УДК 343.3/.7

ОЦІНКА ТЕРОРИСТИЧНИХ РИЗИКІВ ЯК ОСНОВА ПЛАНУВАННЯ АНТИТЕРОРИСТИЧНОГО ЗАХИСТУ

Волошин О.В., аспірант
Національна академія Служби безпеки України

У статті розглянуто основні підходи до вибору методів оцінювання терористичних ризиків для побудови сучасних моделей антитерористичного захисту. Проаналізовано поняття терористичного ризику та його складових. Охарактеризовано теоретичні основи застосування методології оцінки ризиків для планування захисту об'єктів можливих терористичних посягань від терористичних загроз.

Ключові слова: *тероризм, боротьба з тероризмом, антитерористичний захист, терористичний ризик, оцінка терористичних ризиків.*

В статье рассмотрены основные подходы к выбору методов оценки террористических рисков для построения современных моделей антитеррористической защиты. Проанализировано понятие террористического риска и его составляющих. Охарактеризованы теоретические основы применения методологии оценки рисков для планирования защиты объектов возможных террористических посягательств от террористических угроз.

Ключевые слова: *терроризм, борьба с терроризмом, антитеррористическая защита, террористический риск, оценка террористических рисков.*

Voloshin O.V. TERRORIST RISK ASSESSMENT AS THE BASIS FOR PLANNING OF ANTITERRORIST PROTECTION

The article deals with the basic approaches to methods of terrorist risk assessment for creation of modern models of antiterrorist protection. The definition of terrorist risk and its components have been analyzed. The theoretical basis for the use of risk assessment methodology for planning the protection of objects of possible terrorist attacks from terrorist threats has been characterized.

Key words: *terrorism, fighting terrorism, antiterrorist protection, terrorist risk, terrorist risk assessment*

Постановка проблеми. Тероризм залишається одним із найнебезпечніших явищ у житті світового співтовариства. Теракти, що відбулися у світі упродовж останніх десятиліть, значною мірою продемонстрували уразливість громадянського суспільства до їх вражаючих факторів. Вибір ефективних методів боротьби з тероризмом та захисту населення від цієї загрози давно перестав бути засекреченою діяльністю спецслужб, а став предметом досліджень науковців різних спеціальностей. Подальше поширення терористичних ризиків і загроз зумовлює необхідність удосконалення існуючих та пошуку нових підходів до побудов сучасних моделей антитерористичного захисту, заснованих на застосуванні різноманітних методик оцінки ризиків (risk assessment), управління ризиками (risk management).

Початок застосування європейським співтовариством підходу «антикризового управління» (crisis management) у боротьбі з тероризмом, який являє собою складову частину більше широкого підходу «всіх небезпек» (all hazard) та все більш активно використовується в ЄС для розгляду загроз безпеці, пов'язується з прийняттям у грудні 2005 року нової Контртерористичної стратегії ЄС під назвою «Запобігати, Захищати, Руйнувати, Відповідати» (Prevent, Protect, Disrupt, Respond). Стратегія відображає усвідомлення того, що репресивні заходи щодо боротьби з тероризмом необхідно поєднувати з превентивними [1, с. 90].

Ефективні методології оцінки ризиків є основою програм захисту об'єктів критичної інфраструктури зарубіжних країн від широкого спектра природних та техногенних загроз, у тому числі терористичного характеру. Вони необхідні для ідентифікації загроз, оцінки уразливості об'єктів захисту від їх впливу, беручи до уваги ймовірність реалізації загроз. Це ключове положення відрізняє методики оцінювання ризиків від звичайних методик оцінки впливів.

Попри значну кількість джерел невизначеності навколо визначення терористичних ризиків, їх оцінювання необхідне для правильного розподілу (перерозподілу) внутрішніх безпекових ресурсів. Колишній секретар Департаменту внутрішньої безпеки США Мічел Чертофф (2006) справедливо відзначав: «Ми повинні ідентифікувати та визначити за пріоритетами ризики – розуміючи загрозу, вразливість та наслідки. І тоді ми повинні розподіляти наші ресурси економічно ефективним способом» [2, с. 575].

Аналіз останніх досліджень. Вивченню теоретичних та методологічних аспектів застосування методології оцінки ризиків для боротьби з тероризмом присвячена значна кількість праць закордонних учених. Заслуговують на увагу публікації таких дослідників: Г.Г. Вілліс, А.Р. Моррал, Т.К. Келли, Дж.Дж. Медбай, Б.Ч. Езел, С.П. Беннет, Д.В. Вінтерфілд, Дж. Соколовски, А.Дж. Коллинс, Г. Гианнопоулс, Р. Філіппіні, М. Шиммер, К. Роббертс, Дж. Хорган, Г.Г. Браун, Л.А. Кокс та ін.

