинників життєзабезпечення, як тепло, дах, чиста питна вода.

На сьогодні понад чверть населення України має дохід, менший за прожитковий мінімум. Причому, підкреслю, прожитковий мінімум був визначений у «голодному» 2000 р., коли споживча вартість заробітної плати в Україні була найменшою. І на сьогодні (навіть за таким критерієм!) значній частині українського населення фінансово недоступно чимало з того, що, напевно, має бути віднесено до послуг критичної інфраструктури.

Кілька слів стосовно ініціатив Президента України. Федерація профспілок, безперечно, підтримує їх, адже вони захищають найбільш знедолене населення. Проте (і це постійно привертає нашу увагу) ці ініціативи поглиблюють диспропорції, що склалися в Україні. Сьогодні заробітна плата в сукупних доходах населення складає вже менше 40%, хоча мала б складати 65–70%. Решта – це пенсії, соціальна допомога, житлові субсидії тощо. Отже, сьогодні, на жаль, заробітна плата є неплатоспроможною. Вона взагалі є нерентабельною з погляду економічних оцінок, і це призводить до того, що споживачами платних послуг від критичної інфраструктури є досить незначна частина населення. Понад те, більшість навіть не має доступу до цих платних послуг.

З іншого боку, така ситуація призводить до загального соціального відторгнення тез щодо активної фінансової участі держави в забезпеченні розвитку, формування та підтримки критичної інфраструктури. Тут необхідно вживати комплексних заходів.

СКАЛЕЦЬКИЙ Ю. М. :

Хотів би підтримати Сергія Михайловича та Галину Миколаївну. Відоме таке поняття, як сприйняття ризику населенням. Наприклад, можна говорити, що наслідки аварії на Чорнобильської АЕС у плані радіаційних ризиків (згідно з порівнянням результатів наукових і соціологічних досліджень) переоцінюються населенням. Ідучи на поводу в населення, політики приймали відповідні законодавчі акти, які практично не можуть забезпечуватися фінансовими можливостями держави. Саме через це виникає конфлікт між населенням і державою.

Тому потрібні механізми, які б об'єктивно оцінювали такі ризики. Це питання можна було б порушити перед Громадською радою з питань вивчення ризиків, що функціонувала при МНС і НАН України.

КОНДРАТОВ С. І.,
старший науковий співробітник
відділу екологічної та техногенної безпеки
Національного інституту стратегічних досліджень

Хотів би повернутися до питання про критичну інфраструктуру та доцільність введення цієї концепції в Україні. На мою думку, можна додати декілька аргументів на захист цього. По-перше, якщо в ЄС і таких провідних країнах, як США та РФ, концепція захисту критичної інфраструктури прийнята, то Україні теж є сенс розпочати такий процес. Оскільки ми й досі прагнемо інтегруватися в ЄС, то це передбачає гармонізацію підходів у сфері безпеки.

По-друге, витрати на забезпечення безпеки дійсно завжди суттєві, і необхідно здійснювати аналіз ситуації у цій сфері. В Україні діє низка державних систем, функціонування яких недофінансовується, однак кошти на них виділяються. Можливо, більш раціональним було б утримання однієї системи, здатної ефективно реагувати на всі види загроз.

До того ж варто нагадати, що у рішенні Сеульського саміту з фізичної ядерної безпеки в одному з пунктів ішлося про поєднання зусиль щодо боротьби з ядерним тероризмом *(nuclear security)* і технічної ядерної безпеки *(nuclear safety)*. Тут реалізується так званий підхід *all hazard approach*, який ураховує всі види загроз.

Стосовно МНС та успішної роботи. Так, ми можемо назвати певні досягнення у цьому напрямі. Проте МНС не діє в межах підходу, рекомендованого МАГАТЕ і ще раз проголошеного на Сеульскому саміті. Зокрема не враховуються загрози ядерного тероризму, а хіба

МНС працює з терористичними загрозами? Ні. Тобто попередження й реагування здійснюється на стику роботи СБУ та МНС, і саме тут виникають проблеми.

