УДК 517:338.49:574.2

АНАЛІЗ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА НАПРЯМКИ ДОСЛІДЖЕНЬ СИСТЕМ ЖИТТЄЗАБЕСПЕЧЕННЯ ОБ'ЄКТІВ УКРАЇНИ

здобувач В.М. Чернета, головний ассистент Ю.Е. Варадинова*

Дніпропетровська державна фінансова академія,

**Вище транспортне училище імені Тодора Каблешкова, м. Софія, Болгарія*

Частина цивільної інфраструктури, що представляє собою сукупність фізичних або віртуальних систем і засобів, важливих для держави в такій мірі, що їх вихід з ладу чи знищення може призвести до згубних наслідків в області оборони, економіки, охорони здоров'я та безпеки нації називається критичною.

Дослідження критичної інфраструктури стають пріоритетними в багатьох країнах світу, в першу чергу в США, де рівень розвитку інформаційних технологій та можливості сучасних комплексів імітаційного моделювання постійно підвищуються. Серед цілей подібних досліджень виділяють захист національної критичної інфраструктури та організацію впливу на її об'єкти у супротивника. При цьому головне завдання полягає у виявленні ключових об'єктів (або їх сукупності), вплив на які може надати найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці наслідків подібного впливу та розробці механізмів зниження таких ризиків. Так, наприклад в законодавстві Республіки Болгарія критична інфраструктура визначена як система або її частини, які мають основне значення для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, надійності, економічного чи соціального добробуту населення, і чиє порушення або знищення мало б значні негативні наслідки для держави в результаті неможливості зберегти ці функції. [1]

Разом з тим, однією з основних труднощів при виявленні ключових об'єктів критичної інфраструктури до недавнього часу була відсутність чіткого математичного апарату, що не дозволяло сформувати кількісні показники вразливості об'єктів. Ймовірно, цим і можна пояснити те, що в основі більшості подібних досліджень лежав метод експертних оцінок, який передбачає обов'язкову наявність інформації про можливу шкоду «еталонного об'єкту» або розробку спеціальної шкали факторів ризикованості («небезпечності») таких.[2]

Яскравим прикладом подібної роботи є модель, розроблена фахівцями міністерства внутрішньої безпеки (МВБ) і міністерства оборони США, в основу якої покладена методика визначення пріоритетності об'єктів ключових фондів військово-промислової бази (The Asset Prioritization Model - APM). Суть її полягає в розрахунку індексу ризикованості об'єкта, залежного від рейтингу об'єкта за шкалою категорії факторів і значущості даного чинника. Основний недолік подібних моделей полягає в тому, що дослідження, як правило, здійснювалися без урахування зв'язності вхідних до неї об'єктів. У той же час без

урахування і аналізу мережевої складової кожного сектора критичної інфраструктури (економічного, фінансового, енергетичного і т. д.) дуже проблематично забезпечити достатню адекватність моделі об'єкту дослідження.[3]

Складність взаємозв'язку елементів критичної інфраструктури та важливість їх розуміння відображає інцидент, що стався 19 липня 2001 року, коли поїзд з 62 цистернами, що перевозив небезпечні хімічні речовини, зійшов з рейок у тунелі на Говард-стріт в м. Балтімор, США. Крім порушення залізничного і автомобільного сполучення, відбулося каскадне руйнування інфраструктури. Так, в результаті інциденту були пошкоджені: труба магістрального водопроводу діаметром 20 дюймів, сталося затоплення тунелю на глибину до трьох футів, в результаті чого вийшла з ладу система електропостачання ділового району м. Балтімор; оптоволоконний кабель, що призвело до порушення роботи телефонних станцій, інформаційних та поштових служб, включаючи телекомунікаційні компанії Крім того, руйнування залізничного сполучення мало наслідки і для штатів Нью-Джерсі, Пенсільванія, Делавер, Нью-Йорк і Меріленд у вигляді затримок доставки вугілля і сталі. Для усунення виявлених недоліків в США почалося формування цілого кластера науково-дослідних організацій, що займаються питаннями розробки сучасних математичних моделей для дослідження критичної інфраструктури.

