УДК 354:340.133:340.134

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID:https://orcid.org/0000-0002-2488-7377.
ШОСТАК Р.М., *кандидат технічних наук,* старший науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

РОЗВИТОК МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ АНТИТЕРОРИСТИЧНОЇ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (НА ПРИКЛАДІ США)

Анотація. *Стаття присвячена аналізу проблем антитерористичної захищеності об'єктів критичної інфраструктури. Досліджуються проблемні питання методичного забезпечення цієї діяльності. Описані сучасні тенденції дослідження критичної інфраструктури в США. На базі аналізу позитивного американського досвіду запропоновані заходи з удосконалення методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури України.*

Ключові слова: *антитерористична захищеність, об'єкти критичної інфраструктури, методичне забезпечення, терористичні акти, методологія прогнозування.*

Summary. *The article is dedicated to the analysis of the problems of antiterrorist protection of the objects of critical infrastructure. The article provides research of the problematic questions of the methodical support of this activity. Recent trends in the research of critical infrastructure in the United States are described. On the basis of the analysis of positive American experience, measures are proposed to improve methodical support of the protection the objects of critical infrastructure of Ukraine.*

Keywords*: antiterrorist protection, objects of critical infrastructure, methodical support, terrorist acts, forecasting methodology.*

Аннотация*. Статья посвящена анализу проблем антитеррористической защищенности объектов критической инфраструктуры. Исследуются проблемные вопросы методического обеспечения этой деятельности. Описаны современные тенденции исследования критической инфраструктуры в США. На основании анализа позитивного американского опыта предложены меры по совершенствованию методического обеспечения антитеррористической защищенности объектов критической инфраструктуры Украины.*

Ключевые слова*: антитеррористическая защищенность, объекты критической инфраструктуры, методическое обеспечение, террористические акты, методология прогнозирования.*

Постановка проблеми. Проблематика захисту критичної інфраструктури пов'язана із бурхливим розвитком нових підходів до забезпечення національної безпеки в розвинених країнах світу, що зумовлено швидкими змінами, які відбуваються у безпековому середовищі у глобальному, регіональному та національному вимірах [1].

Відповідно до Стратегії національної безпеки України [2] серед основних напрямів державної політики в сфері національної безпеки виділяється забезпечення безпеки та необхідного рівня захищеності об'єктів критичної інфраструктури України, насамперед від загроз терористичного та диверсійного характеру.

Одним із завдань запобігання терористичній діяльності є підвищення ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, у тому числі шляхом розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів. Водночас, усунення та мінімізація наслідків терористичної діяльності передбачає вирішення завдань опрацювання комплексу заходів щодо забезпечення якнайшвидшого відновлення штатного режиму функціонування об'єктів, передусім об'єктів критичної інфраструктури, щодо яких вчинено терористичний акт (розд. IV Концепції боротьби з тероризмом) [3].

Результати аналізу наукових публікацій. Дослідженням проблемних питань захищеності об'єктів критичної інфраструктури займалися такі вітчизняні науковці, як Алексеєв О. [4], Антипенко В. [5], Кондратов С., Крутов В. [6], Кудінов С. [7], Рижов І. [8] та інші. Вагомий внесок у розроблення методів, засобів і технологій ідентифікації об'єктів критичної інфраструктури внесено дослідженнями, проведеними зарубіжними вченими. Це, зокрема, праці Дуденхофера Д., Педерсена П., Пермана М., Маніка М. [1], Дженкінса Р.та Хантера Р.

Незважаючи на те, що останнім часом з'явилася значна кількість публікацій, присвячених проблемам антитерористичної захищеності об'єктів критичної інфраструктури, залишається недостатньо дослідженим питання методології забезпечення антитерористичної захищеності таких об'єктів, на підставі якої впроваджується методологічний апарат для аналізу критичної інфраструктури та оцінки захищеності об'єктів критичної інфраструктури. Ця проблема набуває особливого значення в умовах зростання рівня терористичної загрози.

Мета статті полягає у проведенні аналізу досвіду антитерористичного забезпечення захисту об'єктів критичної інфраструктури США для удосконалення методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури України.

Виклад основного матеріалу. Дослідження критичної інфраструктури є надзвичайно актуальними в багатьох країнах світу, і, в першу чергу, в США у зв'язку з суттєвим підвищенням рівня терористичних загроз на початку XXI ст. Що стосується антитерористичного забезпечення захисту критичної інфраструктури, і визначення його напрямів в основних стратегічних документах у даній галузі, то попередньо доцільно охарактеризувати напрями антитерористичного забезпечення захисту критичної інфраструктури на прикладі США, оскільки ця країна має значний досвід розв'язання цієї проблеми.