Ми з колегами намагалися аналізувати ситуацію в Кримську, де формально населення було попереджене про загрозливі природні умови, з дощами, можливим штормовим попередженням тощо. Саме на стику взаємодії відомств, місцевої влади та МНС РФ виникли проблеми. У результаті населення не було готове до природного лиха. Коли система аналізується в цілому, вона готова реагувати на загрози різного характеру, і є можливість відслідковувати й урахувати всі взаємозв'язки.

КОРЖ І. Ф.,
головний консультант Комітету Верховної Ради України з питань національної безпеки і оборони

Хочу висловити кілька зауважень. Цілком згоден з В. В. Бєгуном у тому, що російський варіант визначення «критично важливі об'єкти» більш вдалий. Проте життя не стоїть на місці, воно вносить свої корективи. На сьогодні існують не тільки критичні об'єкти, а й критично вразливі системи. Наприклад, правова система держави або система судочинства, які існують у своїй цілісності. Викинути якийсь об'єкт із такої системи неможливо. Тому, на мій погляд, більш вдалим буде визначення «критичні об'єкти й системи».

Період нещодавньої економічної кризи продемонстрував, яка є загроза фінансово-кредитній системі, прикладом чого стали події в низці країн Заходу, насамперед у Греції та Іспанії, на черзі – Італія. На сьогодні існують і виникають нові загрози соціально-політичного характеру. Ще у 2008 р. в газеті «Правда України» було надруковано статтю про політичну корупцію та правову безпеку, де наголошувалося на правовій безпеці держави, адже негативний вплив відповідних чинників може спричинити загрози існуванню держави.

На сьогодні ми бачимо певні ризики (на перший погляд латентні), які можуть мати далекосяжні наслідки для держави, суспільства, людини. Це спостерігається і в культурній, і в соціальній сферах. Останні події, що похитнули існуючу державно-політичну систему (насамперед щодо системи стримування противаг), теж викликають відповідні загрози, на які ми звертаємо увагу, розробляючи документи, напрацьовуючи пропозиції. На жаль, до цього часу позитивних зрушень мало.

Чи потрібно створювати нові інституції задля забезпечення безпеки критичних об'єктів? У нас є Рада національної безпеки і оборони

України, яка має поєднувати в собі усі заходи, пропозиції, напрацьовані суспільством, для того, аби усунути загрози, які виникають, або можуть виникнути. Це дійсно має бути тим інститутом, який повинен реагувати і превентивно, і реально на існуючі та ймовірні загрози. На жаль, РНБО поки що не виправдовує свою назву. Можливо, грубо буде сказано, але на сьогодні її Апарат перетворено на політичний «відстійник». Адже був період, коли Апарат РНБО працював під керівництвом Володимира Павловича Горбуліна, коли діяльність цієї інституції була дійсно продуктивною і добре скоординованою.

Тепер щодо проекту рекомендацій: помітив, що основний акцент зроблено лише на двох аспектах – загрозах техногенного й природного характеру. А третьому аспекту – загрозам соціально-політичного характеру – взагалі не приділено уваги.

Вважаю, зі мною погодиться Василь Іванович Варус у тому, що з будь-якою хворобою або епідемією боротися можна вічно, якщо не проаналізувати причини й умови її виникнення. І тільки усунувши останні можна боротися із загрозами.

Якщо проаналізувати загрози техногенні, то всі погодяться, що значна частка провини – це діяльність людини. А це можна добре вивчити і мінімізувати саме завдяки вивченню системи соціально-політичного характеру. Тому пропоную окремо розглянути питання загроз і викликів, які існують у соціально-політичній сфері. Адже роль людини для нас досить важлива і у виникненні цих загроз, і в їх усуненні.

О. В. Литвиненко у вступному слові говорив про соціально-політичні загрози з акцентом на тероризмі. Раніше терористичні акти вже відбувалися в Україні: в Криму, Чернігові, Запоріжжі. Але чим вони були викликані? Не меркантильними інтересами, а безвихіддю, в якій опинилися люди, зіштовхнувшись із безправ'ям у судовій системі. Коли вони не могли знайти правду і справедливість при вирішенні тих чи інших питань. Саме ця безвихідь підштовхувала людей на крайні заходи. Навесні я був присутнім у НІСД на засіданні з питання радикалізму й тероризму. Ішлося про необхідність напрацювання певних законодавчих пропозицій щодо боротьби з екстремізмом. Адже він виникає як реакція на несправедливі дії влади і підштовхує до маргінальних дій. Якщо влада проаналізує причини й умови виникнення таких негативних чинників, то потреба в коштах і силах буде набагато меншою, і, вважаю, результат буде ліпшим.