У Болгарії повені в літі 2005 року було саме спустошливе лихо, що спіткало країну. Загинули 31 людини. Тоді при хвилі в липні нанесені збитки на вартість 274 млн. доларів (205280800 Euro). Ще 200 млн. доларів (149840000 Euro) коштував другий потоп за цей рік в серпні. При ньому було і найбільша кількість людей, порушених лихом у країні. Постраждало більше 13 000 болгар, та задіяні – одним із способів були більше 60 тис. людей. Постраждала 70% території держави, потонуло 11 тис. сільськогосподарських тварин, а над 3 тис. будівель стали непридатними для перебування. В результаті цих кризових подій були нанесені збитки республіканської дорожньої мережі в розмірі 85829,5 тис. лв.(43883509 Euro), причому постраждали 4656,8 км. дорожньої мережі, 26751,0 кв. км. підпірних стін і 53 мостів. Нанесені збитки в муніципалітетах були в розмірі 156935,2 тис. лв. (80239398 euro), при цьому постраждали 1805,4 км. вуличної мережі, 1005,7 м. гребель, 13607,8 кв. м. підпірних стін , 726,1 км. дамб, 20,0 км. рейкових доріг міського транспорту. Внаслідок повеней у 2005 р. Рада міністрів розробила і затвердила два проекти законів - один для зміни та доповнення Закону про управління у разі криз, і інший - це новий Закон про захист при лихах.

Вивчення та аналіз критичної інфраструктури відносно молоде явище. Це питання стало привертати до себе пильну увагу тільки в кінці минулого століття. Саме події середини 90-х років (теракт в Оклахома-Сіті в 1995-му, публікація висновків доповіді наукового комітету МО США по інформаційній війні в 1996-му), а також тотальна комп'ютеризація систем управління і конт-

ролю різних секторів критичної інфраструктури суттєво підвищили значимість і необхідність таких досліджень.[4]

Так, в липні 1996 року адміністративним указом президента США № 13010 «Про роботу по дослідженню вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» була сформована комісія із захисту критичної інфраструктури при президенті США (President's Commission on Critical Infrastructure Protection - PCCIP). Перша доповідь комісії опублікована вже через рік. Незважаючи на те, що доповідь не визначала прямих загроз національній безпеці, в ній відзначалася важливість взаємозв'язку складових критичної інфраструктури, включаючи енергетику, транспорт, служби з надзвичайних ситуацій, банківський і фінансовий, телекомунікаційний сектори економіки та інші життєво важливі ресурси.

У травні 1998 року у світ вийшла директива президента № 63 «Стратегія спільних зусиль адміністрації США і приватного сектора в галузі захисту критичної інфраструктури». Вона визначала мету і завдання, які вирішуються для забезпечення захисту національної інфраструктури від навмисних атак, і супроводжувалася адміністративними указами президента № 13130 «Про Національну раду з критичної інфраструктури» та № 13231 «Про захист національних критичних інформаційних систем». У відповідності з цими документами почалося формування центрів інформаційного обміну та аналізу (Information Sharing and Analysis Centers), а також національної ради з критичної інфраструктури (National Infrastructure Advisory Council - NIAC). В кінці 2001 року був створений Національний центр аналізу та імітаційного моделювання інфраструктури (The National Infrastructure Simulation and Analysis Center - NISAC), а в листопаді 2002-го утворено Міністерство внутрішньої безпеки (МВБ), на яке і було покладено загальне керівництво заходами забезпечення захисту національної інфраструктури від різних загроз.

У Республіці Болгарія з 23 жовтня 2012 року вступило в силу Положення про порядок компетентних органів для встановлення критичних інфраструктур та їх об'єктів і для оцінки ризику для них. Положення має за мету досягнення більш ефективної превентивної діяльності в результаті своєчасного встановлення критичних інфраструктур та прилеглих до них об'єктів і відповідної оцінки ризику. Це призведе до зменшення їх вразливості від природних лих або умисних посягань. Положення відповідає вимогам для ідентифікації та позначення європейських критичних інфраструктур та оцінки необхідності у поліпшенні їх захисту. Всі заходи запроваджені Законом про захист при лихах. З точки зору європейського законодавства проблема порушена в Директиві 2008/114/ЕО Європейського парламенту і Ради від 8 грудня 2008 року щодо ідентифікації та позначення європейських критичних інфраструктур та оцінки необхідності у поліпшенні їх захисту. Директива є основним документом, поряд з так званою «Зеленою книгою Європейської програми на захист критичних інфраструктур» (ЗКІ), для ідентифікації і забезпечення Європейської кри-

тичної інфраструктури та оцінки необхідності в поліпшенні її захисту. У ній визначено основні поняття як «критична інфраструктура», «аналіз ризику», «захист», «чутлива інформація, пов'язана з ЗКІ» та ін. Директива охоплює в основному сектори енергетики та транспорту де планується її перегляд, включаючи у сфері її застосування і інші сектори. Додаткові вимоги вносить і директива Європейського парламенту та Ради Європи, що встановлює інфраструктурну просторову інформацію в спільності/INSPIRE/, яку, в якості держави - члена ЄС, Болгарія транспортує.