Відповідно до директиви Президента США № 63 "Стратегія спільних зусиль адміністрації США і приватного сектору у сфері захисту критичної інфраструктури" головне завдання досліджень у цій сфері полягає у виявленні ключових об'єктів (або їх сукупності), вплив на які може спричинити найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці прогнозованих наслідків подібного впливу й розробці механізмів зниження таких ризиків [9].

Першим результатом цієї роботи було впровадження методики визначення пріоритетності об'єктів ключових фондів військово-промислової бази (The Asset Prioritization Model – APM) з використанням якої розроблена фахівцями міністерства

внутрішньої безпеки (МВБ) і міністерства оборони США модель загальної структури об'єкта. Методика регламентувала визначення індексу ризикованості об'єкта, що залежить від рейтингу об'єкта по шкалі категорії факторів і значимості даного фактора [10].

Згідно з чинним законодавством США, під критичною інфраструктурою розуміються: "системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище" [11].

Водночас, створення моделі саме критичної інфраструктури держави зумовило потребу визначення та врахування взаємного зв'язку вхідних у неї об'єктів, їх характеру та взаємозалежності.

Без вирішення цих питань, в тому числі обліку й аналізу мережевої складової кожного сектору критичної інфраструктури (економічного, фінансового, енергетичного і т.д.), вбачається проблематичним забезпечення достатньої адекватності моделі та об'єкту дослідження [10].

Для усунення виявлених недоліків у США розпочався етап формування цілого кластера науково-дослідних організацій, які займаються розробкою імітаційних математичних моделей для дослідження критичної інфраструктури. За результатами наукових досліджень у цій сфері були вироблені методичні підходи для аналізу критичної інфраструктури та з'ясовані особливості її функціонування.

На думку зарубіжних експертів [12; 13], критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об'єктів та параметрів системи; 2) важко прогнозована поведінка об'єктів, для яких характерна велика кількість взаємозв'язків, які класифіковано по різних секторах [14].

У роботі "Розкриття, розуміння й аналіз взаємозв'язків об'єктів критичної інфраструктури" [15] представлена класифікація взаємозв'язків між об'єктами критичної інфраструктури, зміст якої складають: фізичний, кібернетичний, географічний (топологічний), логічний.

У роботах інших зарубіжних дослідників [1] зустрічається більш уточнена класифікація взаємозв'язків за характером:

фізичний – визначає інженерну взаємозалежність між об'єктами;

інформаційний – залежність від інформаційного обміну (потоку інформації) між об'єктами;

геопросторовий – взаємозалежність виникає в результаті спільного розташування компонентів інфраструктури на місцевості. Наприклад, повінь або пожежа виводить з ладу всі розміщені на площі стихійного лиха об'єкти мережі;

процедурний (політичний) – подібна взаємозалежність виникає при будь-якій зміні (події) в одному з компонентів сектору інфраструктури й спричиняє вплив на об'єкти інших секторів;

соціальний – така взаємозалежність може виражатися через соціальні фактори: суспільна думка, суспільна довіра, страх тощо.

З наведеної класифікації випливає, що критична інфраструктура будь-якої держави є не що інше, як велика складна система стратегічного масштабу (ВССМ), що представляє собою сукупність значної кількості елементів різного типу, об'єднаних зв'язками різної природи, для яких характерна загальна властивість (призначення, функція), яка відмінна від властивостей окремих елементів усієї сукупності, що й вимагає розробки спеціальних методів дослідження [10].

Цілком очевидно, що структура критичної інфраструктури має містити величезну кількість різнотипних об'єктів та зв'язків між ними. Для оптимізації досліджень застосовуються методи групування об'єктів критичної інфраструктури відповідно до їх взаємозалежності за секторами різного рівня з урахуванням їх важливості, зміст якої відображений в Національній стратегії з фізичного захисту критичної інфраструктури та ключових об'єктів (The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets) 2003 року [16].

За результатами такої оцінки найвищий рівень захисту в ієрархії ключових об'єктів отримали об'єкти військово-промислового комплексу, системи охорони здоров'я та попередження надзвичайної ситуації. Наступне місце в ієрархії посідають об'єкти фінансового та транспортного сектору. І, нарешті, найнижчий рівень складають об'єкти інформаційно-телекомунікаційного та енергетичного сектору, а також сектору водозабезпечення. При цьому сектори вищого рівня взаємозалежать від секторів нижчого рівня. Зауважимо, що у США критичну інфраструктуру розглядають у більш широкому розумінні, включаючи до неї національні символи (пам'ятки культурної спадщини).