Пропоную провести саме цільовий захід із розгляду проблем соціально-політичного характеру. Адже причини і технологічні, і природного й соціально-політичного характеру пов'язані між собою. Тіль-

ки з огляду на їх взаємозв'язок можна вирішити проблеми безпеки, на яких акцентувалася увагу на цьому засіданні.

СКАЛЕЦЬКИЙ Ю. М. :

Саме з метою врахування людського чинника у системі безпеки в Інституті було проведено два засідання з питань екологічної безпеки й культури безпеки. І, напевно, найближчим часом ви отримаєте доопрацьовані рекомендації останнього заходу разом з науково-аналітичною доповіддю.

КАЧИНСЬКИЙ А. Б. :

Хотів би повернутися до витоків терміна «критична інфраструктура». На сьогодні відомі (принаймні мені) два випадки, коли дійсно виникала реальна загроза критичній інфраструктурі окремих держав. Перший – у 1999 р., коли понад половину Канади було знеструмлено через магнітну бурю на Сонці, яка спричинила збої в комп'ютерних та електронних приладах. Унаслідок цього Канада втратили надвеликі кошти. Це приклад природно-техногенного складника. Другий випадок – це міленіум 2000 р., коли на порозі зміни тисячоліть очікувалися масові збої обчислювальних систем, через що, відповідно, мала постраждати вся інфраструктура – глобальна, а не тільки окремої держави.

Справді, на Заході з'явилося поняття «критична інфраструктура». Що спричинило його виникнення? Безумовно, американці, коли почали аналізувати перші хакерські атаки, дійшли висновку, що комп'ютерне обладнання, як зазначив попередній доповідач, потрібно розглядати як систему. На сьогодні всі системи життєзабезпечення зав'язані на мережеве та комп'ютерне обладнання. Останнє має таку особливість, як програмні закладки (у т.ч. протоколи тощо), які волоконними мережами пов'язують мільйони комп'ютерів у системах передачі інформації. Тобто є три групи: семантичні, лінгвістичні й математичні методи захисту інформації від нападу на комп'ютерні системи.

Можна згадати випадок з естонським солдатом, який перебуваючи в Лос-Анджелесі, здійснив атаку на сайт уряду Естонії. Тоді стало зрозуміло, наскільки системи життєзабезпечення Сполучених Штатів вразливі до кіберзагроз, а також те, що не треба починати війну – достатньо вивести одну за одною системи життєзабезпечення, паралізувати діяльність столиці чи цілої галузі, використовуючи сучасні комп'ютерні технології. Саме тоді почали говорити про критичну інфраструктуру, а при Пентагоні було створено кібервійська.

Така ситуація характерна для високотехнологічного суспільства, високотехнологічної економіки, основою управління якої є комп'ютерні системи – інформаційний складник. У нас, на превеликий жаль, такого рівня комп'ютеризації не досягнуто.

В Україні на понад 85% зношені основні виробничі фонди. Говорити про те, що ми побудуємо реальну систему захисту критичної інфраструктури за умов такої зношеності фондів, – нереально. Насамперед треба вкласти кошти в модернізацію основних фондів, а потім інвестувати в безпеку, що вкрай дорого. Тому, коли ми говоримо про ризики й безпеку, зрозуміло, що чим більші ризики, тим більше коштів треба витратити на забезпечення безпеки. Усе залежить від коштів, а їх в Україні немає.

Тому в управлінні ризиком є поняття прийнятної величини ризику, рівень якого у нас досить високий. Якщо повернутися до піраміди потреб Маслоу, яку тут уже згадували, то чи варто говорити про забезпечення потреб у безпеці, коли у нас один із найбільших у світі рівнів суїцидів. А це показник, що характеризує вартість життя і ставлення до безпеки. Тим більше, що суїцид здійснює переважно молодь віком до 38 років з вищою освітою.