Недавні трагічні події в Росії – затоплення Кримську та в Комсомольскіна Амурі, ще раз засвідчило важливість підтримання в належному стані критичної інфраструктури, зокрема, гребель, дамб та інших гідротехнічних об'єктів. "Коли ми нехтуємо безпекою таких об'єктів критичної інфраструктури, - відповідь природи (стихії) не забариться" 17 липня 2012 р. застеріг всіх на засідання круглого столу "Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні" заступник директора Національного інституту стратегічних досліджень (НІСД) Олександр Литвиненко.

Підхід до забезпечення захищеності критичної інфраструктури, що враховує усі загрози (англ., all hazard approach), стає домінуючим в політиці безпеки окремих держав та міжнародних організацій, і це знайшло своє відображення, зокрема в 2012 році у комюніке Сеульського саміту з (фізичної) ядерної безпеки, в якому одним з пріоритетних напрямів діяльності держав-учасниць і міжнародних організацій в ядерній сфері визнано інтегрований підхід до технічної ядерної безпеки (англ. nuclear safety) та фізичної ядерної безпеки (nuclear security).

В якості порівняння, кроки виконані в Російський Федерації, де в 2004 році була створена Міжвідомча координаційна група з вирішення ключових проблем забезпечення захищеності населення країни та критично важливих для національної безпеки об'єктів інфраструктури, а згодом і перелік таких об'єктів, затверджена Концепція федеральної системи моніторингу критично важливих об'єктів і (або) потенційно небезпечних об'єктів інфраструктури (2005 р.) та Методичні рекомендації з розробки планів підвищення захищеності критично важливих об'єктів. Досвід міжнародних науково-дослідних інститутів, зокрема Інституту прикладного системного аналізу (Австрія), показує, що проблема захисту критичної інфраструктури формулюється як задача стратегічного управління безпекою.

В той же час, в Україні на сьогодні активізувалося питання тероризму. В цих умовах, зважаючи на значну кількість життєво важливих об'єктів (починаючи з 15 ядерних енергоблоків, дніпровського гідротехнічного комплексу, розвинутої хімічної промисловості) їхнє руйнування може призвести до катас-

трофічних наслідків. Крім того, зношеність основних фондів України перевищує 85%.[5] Тому проблема захисту критичної інфраструктури з кожним роком набуває все більшої ваги.

На теперішній час державна служба України з НС (раніше МНС України), як основний підрозділ по ліквідації наслідків надзвичайних наслідків на Україні, в своїй діяльності не виконує функції забезпечення безпеки об'єктів, а тільки забезпечує захист населення у випадку аварії. Однією з причин важкого становища в сфері техногенної безпеки в Україні є недосконаліть нормативно-правової бази, що регулює дану сферу. Навіть, в планах науково-дослідних робіт ДСУ НС, науково-дослідних та освітніх планах профільних інститутів словосполучення «критично важливі об'єкти» або «критична інфраструктура» поки що відсутні.

Критично важливі об'єкти можна розглядати з одного боку як такі, що вразливі до певних загроз, а з іншого - як такі, що необхідні для попередження та реагування на загрози безпеці держави, суспільства, населення. На сьогодні законодавча база, яка створювалася за умов реформування органів виконавчої влади та політичних дискусій, потребує вдосконалення. Визначення об'єктів, що є критичними для життєдіяльності країни, є справою держави. Саме держава повинна забезпечувати захист від загроз, пов'язаних із втратою критичної інфраструктури. В той же час, держава повинна стратегічно визначити роль та повноваження між органами влади та підприємцями, враховуючи обмеженість ресурсів та активніше використовувати ризик-орієнтований підхід при попередженні загроз критичній інфраструктурі.

У Болгарії під час встановлення критичних інфраструктур і прилеглих до них об'єктів, прикладають наступні критерії:

1. потенційна кількість постраждалих - оцінюється потенційна кількість загиблих і / або поранених;

2. потенційні економічні наслідки - оцінюється значимість економічних втрат та / або покращена якість продуктів або послуг, в тому числі можливі наслідки для навколишнього середовища;

3. потенційні суспільні наслідки - оцінюються наслідки для суспільної довіри, фізичного страждання і порушення щоденного життя, в тому числі і втрата основних послуг.