Українськими авторами ґрунтовний аналіз методології оцінки ризиків здійснено переважно у контексті безпеки функціонування екологічних та соціальних систем, промислових виробництв, об'єктів критичної інфраструктури, запобігання виникнення над-

звичайних ситуацій. У цьому зв'язку варто виділити роботи А.Б. Качинського, Г.А. Хміля, Д.Г. Бобра, М.З. Згуровського, В.В. Кривошеїна, Ю.П. Стародуба, А.П. Гаврися, Я.І. Федюка, Г.М. Коломійця, Л.Г. Руденко, О.Л. Дронової та багатьох інших.

З урахуванням тривалого проведення антитерористичної операції на сході України, можливості поширення тероризму на інші регіони та необхідності протидії загрозам терористичного характеру, обґрунтування методів оцінювання терористичних ризиків для побудови моделей антитерористичного захисту об'єктів можливих терористичних посягань (насамперед критичної інфраструктури) потребує додаткового дослідження.

Метою публікації є розгляд підходів до вибору методів оцінювання терористичних ризиків як підґрунтя для подальшого планування антитерористичного захисту об'єктів можливих терористичних посягань від терористичних загроз.

Виклад основного матеріалу. Сутність оцінювання терористичних ризиків необхідно розпочинати власне з терміну «ризик», відносно якого, як справедливо відмічає А.Б. Качинський, існує значна невизначеність [3, с. 318]. Різними авторами та засобами масової інформації терміни «ризик» (risk), «небезпека» (hazard), «загроза» (threat) та «невизначеність» (uncertainty) часто вживаються як синоніми. У науковій літературі наводиться 18 визначень терміну «ризик» [3, с. 320-327], у чинному законодавстві України – близько 30-ти [4, с. 52]. У більшості науково-технічних публікацій із даної тематики ризиком є кількісна міра небезпеки, що дорівнює добутку ймовірності реалізації певної загрози, помноженій на ймовірність величини можливого збитку від неї [3, с. 319].

У контексті протидії тероризму заслуговує на увагу визначення терористичного ризику та методологія його оцінювання, запропонована Центром політики управління терористичними ризиками (CTRMP) корпорації RAND (США) [5]. Терористичний ризик розглядається як сукупність трьох компонент: 1) загроза цілі (threat); 2) уразливість цілі до загрози (vulnerability); 3) наслідки можливої успішної реалізації терористичної загрози (consequences). Іншими словами, терористичний ризик являє собою очікувані наслідки атаки, враховуючи вірогідність того, що атаки відбудуться і будуть успішними для терористів. У термінах теорії ймовірності ризик атаки певного типу це безумовне математичне очікування збитків певного виду.

Не вдаючись до детального розгляду недоліків ймовірнісно-статистичного методу розрахунку терористичних ризиків та порівняння його з іншими методами (теоретико-ймовірнісними, евристичними), відзначимо лише, що таке формулювання терористичного ризику має дві переваги. По-перше, воно забезпечує підхід до порівняння ризиків та їх складання (об'єднання). По-друге, дозволяє встановлювати чіткі зв'язки між оцінкою ризиків (risk assessment), подальшим управлінням ризиками (risk management) та зниженням ризиків (risk reduction).

Для обґрунтування методів розрахунку терористичних ризиків необхідно враховувати те, що ймовірнісно-статистичні методи мають деякі недоліки та створюють суттєву невизначеність в оцінці ризику, найбільший внесок в яку дає етап оцінки терористичної загрози. Якщо для оцінки наслідків терористичних актів можуть бути використані вже розроблені моделі та розрахунки для природних та техногенних надзвичайних ситуацій, то для оцінки загроз це зробити неможливо, адже вона базується на інформації про цілі, мотиви та можливості терористів. І якщо можливості та тактика дій терористів ще можуть бути більш-менш адекватно передбачені, то оцінити об'єкт, який стане ціллю, можна дуже приблизно.