Отже, навіть власне життя в українському суспільстві для значної частини нічого не варте (однією з причин є те, що заробітна плата перестала виконувати свою соціальну функцію). Тому сісти, порадитися і запропонувати вихід, за відсутності в державі коштів нереально. Повторюся: безпека – це дуже дорого.

Тому, аби наслідки нашого «круглого столу» мали результат, ми повинні обмежитися реальними рекомендаціями. Дійсно, я погоджуюся, нормативно-правова база має відповідати міжнародним нормам. Як уже говорив Сергій Іванович Кондратов, якщо вище керівництво нашої держави декларує те, що ми йдемо в Європу, то необхідно привести у відповідність свою нормативно-правову базу. Це перше.

Друге, на мою думку, – це людський чинник, депрофесіоналізація. У нас люди обіймають вищі посади, не маючи ані відповідних дипломів про освіту, ані життєвого досвіду. Подивіться: хто є заступниками міністрів, хто є керівниками департаментів? У Закон України «Про державну службу» треба внести пункт, який би регламентував вимоги до керівників: десять років практичної діяльності в даній сфері й наявність диплома про освіту.

Третє. Для критичної інфраструктури актуальні асиметричні, несилові загрози. Тероризм, спецоперації, зокрема людський і природний чинники. Усі ці загрози прописані в Законі України «Про основи національної безпеки», у т.ч. і за галузевими напрямами (надзвичайні

ситуації, екологія тощо). Треба просто виконувати те, що на сьогодні вже регламентовано.

Я вчений, і хотів сказати ще про ризик. Тут неодноразово говорили про відсутність уніфікованої математичної моделі ризику. Хто вірить, що така можливість – це утопія? Моя перша дисертація (ще за часів СРСР) була присвячена загальній теорії ризиків. Прикладом найбільш розроблених математичних моделей ризиків є фінансові інструменти. Ми всі пам'ятаємо класичні моделі Марковіца й Шарпа з фінансової математики. Сьогодні всі звинувачують такі підходи з управління ризиком, страхування та перестрахування в тому, що фінансова система була штучно «роздута» страховими інструментами (ф'ючерси, форварди, хеджи, опціони), і саме це спричинило сучасну світову фінансову кризу.

Ризик характеризують два складники: імовірність загрози та розмір збитків, пов'язаних із нею. Якщо в тому, що ви розглядаєте, вони відсутні, то ніякої навіть найбільш простої математичної моделі бути не може. Управління ризиком, коли ми говоримо про державу, може здійснюватися тільки з огляду на величину прийнятного ризику.

Ще раз наголошую, коли в нас очікувана тривалість життя всього 63 роки (для чоловіків), імовірність низки тяжких хвороб 10^{-4} (у Європі 10^{-6}), то про який вигляд критичної інфраструктури для України ми повинні говорити? Це питання треба обміркувати більш детально.

З одного боку, внаслідок того, як складається політична ситуація, ми повинні враховувати задекларовані політичним керівництвом держави напрями розвитку, а з іншого – на це немає фінансових можливостей. Тут треба знайти компроміс, аби результати нашої сьогоднішньої дискусії мали реальні результати.

БОЧАРНИКОВ В. П.,
провідний науковий співробітник
Національного університету оборони України

Сьогодні ми розглядаємо дійсно важливе питання, а зважаючи на те, що розглядається воно у Національному інституті стратегічних досліджень, статус його високий.

На жаль, на мій погляд, низка питань випала з розгляду. Майже не приділялася увага таким питанням: місце і роль Міноборони, МВС, СБУ в попередженні загроз соціально-політичного характеру, особливо в умовах особливого періоду, в т.ч. і воєнного часу. Крім того, чи правильно я зрозумів, що в цілому реєстру об'єктів критичної інфраструктури не існує. Тобто такі об'єкти не визначені через відсутність самого реєстру, відповідно, відсутні і паспорти цих об'єктів, структура їх охорони та оборони, порядки залучення відповідних

міністерств і відомств (у т.ч. Міноборони, внутрішніх військ, СБУ), також повністю відсутня їх взаємодія.