Слід зазначити, що складність повного врахування всіх взаємозв'язків і взаємозалежностей між об'єктами інфраструктури не дозволяла об'єктивно досліджувати критичну інфраструктуру [17].

Тому основні напрямки наукових досліджень критичної інфраструктури спрямовані на створення моделей, що точно імітують функціонування критичної інфраструктури, в тому числі під час реалізації загроз терористичного або диверсійного характеру. Таке моделювання дозволяє визначати взаємозв'язки між її об'єктами, за результатами якого виявляти найбільш уразливі з них. Таким чином, імітаційне моделювання як один з видів математичного моделювання стає реальним інструментом для аналізу й повноцінного дослідження критичної інфраструктури, що являє собою ВСССМ [18, с. 29].

Одним з найбільш яскравих прикладів сучасних імітаційних моделей є "Система моделювання критичних інфраструктур" (Critical Infrastructure Interdependency Modeling (CIMS), яка розроблена національною лабораторією Айдахо. Модель CIMS являє собою систему імітаційного моделювання, що поєднує дані геопросторової інформації та чотиривимірний (просторово-тимчасовий) ефект. Це дозволяє імітувати певні сценарії різних подій з відображенням каскадних ефектів [18, с. 29]. В залежності від обраних сценаріїв модель може відображати наслідки аварійних подій (імітаційне моделювання), наслідки вчинених терактів (ситуаційне моделювання), а також може слугувати інструментом для планування спеціальних операцій та диверсій (стратегічне моделювання).

Пошуком ключових об'єктів, вплив на які може визначити найбільш негативний ефект, дослідження критичної інфраструктури не обмежується. Це тільки перший крок, за результатами якого, як правило, проводиться оцінка уразливості розкритих "центрів ваги" за допомогою інженерного методу побудови дерева відмов, яке трансформується в дерево подій. Це дозволяє визначити можливі наслідки уразливості інфраструктури, а також їх варіації. Дерево відмов являє собою бінарне дерево з усіма можливими логічними подіями для кожної потенційної відмови. Саме дерево відмов і подій дозволяє сформулювати й розробити можливі заходи щодо захисту критично важливих і вразливих об'єктів інфраструктури. У випадку прогнозування наслідків аварійних подій, результатом формування дерева події є перелік уразливостей об'єктів, який

використовується для розрахунків ймовірності їх виникнення, а також формування гістограми ймовірності відмов [10].

На наступному етапі розроблюються алгоритми оцінки ризиків, зміст яких полягає у визначенні ресурсів, необхідних для забезпечення безпеки (впливу) найбільш важливих з виявлених об'єктів критичної інфраструктури. При цьому однією з головних умов залишається дотримання критерію "вартість – ефективність", а ключова проблема полягає в тому, щоб правильно вибрати способи й засоби для організації захисту таких об'єктів [10].

Таким чином, на сьогодні в США функціонує збалансована система забезпечення захисту критичної інфраструктури держави, зміст якої охоплює:

– визначений уповноважений орган (МВБ) для організації, координації та здійснення контрольно-наглядових функцій щодо заходів безпекового напряму;

– методичний апарат для аналізу та прогнозування наслідків як подій техногенного характеру, так і диверсій чи терористичних актів;

– систему науково-дослідних установ, які забезпечують науково-технічне супроводження функціонування системи аналізу стану критичної інфраструктури та експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури.

В Україні ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, в основу якої покладено методологічний підхід аналізу ризиків, які обумовлювалися надійністю функціонування елементів, складових, об'єктів тощо. Іншими словами, ризик виникнення надзвичайної ситуації визначався вірогідністю відмов природнього характеру, аварій, інших надзвичайних подій (ймовірність виникнення та розвитку подій внаслідок умисного пошкодження елементів не враховувався та не розглядався взагалі).

Проте, антитерористичне забезпечення передбачає інший підхід, в основу якого покладено оцінку можливих сценаріїв вчинення терористичних актів (та їх прогнозованих наслідків), спрямованих в найбільш уразливе місце об'єкта (що призводить до максимально можливих втрат з мінімальними витратами ресурсів), в найбільш незручний час з точки зору функціонування (виробничого циклу) об'єкта і стану його системи фізичного захисту. Оцінка можливих сценаріїв вчинення терористичних актів потребує, в свою чергу, отримання результатів розрахунку прогнозованих людських, економічних, екологічних, суспільно-політичних, культурних та інших втрат внаслідок події можливих впливів на об'єкт терористичного чи диверсійного характеру.