На думку автора, статистичні методи для розрахунку терористичних ризиків є не зовсім придатними, оскільки для них необхідний великий обсяг статистичної інформації, яку не завжди можна отримати у контексті скоєння терористичних актів стосовно конкретного об'єкта. Зокрема, обсяг спостережень повинен перевищувати деяку величину № 1, яка залежить від ймовірності, що оцінюється, при цьому число реалізованих негативних подій за один рік повинно бути більше ніж 100 [6, с. 141]. До того ж, як відзначають Г.Г. Браун та Л.А. Кокс, традиційний ймовірнісний аналіз ризиків (probabilistic risk assessment), призначений для розрахунку ризиків природних та інженерних систем, містить суттєві відмінності від аналізу терористичних ризиків. Основні з них полягають у тому, що терористи можуть бути обізнані про посилення антитерористичних заходів правоохоронними органами і проводити власні дослідження ризиків перед проведенням атак. У той же час, правоохоронці оцінюють терористичні загрози виходячи з інформації, відомої про терористів. При цьому, правоохоронним органам достеменно не відомо про обсяг інформації, яку терористи можуть знати про особливості функціонування систем антитерористичного захисту і яка може вплинути на прийняття ними рішень стосовно майбутніх атак. Такі застереження не можуть бути застосовані для інженерних систем та стихійних лих [7].

Ураховуючи викладене, для розрахунку терористичних ризиків більш придатними вважаються евристичні методи, до яких належить метод експертного оцінювання, що заснований на використанні суб'єктивних ймовірностей, отриманих під час експертного оцінювання, та дозволяє провести якісно-кількісне ранжування ризиків [6, с. 140]. Сутність експертного методу оцінки показників ризику полягає у тому, що експертам пропонують відповісти на питання про стан або майбутню поведінку об'єктів, що характеризуються невизначеними параметрами або недослідженими властивостями. Експертні оцінки оформляють у вигляді якісних характеристик або кількісних значень ймовірностей подій, що розглядаються, віднесених до певного відрізка часу. Важливе значення при цьому надають формуванню оцінювальної шкали, яка використовується експертами. Оптимальна оціночна шкала повинна

мати порівняно невелике число градацій (від 3 до 8); кожній градації приписують певний ймовірнісний інтервал. Крім того, кожна градація повинна супроводжуватися короткою текстовою якісною характеристикою. Для інтерпретації та математичної обробки експертних даних можна залучати математичні моделі. Підвищення вірогідності експертних оцінок вимагає відповідних процедур відбору експертів за багатьма критеріями і кількісних методів обробки їх думок. За умов правильної організації процедури експертизи та перевірки узгодженості думок експертів забезпечується достатня достовірність оцінок [6, с. 164-165].

Для обробки суджень експертів під час розрахунку терористичного ризику доцільно використовувати метод аналітичних мереж (МАМ) та його спрощений варіант – метод аналізу ієрархій (МАІ), які докладно описані у працях американського математика Томаса Сааті на початку 70-х років XX століття [8; 9] та придатні для використання у процесі експертного оцінювання. Зауважимо, що МАМ та МАІ допомагають структурувати проблему (у тому числі ту, що погано формалізується), побудувати набір альтернатив, виділити фактори, які характеризують ці альтернативи, задати значущість самих факторів, оцінити альтернативи по кожному з факторів, знайти неточності та суперечності у судженнях експертів, проранжувати альтернативи, провести аналіз рішення та обґрунтувати отримані результати [10, с. 7]. Методи засновані на декомпозиції задачі і представлення її у вигляді аналітичних мереж (ієрархічних структур), що дозволяє використати всі наявні в експертів, які залучаються до дослідження, знання з розв'язуваної проблеми та подальшій обробці їх суджень. У результаті може бути виявлен відносний ступінь взаємодії елементів в ієрархії, які потім виражаються чисельно. МАМ (МАІ) включають процедури синтезу множинних суджень, отримання пріоритетності критеріїв і знаходження альтернативних рішень.