Також, як я розумію, суто відомчий характер мають плани забезпечення охорони об'єктів критичної інфраструктури в умовах мирного та особливого періоду, в т.ч. і воєнного часу. В такій ситуації важливою є наявність єдиного центру, хоча б чітко визначеної системи моніторингу та прогнозу ризиків і загроз за відповідними напрямами. Причому має бути тісна взаємодія з такими центрами, як Антитерористичний центр при СБУ, Центр оцінки і прогнозу військово-політичної обстановки тощо. Ці питання залишаються нерозглянутими. Нагадаю, що на початку місяця була прийнята оновлена Стратегія національної безпеки, нова редакція Воєнної доктрини України, на які слід зважувати, розглядаючи питання захисту критичної інфраструктури.

Відповідно, якщо говорити про методологію, то, наприклад, для загроз жоден імовірнісний підхід не годиться. Немає оцінки ймовірності терористичної атаки 9/11. Це унікальний випадок, проте його можна було б передбачити й вчасно запобігти. Отже, говорячи про методологію, можна стверджувати, що, безумовно, однієї теорії імовірності тут не вистачить – потрібно використовувати сучасні підходи: теорію можливості, нечіткі моделі тощо. Тому, чесно кажучи, хотілося б, аби порушені мною питання увійшли до рішення «круглого столу».

СКАЛЕЦЬКИЙ Ю. М. :

Ви порушили широкий спектр проблем, Вікторе Павловичу, які, ми з вами згодні, потрібно розв'язувати. Наступного року в Інституті заплановано проведення конференції з напряму «захист критичної інфраструктури». І ми зможемо в більш розгорненому форматі винести ці питання на обговорення. Стосовно оновленої Стратегії національної безпеки та нової Воєнної доктрини України, то Інститут брав безпосередню участь в опрацюванні цих документів, тому вони, безумовно, будуть враховані.

ХАРЧЕНКО В. С.,
завідувач кафедри комп'ютерних систем і мереж факультету радіотехнічних систем літальних апаратів, Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

Як представник Національного аерокосмічного університету хотів би сказати про нашу дослідницьку діяльність у сфері захисту критичних інформаційних технологій. На базі нашої кафедри вже кілька років працює Науково-технічний центр з інфраструктурної безпеки,

і понад десять років ми здійснюємо дослідження з безпеки в галузі атомної енергетики, передусім інформаційних технологій.

Підкреслю, що важливим складником критичної інфраструктури є інформаційна інфраструктура. Використовуються терміни «критичні *IT*-інфраструктури», тому що вони, з одного боку, створюють можливості для підвищення безпеки об'єктів, з іншого – нові технології привносять додаткові дефіцити безпеки. Разом з тим хочу зазначити, що коли ми обговорюємо питання безпеки цього складника (*IT*-інфраструктур), потрібно вивчати не тільки інформаційну, а й функціональну безпеку. Оскільки, наприклад, під час розгляду питання безпеки автоматизованих систем управління ядерними реакторами саме функціональна безпека виходить на перший план. Украй важливим є комплексний характер такого аналізу, і тішить, що Україна посідає гідне місце у світовому товаристві із цього питання, про що свідчить високий рівень модернізації інформаційно-керуючих систем (близько 90%).

Це вже обговорювалося на міжнародних конференціях у Сполучених Штатах та Канаді, і, як не дивно, у цих країнах рівень модернізації відповідних систем нижчий, а системи побудовані на мікросхемах 40-річної давнини. Це створює суттєві проблеми для модернізації, а наші вітчизняні науковці мають певний досвід з їх вирішення.

Підтримую думку про те, що наша країна має обмежені можливості, тому потрібно їх використати ефективно. Наведу такий приклад: на базі кафедри постійно організовуються семінари, уже сім років проводиться міжнародна конференція з надійності безпеки, або гарантоздатності комп'ютерних систем. І в питанні безпеки потенційно небезпечних об'єктів інформаційні технології можуть зіграти важливу роль.

Потужно розвиваються так звані хмарні обчислення *(cloud computing)*. Зважаючи на їхні можливості, можна було б оптимізувати кошти, що витрачаються на створення інформаційних систем для потенційно небезпечних об'єктів за рахунок створення корпоративних або національних систем із хмарних обчислень. Це могло б зменшити витрати на вказані системи і разом з тим підвищити оперативність інформації у цій сфері.