На наш погляд, створення системи антитерористичного забезпечення захисту критичної інфраструктури держави зумовлює:

– законодавче визначення повноважень Служби безпеки України з науково-технічного забезпечення процедур захисту об'єктів критичної інфраструктури (у т.ч. реалізації функцій з координації, здійснення контролю та нагляду, експертної оцінки, організації заходів компенсаційного та превентивного характеру тощо);

– створення в системі СБУ науково-дослідних установ, які будуть забезпечувати науково-технічне супроводження функціонування системи аналізу стану критичної інфраструктури та здійснювати експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури;

– розробку та впровадження необхідного методичного та нормативного забезпечення аналізу та прогнозування наслідків диверсії або терористичних актів.

Одним з важливих елементів цієї системи є створення та впровадження єдиного методичного апарату для проведення технічної та судової експертизи у даній галузі, який має враховувати взаємозв'язки різного рівня між елементами окремого об'єкта, об'єктів між собою, об'єкта та системи, а також різних систем.

Для вирішення цього завдання в Українському науково-дослідному інституті спеціальної техніки та судових експертиз СБУ впроваджено нові експертні спеціальності.

Зокрема, до основних завдань експертизи за спеціальністю 5.3 "Оцінка можливих наслідків застосування вибухового пристрою (вибуху)" належать:

– надання висновку щодо здатності досліджуваного вибухового пристрою (вибухової системи) до вибуху;

– надання оцінки щодо потужності вибуху, наслідків дії вибуху (у т.ч. параметрів вибухової хвилі, фугасної та бризантної дії, радіусу та ступеня осколкових уражень, термічної дії);

– оцінка ступеня ураження факторами вибуху існуючих (розташованих) в межах дії безпосередніх факторів вибуху об'єктів (в т.ч. будівель, споруд, машин, механізмів, транспортних засобів, обладнання тощо), а також людей та інших об'єктів, а за наявності, негативних наслідків іншого характеру;

– оцінка достатності існуючого рівня захищеності об'єктів дослідження до впливу безпосередніх факторів вибуху;

– у разі необхідності обґрунтування рекомендацій з підвищення рівня живучості (стійкості) об'єктів дослідження та систем в цілому;

– встановлення причинових зв'язків між існуючим станом захисту об'єктів дослідження та настанням наслідків в результаті впливу факторів прогнозованого вибуху;

– встановлення причинових зв'язків між діями (бездіяльністю) певних відповідальних осіб та настанням негативних наслідків в результаті застосування вибухових пристроїв (вибуху).

До основних завдань судової експертизи за спеціальністю 5.5 "Оцінка наслідків впливу технічних факторів диверсії (терористичного акту) іншої надзвичайної ситуації" належать:

визначення ступеня впливу на об'єкт дослідження (систему) технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації з оцінкою можливості їх подальшого функціонування;

надання прогнозу розвитку та наслідків каскадної аварії в результаті взаємозалежності суміжних систем об'єктів та впливу на них технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації;

визначення необхідних та достатніх вимог забезпечення функціонування об'єкта (системи в цілому) з урахуванням прогнозованого рівня загроз, а також відповідності існуючого стану захисту об'єктів вимогам діючих нормативних актів;

за потреби надання рекомендацій з підвищення рівня захисту об'єктів дослідження та систем в цілому;

встановлення причинових зв'язків між діями чи бездіяльністю певних відповідальних осіб та настанням негативних наслідків в результаті можливої реалізації диверсії чи терористичного акту.

Впровадження зазначених експертних спеціальностей спрямоване на всебічне експертне дослідження аспектів захисту об'єктів критичної інфраструктури, яке передбачає врахування взаємозв'язків різного рівня та різного характеру взаємозалежностей об'єктів та систем.

Для вирішення широкого кола різнопланових завдань з оцінки (прогнозування) наслідків системного характеру (диверсій, терористичних актів чи інших надзвичайних ситуацій) в рамках експертних спеціальностей 5.3 та 5.5 розробляється проект методики, який містить загальний методичний підхід, зміст якого передбачає системне врахування причинових зв'язків різного рівня та характеру.

Такий підхід базується на структуризації наслідків події різного характеру, а саме:

– наслідків І роду – наслідків безпосередньо фізичного впливу на об'єкт дослідження факторів диверсії або терористичного акту;

– наслідків ІІ роду – наслідки, що настають для інших пов'язаних елементів об'єкта в межах однієї системи, і є результатом опосередкованого впливу наслідків І роду на інший його елемент;

– наслідки ІІІ роду – наслідки, що настають для суміжних систем, що пов'язані зв'язками різного характеру (фізичні, інформаційні, геопросторові, процедурні (політичні), соціальні), і є результатом впливу наслідків І та ІІ роду.