На першому етапі застосування МАМ (МАІ) проводиться структурування проблеми вибору у вигляді ієрархії або мережі. У найбільш загальному вигляді ієрархія будується з вершини (мети), через проміжні рівні – критерії (параметри) до самого нижнього рівню, який, як правило, є набором альтернатив. Логіка вказаного алгоритму дозволяє формулювати питання до експертів, які нададуть можливість визначити категорію об'єктів, зокрема: від кого необхідно захищати об'єкт, яка ймовірність нападу на нього, які види протиправних дій він може вчиняти, яка уразливість об'єкта щодо кожного виду нападу, які суспільно небезпечні наслідки можуть виникнути внаслідок кожного виду нападу, до якої категорії за рівнем терористичного ризику необхідно віднести об'єкт. Завдання експертів на кожному рівні ієрархії провести попарні порівняння елементів ієрархії за критерієм, встановленим на вищому рівні ієрархії. Для підвищення достовірності суджень експертів в оцінці ймовірностей атак з боку конкретної терористичної організації, групи чи особи щодо ОТП доцільно використати метод «чек-листів» (checklist method) зі зваженими коефіцієнтами. Чек-лист уявляє собою список контрольних пунктів, виконання яких необхідне для успішного завершення всього обсягу роботи або процедури [11]. Для нашої задачі чек-лист повинен включати список питань (критеріїв), які експерт має прийняти до уваги для оцінки та подальшого порівняння ймовірностей терористичних загроз. До цього списку, зокрема, доцільно включити питання, які можуть свідчити як на користь збільшення ймовірності терористичної діяльності, так і у напрямку її зменшення, для чого можна запозичити досвід Департаменту оборони США в оцінці терористичних загроз [12].

Перед переходом до наступного етапу – встановлення пріоритетів суспільно небезпечних наслідків – необхідно оцінити уразливість об'єкта до кожного з прогнозних сценаріїв ППД. Аналіз уразливості використовується для визначення чутливості об'єктів до атак від загрози, виявленої на етапі аналізу загроз. Аналіз уразливості повинен відповісти на питання «до якого виду атак об'єкт є найбільш/найменш уразливим?». Уразливість притаманна кожному об'єкту, на який направлена терористична загроза. Уразливість існує завжди, незалежно від політик, процедур, структури та захисного обладнання. Враховуючи те, що терористичні загрози досить важко контролювати, вони піддаються оцінці і вразливість об'єкта до цих загроз може бути знижена. Ідентифікація і розуміння уразливості є важливим для визначення достатності захисту об'єктів від потенційних втрат. З урахуванням того, що уразливість є компонентом терористичного ризику, потенційний терористичний ризик для об'єкта можна знизити шляхом зниження уразливості.

Для методології оцінки уразливості важливим етапом є визначення критеріїв, за допомогою яких можливо проводити відповідну оцінку. Як приклад, Департамент оборони США розробив декілька інструментів для допомоги у проведенні оцінки уразливості, найбільш відомими з яких є методи MSHARPP (Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity) та CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability), які використовують різні критерії оцінки [12].

Зокрема, назва методу MSHARPP є акронімом, яка складається з назв критеріїв уразливості, таких як функціональність (mission), символізм (symbolism), доступність (accessibility), розпізнаваність (recognizability), людський фактор (population) та близькість (proximity).

Назва CARVER відбиває у собі такі критерії як критичність (criticality), доступність (accessibility), відновлюваність (recuperability), уразливість (vulnerability), вплив на населення (effect on the population), розпізнаваність (recognizability).

Для оцінювання рівня суспільно небезпечних наслідків необхідно визначити можливі види цих наслідків, спричинених терористичними атаками. Загальноприйняті в ЄС процедури виявлення і встановлення європейських критичних інфраструктур ("ECIs") і проведення оцінки необхідності посилення

їхнього захисту, формування критеріїв значущості об'єктів, зокрема, у контексті наслідків можливих терористичних посягань, є комплексними та мають враховувати [13]:

a) критерій за кількістю жертв (оцінка проводиться з урахуванням кількості потенційних загиблих або поранених);

b) критерій, пов'язаний з економічними наслідками (оцінка проводиться з точки зору значущості економічних втрат та/або ступеня погіршення якості продуктів або послуг, включає можливі наслідки для навколишнього середовища);

c) критерій впливу на населення (оцінка проводиться з точки зору впливу на суспільну довіру, фізичних страждань і порушення у повсякденному житті, включаючи втрату можливості надання важливих послуг).

Як справедливо відмічає І.М. Рижов, такий підхід є оптимальним для оцінки диверсійно-терористичних впливів, якщо мова йде лише про загрозу впливу на об'єкт та оточуюче його середовище, враховуючи й соціальне. Але не йдеться про впливи на соціально-політичні алгоритми управління у суспільстві, зміна або примусова корекція яких, власне, і є головною метою терористичної діяльності [14, с. 273]. Тому однією зі складових можливих наслідків терористичного акту є соціально-політична реакція суспільства на небезпеку внаслідок сукупного впливу на даний об'єкт вражаючих факторів терористичних загроз.