Також хочу наголосити на тому, що важливим складником критичної інфраструктури є енергетика (зокрема атомна), яка має специфічні ризики. Є можливість використання *Smart Grid*-технологій, які б могли зменшити втрати на всіх етапах від генерування електроенергії до використання кінцевим споживачем. Такі технології активно поширюються у всьому світі. Наприклад, у Росії цей нап-

рям має вагому підтримку. В Україні, на жаль, це питання майже не розглядається. Проте, з одного боку – це питання безпеки, а з іншого – економіки та екології. Вважаю, цим аспектам потрібно надавати особливої уваги.

СУСЛОВ С. М.,
головний фахівець відділу нагляду з питань техногенної безпеки та контролю за органами виконавчої влади Управління техногенної безпеки Державної інспекції техногенної безпеки України

Підкреслю, що на сьогодні Державна інспекція техногенної безпеки є органом, який знаходиться в юрисдикції Міністра з надзвичайних ситуацій. Зауважу, що тут все говорилося з позиції Міністерства, а не Інспекції.

Справа в тому, що МНС не виконує функції забезпечення безпеки певних об'єктів: чи атомних установок, чи інших промислових об'єктів. Воно забезпечує захист населення у випадку аварії на цих об'єктах. Відповідно, сьогодні було порушено питання стосовно того, що МНС не підтримує зв'язок з Антитерористичним центром та іншими структурами. Навпаки, у системі МНС створено відповідні відділи, укомплектовано спеціалістами, які тісно співпрацюють з тим самими центрами або іншими структурами. Це питання знаходиться на контролі МНС.

Стосовно того, чи існує на сьогодні поняття «об'єкти критичної інфраструктури» або «критично важливі об'єкти». Це теж можна розуміти по-різному: об'єкти, що можуть виконувати певні функції в умовах надзвичайних ситуацій (і через це бути критичними), або ж об'єкти, що можуть піддаватися загрозам, впливам унаслідок надзвичайних ситуацій. Є також низка пов'язаних із проблемою аспектів.

На сьогодні законодавча база є недосконалою – навіть у системі МНС (вона створювалася фактично зі Штабу цивільної оборони на основі досвіду ліквідації наслідків аварії на ЧАЕС). Відповідно, всі функції Міністерства щодо захисту населення були сформовані під впливом або міжнародних документів, або політичних дискусій. Тому такі назви, як «об'єкти підвищеної небезпеки» і «потенційно небезпечні об'єкти», не приживаються в інших міністерствах, хоча й існують у законодавстві .

І саме різне трактування зазначених понять інколи унеможливлює спілкування однією мовою. Якщо ми говоримо, що існують вказані об'єкти, то, підкреслю, з-поміж іншого, є об'єкти з високим ступенем

ризику[112], що визначаються залежно від їх впливу на техногенну безпеку й екологію.

Об'єкти, якими управляють комп'ютерні системи (навіть якщо сам об'єкт не є критичним з погляду надзвичайної ситуації), можуть нести суттєві загрози, наприклад фінансова система. Тому, якщо говорити про концепцію критичної інфраструктури, потрібно чітко усвідомлювати, які сфери закладені в цю концепцію, як вони мають відображатися в законодавстві та організаційних структурах.

На сьогодні для виконання завдань щодо забезпечення безпеки населення в надзвичайних ситуаціях системі МНС передано такі функції, як, наприклад, управління охороною праці та промислова безпека. Водночас питання реагування й ліквідації наслідків можливих аварій на атомних станціях потрібно розглядати у двох аспектах. Потрібно зважати на ядерне законодавство, враховувати відповідні плани реагування, регламентацію з безпеки та фізичного захисту ядерних об'єктів. МНС у цих питаннях розглядає АЕС тільки як об'єкти, наслідки аварії на яких можуть бути катастрофічними.

Стосовно компетенції вищих керівних кадрів органів виконавчої влади, зазначу, що за весь час існування МНС лише одного разу на посаді заступника міністра була людина, яка пройшла весь шлях, починаючи від простого співробітника. Але цей випадок, скоріше, виключення, ніж правило.