Список секторів з критичною інфраструктурою в Республіці Болгарія представлений в таблиці 1.

Міністр внутрішніх справ Болгарії створює і підтримує базу даних про критичні інфраструктур та їх об'єктів. Він здійснює і координацію діяльностей щодо встановлення критичних інфраструктур.[6]

Таблиця 1.

Список секторів з критичною інфраструктурою в Республіці Болгарія	
Сектор	Підсектор
I. Енергетика	1. Електроенергія
	2. Нафта
	3. Газ
	4. Теплова енергія
II. Транспорт	1. Автомобільний транспорт і дорожня інфраструктура
	2. Залізничний транспорт і залізнична інфраструктура
	3. Повітряний транспорт та аеропорту
	4. Водний транспорт та порту
III. Інформаційні та комунікаційні технології	1. Електронні з"єднуючі мережі
	2. Информаційна та комунікаційна інфраструктура
IV. Поштові та кур'єрські послуги	
V. Довкілля	1. Довкілля
	2. Води, водопостачання і каналізація
VI. Землеробство і харчові продукти	1. Землеробство
	2. Харчові продукти
	3. Ліси та мисливські господарства
VII. Охорона здоров'я	1. Медична та лікарняна допомога
	2. Лікарські засоби
VIII. Фінанси	
IX. Економіка	
X. Спортивні об'єкти і споруди	
XI. Освіта, наука і технології	
XII. Природні ресурси	
XIII. Туризм	
XIV. Регіональний розвиток та благоустрій	
XV. Оборона	1. Оборонна промисловість
	2. Військова інфраструктура та військові формування
XVI. Юстиція, громадський порядок і безпека	
XVII. Державне та соціальне управління	
XVIII. Захист при лихах	
XIX. Культурна спадщина	1. Нерухомі культурні цінності
	2. Рухомі культурні цінності

З 2011 навчального року методи аналізу ризиків вже викладаються в межах навчальних програм у провідних вищих навчальних закладах України різного спрямування. На жаль, статистика по Україні для застосування цих методів постійно поповнюється новими аваріями на мережах життєзабезпечення, в наслідок руйнівних сил природних лих (як то паводки в Закарпатті, заметілі по всій Україні в березні 2013 року), чи техногенних аварій (Світловодська ТЕС). Адже, запобігання загроз дозволяє значно зменшити можливі наслідки, тому важливим є інформаційне забезпечення, врахування взаємозв'язків між інфраструктурами та елементами всередині інфраструктур, здійснення моніторингу стану об'єктів. Необхідно створити в Україні оперативну інформаційну службу прогнозу, до завдань та компетенції якої буде належати оцінка ризиків критичних інфраструктур та здійснення реагування на загрози задля виживання нації.

Прийшов час переходу від старої радянської культури безпеки через нехтування проблемами безпеки, які були характерні для 90-тих років, до сучасної орієнтованої на захист людини, суспільства і держави культури безпеки. Україна належить до іншої економічної категорії ніж такі країни як ЄС, чи США, тому впроваджувати систему захисту критичної інфраструктури необхідно, зважаючи на можливості та фінансове забезпечення. В сучасних умовах цей напрямок уже став робочим дієвим механізмом забезпечення національної безпеки багатьох європейських держав. Забезпечення безпеки у світі розглядається як вигідна та високотехнологічна економічна діяльність, а інвестування в попередження загроз є менш витратним, ніж ліквідація наслідків можливих аварій.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях, в сила от 23.10.2012 г., приета с ПМС № 256 от 17.10.2012 г., Обн. ДВ. бр.81 от 23 Октомври 2012г., изм. и доп. ДВ. бр.19 от 26 Февруари 2013г.
2. Сучасні тенденції в дослідженні критичної інфраструктури в зарубіжних країнах. А. Кондратьєв, Ж. Закордонний військовий огляд № 1, 2012, С.19-30
3. WorldCom Inc., Verizon Communications Inc., the Hearst Corp. In New York City, Nexlel Communications Inc., і редакції газети The Baltimore Sun.
4. Fast Analysis Infrastructure Tool Department of Homeland Security's Information Analysis and Infrastructure Protection. National Infrastructure Simulation and Analysis Center (NISAC).
5. Матеріали круглого столу «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні», 17 липня 2012 року, м. Київ.
6. Карагьозов К., Размов Т., Варадинова Ю., Тодорова М., Джалева – Чонкова А. "Impact Of Natural Disasters On Transport Systems", ВТУ "Тодор Каблешков" 2012