Висновки. Отже, під терористичним ризиком пропонується розуміти багатокритеріальну (векторну) величину, яка характеризує ймовірність настання певних видів суспільно небезпечних наслідків (людські втрати, матеріальні збитки, екологічні, культурні та суспільно-політичні наслідки) у разі ймовірної реалізації терористичної загрози. Розглянута методологія визначення терористичного ризику, яка поєднує методи експертного оцінювання, аналітичних мереж, аналізу ієрархій, чек-листів зі зваженими коефіцієнтами, містить ряд переваг, а саме: створюється можливість отримання якісно-кількісних характеристик компонентів терористичного ризику – загрози, уразливості та наслідків; визначені ймовірності складових терористичного ризику надають змогу застосовувати методологію управління ризиками (risk management); поруч з кількісними оцінками компонент терористичного ризику стає доступною їх якісна оцінка (яка терористична організація, група та особа становить найбільшу загрозу для об'єкта терористичних посягань, ризик якого виду суспільно небезпечних наслідків є найвищим тощо); з'ясування величини терористичного ризику та його компонент є визначальною умовою для планування антитерористичного захисту, метою якого має стати розроблення антитерористичних заходів, спрямованих на зниження ймовірнісних значень структурних компонент терористичного ризику.

ЛІТЕРАТУРА:

1. Rhinard M. The European Union and Terrorism [Text] / M. Rhinard, A. Boin, M. Ekengren ; ed. by D. Spence. – London : John Harper Publishing, 2007. – 265 p.

2. Probabilistic Risk Analysis and Terrorism Risk [Electronic resource] / B. C. Ezell, S. P. Bennett et al. // Risk Analysis. – 2010. – Vol. 30. – № 4. – P. 575–589. – Mode of access : https://docviewer.yandex.ua/?url=https%3A%2F%2Fwww.dhs.gov%2Fxlibrary%2Fassets%2Frma-risk-assessment-technical-publication.pdf&name=rma-risk-assessment-technical-publication.pdf&lang=en&c=5877677eef51.

3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський. – К. : Інст. пробл. нац. без., Нац. акад. Служби безпеки України, 2004. – 472 с.

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

5. Estimating terrorist risk [Електронний ресурс]. – Режим доступу : https://docviewer.yandex.ua/?url=http%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fmonographs%2F2005%2FRAND_MG388.pdf&name=RAND_MG388.pdf&lang=en&c=58769bd5be36.

6. Вишняков Я.Д. Общая теория рисков : [учеб. пособие для студ. высш. учеб. заведений] / Я.Д. Вишняков, Н.Н. Радаев. – 2-е изд., испр. – М. : Академия, 2008. – 368 с.

7. Brown G.G. How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts / G.G. Brown, L.A. Cox // Risk Analysis. – 2011. – Vol. 31. – № 2. – P. 196 – 204. [Electronic resource] – Mode of access : http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2010.01492.x/full.

8. Саати Т.Л. Принятие решений при зависимостях и обратных связях: аналитические сети / Т.Л. Саати ; пер. с англ. О.Н. Андрейчикова ; науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. – М. : ЛКИ, 2008. – 357 с.

9. Саати Т.Л. Аналитическое планирование: организация систем / Т.Л. Саати, К.П. Кернс ; пер. с англ. Р.Г. Вачнадзе ; под ред. И.А. Ушакова. – М. : Радио и связь, 1991. – 224 с.

10. Бочков А.В. Использование метода анализа иерархий для целей категорирования критически важных объектов по степени совокупного ущерба и риску противоправных действий / А.В. Бочков // Проблемы анализа риска. – 2008. – Том № 5. – № 4 – С. 23 – 27.

11. Checklist method [Electronic resource]. – Mode of access : https://www.slideshare.net/mobile/bibinssb/checklist-method.

12. DoD Antiterrorism handbook [Electronic resource]. – Mode of access : https://docviewer.yandex.ua/?url=http%3A%2F%2Fdownload.cabledrum.net%2Fwikileaks_archive%2Ffile%2Fus-dod-anti-terrorism-handbook-2004.pdf&name=us-dod-anti-terrorism-handbook-2004.pdf&lang=en&c=588f8d80b6d1.

13. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/search.html?lang=en&text=Council+directive+-No.+2008%2F114%2FEC+On+the+identification+and+designation+of+european+critical+infrastructures+and+the+assessment+of+the+need+to+improve+their+protection&qid=1480852873267&type=quick&scope=EURLEX&DD_YEAR=2008.

14. Рижов І.М. Базові концепти антитерористичної безпеки : [монографія] / І.М. Рижов ; Нац. акад. Служби безпеки України. – Київ : Нац. акад. СБУ, 2016. – 327 с.