ВАРУС В. І.,
начальник Науково-дослідного інституту проблем військової медицини Збройних Сил України

Хотів би звернути увагу на одну обставину, яка суттєво впливає на стан національної безпеки. Мається на увазі реформування міністерств і відомств, що відбувається досить бурхливо. Безумовно, поточні події впливають щонайменше на такі п'ять аспектів: матеріально-технічну базу, технології, кадровий потенціал, організацію роботи й поточне постачання. Безумовно, вони впливають на рівень готовності об'єктів, які мають реагувати у випадку надзвичайної ситуації. Так, у результаті реформування Міністерства оборони України військово-медичні ресурси можуть бути зменшені майже удвічі. Але

[112]*Про затвердження* критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки : постанова Кабінету Міністрів України від 29.02.2012 р. № 306 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/306-2012-%D0%BF

їхнє місце мають посісти структури, які у випадку надзвичайної ситуації чи іншого виклику могли б відреагувати у надзвичайних умовах. Тому, на мою думку, важливо, аби розробники концепції передбачили узгодження трансформації міністерств і відомств у аспекті підтримання відповідного рівня національної безпеки.

Вважаю, одна із пропозицій має стосуватися об'єктів (особливо відомчих), що відіграють украй важливу роль у випадку надзвичайної ситуації для всієї держави. Можливо, не варто скорочувати чи розформовувати їх, натомість передати на національний або міжвідомчий рівень, і утримувати на випадок надзвичайної ситуації, а повсякденно доцільно, аби вони виконували функції, скажімо, міжвідомчого характеру.

ЯКОВЛЄВ Є. О. :

Зверну увагу на дві пропозиції, що пролунали сьогодні під час виступів. На мою думку, нам необхідно дотримуватися історичного змісту терміна «критична інфраструктура». Усе-таки розуміння ролі інфраструктури зароджувалося у військових у Європі і певною мірою у США.

Стосовно України, то першими спробами були дослідження з ініціативи Володимира Павловича Горбуліна (тоді ще директора Інституту проблем національної безпеки), коли три відділи (техногенної безпеки, інформаційної безпеки й аграрно-економічний) надали свої оцінки. Уже тоді можна було побачити перелік критичних інфраструктур, до якого увійшли енергетика, насамперед атомні електростанції, транспорт тощо. Європейський підхід не зовсім підходить для України, адже там немає систем водовідведення, не згадується і про органи внутрішніх справ.

Що ж ми маємо зараз? Рівень ризику в житлово-комунальному господарстві – 10^{-4}, проти, як зазначав Анатолій Броніславович Качинський, європейського рівня – 10^{-6}. Якщо не буде зрозуміло, який обсяг фінансування потрібен, аби хоча б на порядок знизити цей ризик (адже різниця у 100 разів), то ми не вийдемо на державну компенсацію страхових внесків, які знаходяться між європейським рівнем і нашим.

Тепер щодо систем водовідведення. Наприклад, Бортницька система є критичною чи ні?

Атомна енергетика. Говорять, що рівень фізичної та ядерної безпеки достатній. Однак у результаті подовження терміну експлуатації на Рівненській АЕС під час ремонту ми мали надзвичайну ситуацію. Який зараз стан мають Південноукраїнська, Запорізька АЕС? Та сама

Рівненська АЕС? Їхні показники не увійшли навіть до програми подовження терміну експлуатації. То вони є критичними об'єктами? Так, без сумніву. Але мають інший набір параметрів, відмінний від того, який є за відомчими документами.

Якщо наводити приклади загроз, про які говорив Василь Васильович Бєгун, то необхідно згадати, як нещодавно у м. Львові унаслідок розрушення будівлі загинули дві людини, одна з них – іноземець. Якщо взяти щорічні запуски теплових мереж, то у нас за критичністю навіть житловий комплекс виходить на перший план.

Проте, на мою думку, зважаючи на все сказане, перелік рекомендацій вимагає скорочення. Обов'язково необхідно залишити пункт про Робочу групу при РНБО для створення переліку об'єктів критичної інфраструктури (за кожним відомством, кожною галуззю).