Цей системний підхід може слугувати базисом для подальшого удосконалення методичного забезпечення експертних досліджень з оцінки (прогнозування) наслідків диверсії або терористичного акту та аналізу ступеня захисту об'єктів критичної інфраструктури.

Проблема запровадження системного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише понятійного та методологічного апарату. На перше місце висувається завдання створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди ключовим (вузловим) елементам критичної інфраструктури внаслідок дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа [19, с. 3].

Висновки.

На базі аналізу позитивного досвіду США у сфері антитерористичного захисту об'єктів критичної інфраструктури можна дійти висновку, що методичне забезпечення таких об'єктів в Україні потребує вдосконалення за напрямами:

– ідентифікації та градації об'єктів критичної інфраструктури;

– проведення аналізу ризиків та узагальнення вимог до рівнів захищеності (обґрунтування рівнів проектних загроз) об'єктів в залежності від вразливості об'єкта та масштабів його впливу на інші об'єкти та системи;

– аналізу та визначення найбільш ймовірних сценаріїв терористичних актів та диверсій на об'єктах критичної інфраструктури;

– розробки правил антитерористичної безпеки для об'єктів різного функціонального призначення;

– нормативної регламентації діяльності органів і підрозділів СБУ із захисту об'єктів критичної інфраструктури.

Використана література

1. Dudenhoeffer D.D., Permann M.R. and Manic M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. Submitted to Proceedings of the 2006. Conference: Proceedings of the Winter Simulation Conference WSC 2006, Monterey, California, USA, December 3-6. 2006. URL: https://www.researchgate.net/publication/221527820_CIMS_A_Framework_for_ Infrastructure_ Interdependency_Modeling_and_Analysis (дата звернення: 19.06.2020).

2. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287. *Офіційний вісник України*. 2015. № 43. Ст. 1353.

3. Концепція боротьби з тероризмом: Указ Президента України від 5.03.19 р. № 53. *Офіційний вісник України*. 2019. № 21. Ст. 710.

4. Алексеев О.Н. Противодействие терроризму в США: опыт и проблемы. *Теория и практика общественного развития.* 2012. № 7. С. 201-203. URL: https://cyberleninka.ru/article/n /protivodeystvie-terrorizmu-v-ssha-opyt-i-problemy (дата звернення: 19.06.2020).

5. Антипенко А.Ф. Міжнародна кримінологія: досвід дослідження тероризму : монографія. Одеса. Фенікс, 2011. 317 с.

6. Крутов В.В., Форноляк В.М. Система суб'єктів боротьби з тероризмом, їх адміністративно-правовий статус. *Інформаційна безпека людини, суспільства, держави*. 2019. Вип. 2. С. 56-64. URL: http://academy.ssu. gov.ua/ua/page/page_1581342762.htm (дата звернення: 19.06.2020).

7. Кудінов С.С. Міжнародний досвід протидії тероризму та його значення для України. *Вчені записки ТНУ імені В.І.Вернадського*. *Серія: юридичні науки*. 2019. № 1. Т. 30. С. 117-123.

8. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ. Нац. акад. СБУ, 2016. 327 с.

9. Executive Order. 13010. Critical Infrastructure Protection. *Federal Register*. Vol. 61, № 138. July 17. 1996. P. 3747-3750.

10. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах. *Зарубежное военное обозрение*. 2012. № 1. С. 19-30. URL: http://pentagon us.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranak h_2012/19-1-0-2082 (дата звернення: 19.06.2020).

11. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT). 2001. URL:http://frwebgate.access.gpo.gov (дата звернення: 19.06.2020)

12. Keating C, Rogers, R., Dryer D., Sousa-Poza A., Safford R., Peterson W., Rabadi G. System of Systems Engineering. *Engineering Management Journal*. 2003. Vol. 15. № 3.

13. Jackson, M. Systems Methodology for the Management Sciences. New York. Plenum, 1991. 298 p.

14. Congressional Research Service Report for Congress. Critical Infrastructures: Background, Policy and Implementation. 2002. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата звернення: 19.06.2020).

15. Rinaldi S., Peerenboom J. and T. Kelly. Idenlifying, Understanding and Analyzing Critical Infrastructure lnterdependencies. IEEE Control Systems Magazine, IEEE, December 2001. P. 11-25.

16. Ted G. Lewis Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Naval Postgraduate School Monterey. California. 2006.

17. Pederson P., Dudenhoeffer D. Hartley S., Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research., M. Permann, August 2006. URL: http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20 Modeling.pdf (дата звернення: 19.06.2020).

18. Mussington D. Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development. RAND: Science and Technology Institute, Santa Monica, CA. 2002.

19. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. 2012. 57 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~