Це питання треба вирішити, адже навіть США із початкової кількості у 33 тис. об'єктів скоротили перелік до 1700 об'єктів, визначених як критичні. А там не було й немає таких систем, як водовідведення. А нам це потрібно, оскільки ситуація, що склалася з Дніпром (а він є джерелом постачання 60% питної води населенню країни), потребує цього.

Також варто записати в рекомендації необхідність обстеження тих масштабних об'єктів, на яких уже були надзвичайні ситуації. І, зрештою, давайте орієнтуватися на таке визначення критичної інфраструктури: сукупність об'єктів, технологій, державних і наукових структур, порушення регламентної діяльності яких впливає на економічну, соціально-політичну, військову, екологічну безпеки. Саме на це нам слід орієнтуватися.

І ще один момент. Продовжу думку професора Качинського. Нам потрібно зважати на те, яку інформацію ми можемо отримати. Вірогідно, що про критичні системи та об'єкти – ніякої. Треба також звернути увагу на взаємодію щодо моніторингу цих об'єктів із Державною системою моніторингу стану навколишнього середовища. Без цього всі рекомендації та побажання залишаться лише гаслом, не будуть фізично забезпеченими ані економічною, ані екологічною, ані соціальною інформацією.

ЄСИПЕНКО Ю. М. :

Підтримую пропозицію про створення дорадчої комісії при РНБО, яка зможе зібрати центральні органи виконавчої влади, переглянути в разі потреби, рівні повноважень і компетенції цих органів.

Щодо централізованого органу з питань захисту критичної інфраструктури, то вважаю, що створювати його недоцільно.

КОНДРЮК С. М. :

Хотілося б, аби в рекомендаціях було вказано про необхідність визначення критеріїв допустимої глибини комерціалізації об'єктів та систем критичної інфраструктури, а також параметрів платоспроможної доступності платних послуг зазначених інфраструктур.

Разом з тим необхідно звернути особливу увагу на кадрове забезпечення об'єктів критичної інфраструктури, а також на мотивацію до високопрофесійної роботи. Чому звертаю увагу на це? На прикладі багатьох підприємств, які належать до критичної інфраструктури, можна побачити, що середня заробітна плата працівників, у ліпшому випадку, близька до середньої по Україні, а найчастіше навіть нижча за середню. Очікувати, що саме на цих підприємствах не буде створено певних ризиків або небезпеки, складно.

ВАРУС В. І. :

Хочу підтримати колегу з Національного університету оборони України в тому, що сьогодні ми так і не почули відповідь на запитання «Чи відносимо ми об'єкти оборони до критичної інфраструктури?» Виходить, що ми забули про такі надзвичайні ситуації, як, наприклад, вибухи боєприпасів на військових складах у с. Новобогданівка Мелітопольського району Запорізької області.

Тому в нас є пропозиція врахувати об'єкти військової сфери і внести їх до пунктів рекомендацій щодо діяльності Міноборони.

СКАЛЕЦЬКИЙ Ю. М. :

Шановні колеги! Зазначу, що на засідання «круглих столів» у Національному інституті стратегічних досліджень ніколи не виносяться питання, які мають тривіальне розв'язання. І сьогоднішній захід – не виняток.

Захист критичної інфраструктури є багатоаспектною проблемою, тому запланована на 2013 р. конференція надасть більше можливостей для обміну досвідом і думками щодо її вирішення.

Ваші пропозиції та побажання, висловлені під час сьогоднішнього обговорення, будуть обов'язково враховані. Дякую всім за активну участь і цікаву дискусію!

ЗМІСТ

Наукове видання

Бірюков Дмитро Сергійович
Кондратов Сергій Іванович

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Аналітична доповідь

Літературний редактор: *О. В. Москаленко*
Коректор: *І. В. Куницина*
Комп'ютерне верстання: *О. В. Москаленко*

Відповідальний за випуск: *В. М. Сизонтов*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел. (044) 234-50-07

Формат 60х84/16. Ум. друк. арк. 5,58. Обл.-вид. 6,73 арк.
Тираж 200 пр. Зам. № _

Віддруковано ПП «Вид-во «ФЕНІКС»
вул. Шутова, 13 Б, м. Київ, 03680
Тел. (044) 501-93-01
Свідоцтво суб'єкта видавничої справи ДК № 271 від 07.12.2000

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК