

ПРОБЛЕМИ РАДІАЦІЙНОЇ БЕЗПЕКИ

УДК 539.1.08

Ю.Л. ЗАБУЛОНОВ, Г.В. ЛИСИЧЕНКО, В.М. БУРТНЯК, Ю.О. МЄДВЄДЄВ

Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України», м. Київ

МЕТОДИ ОЦІНЮВАННЯ ТЕРОРИСТИЧНИХ РИЗИКІВ

В статті розглядаються сучасні підходи до оцінювання ризиків тероризму. Описані складності оцінки ризиків тероризму та пов'язані з цим невизначеності. Розкрита потреба в надійній методології оцінювання ризиків.

Вступ

Науково-технічний прогрес останніх десятиріч та доступність інформації щодо новітніх науково-технічних досягнень, поряд з позитивними результатами, призвели до появи нових загроз для суспільства. Однією з найбільш непередбачуваних і незворотніх за своїми наслідками загроз є технологічний тероризм. За останні десятиріччя це явище зазнало значних змін як у своїй організації, масштабах, ідеології, цілях, так і у формах прояву. Значно збільшилась кількість терористичних актів, а також кількість країн, які тим чи іншим шляхом постраждали від терористичної діяльності. На початку 70-х кількість цих країн становила близько 50-ти, а до 2000-го року ця кількість зросла майже вдвічі[1]. Важливою рисою сучасного тероризму є його транснаціональний та міжнародний характер. Всі великі терористичні організації мають добре організовану систему керівництва, розгалужену мережу підрозділів, опорних пунктів і баз по всьому світу.

Значно зросли цілі терористів і масштабність наслідків реалізованих терористичних актів. Якщо в XIX ст. метою терористичного акту було вбивство конкретної людини, з застосуванням примітивних засобів, то в наш час, як продемонстрували події 11.10.2001, терористи прагнуть до реалізації терористичних актів, результатом яких була б загибель сотень або навіть тисяч людей. Такі прагнення терористів ясно окреслюють той факт, що для досягнення цих цілей їм буде необхідна високотехнологічна зброя масового знищення. Серед усіх технічних засобів для масового знищення, найбільш привабливою для терористів і найбільш небезпечною для населення є ядерна зброя. Ядерною зброєю називається сукупність ядерних боєприпасів, засобів їх управління та доставки. Даний тип зброї, при його застосуванні, перевищує всі інші як за кількістю людських жертв, так і за руйнівною силою вражаючих факторів, впливом на навколишнє середовище. Оскільки, на щастя, отримання або виготовлення ядерної зброї є надзвичайно важким завданням для терористів, то в якості її можливої альтернативи може бути застосована радіологічна зброя, яка являє собою контейнер з радіоактивними речовинами та вибуховий пристрій, при спрацьовуванні якого радіоактивні речовини розповсюджуються на значну відстань. Виходячи з вищезазначеного, під терміном “ядерно-радіаційний тероризм” будемо розуміти наміри, спроби, реалізацію людиною, або групою людей викрадення ядерних матеріалів або зброї, чи радіоактивних матеріалів, та їх застосування або погрозу застосування, а також різноманітні диверсії на ядерних об'єктах для досягнення своїх політичних, соціальних або інших цілей.

Негативним фактором, вигідним для терористів, є те, що загроза ядерно-радіаційного тероризму в перспективі таких держав як Україна мало ким сприймається серйозно.

Хоча даний вид тероризму, на щастя, поки є гіпотетичним, можливість, бажання і ймовірність його реалізації певними терористичними групами є вірогідною. Через це стає актуальною необхідність розробки методики, яка дала б змогу оцінити ризик терористичного акту, завдяки чому зможуть бути проведені запобіжні заходи для попередження або нейтралізації спроб застосування ядерної або радіологічної зброї, та її розкрадання.

Методи аналізу ризику тероризму

Дослідження на цю тему, переважно закордонних спеціалістів, показали, що ризик ядерного тероризму є надто важким для оцінювання. Основною відмінністю оцінювання ризику тероризму від оцінювання ризику, наприклад, техногенних катастроф або природних катаклізмів, є те, що в даному випадку ми маємо справу з людським фактором, який передбачає планування цілеспрямованої акції, її проведення та адаптацію. Через це, будь яка ймовірнісна модель не дасть повного уявлення про ризик, завдяки їй можна лише зробити припущення щодо ключових факторів, які впливають на цей ризик, та оцінити ефективність заходів для його зменшення.

Підходи для оцінювання ризику тероризму включають різні методики аналізу ризиків, такі як метод аналізу ієрархій, нечіткі множини, експертні оцінки, теорія ігор, методи ймовірнісного аналізу безпеки та ін., які можна поділити на кількісні та якісні. Вибір підходу залежить, звичайно, від цілей дослідження.

Результатом застосування кількісних підходів є чіткі значення, як, наприклад, ймовірності, частоти ймовірнісних розподілів та ін., засновані на моделях, що описують різні події, пов'язані з діяльністю терористів. Якщо ціллю дослідження є визначення ймовірності того, що різні типи терористичних атак будуть успішними, та визначення їх наслідків, то найбільш відповідними для моделювання ризику будуть методи, засновані на ймовірнісному аналізі безпеки. Зазвичай розглядається певна інфраструктура, наприклад об'єкт ядерної енергетики, та його найкритичніші, з точки зору безпеки характеристики та елементи, наприклад: місцерозташування, кількість ядерного матеріалу, рівень охорони об'єкту та ін. Повний ризик терористичного нападу звичайно обчислюється за допомогою наступного виразу:

$$R = P(A) \times P(S | A) \times C;$$

де R - ризик тероризму, $P(A)$ - ймовірність нападу, $P(S|A)$ -вразливість(ймовірність успішності нападу, за умови, що він відбувається), та C - очікувані наслідки.

Незалежно від підходу, що застосовується, ймовірність $P(A)$ є найбільш складною для оцінювання. У спрощеному вигляді вона може бути представлена як:

$$P(A) = f(q_i), i = 1, 2, \dots, n;$$

де $f(q_i)$ - спрощене представлення дій терористів, побудоване з ймовірнісних оцінок різних подій, або розподілів випадкових величин, $q_i, i = 1, 2, \dots, n$.

За допомогою такого підходу, можна отримати ймовірність, наприклад того, що певна група зробить спробу крадіжки ядерних матеріалів на певному об'єкті.

Суттєвим недоліком такого підходу є слабкість емпіричних доказів, та майже повна відсутність відповідних результатів спостережень[11]. Для призначення відповідних ймовірностей подіям, спеціалісти мають розглянути величезну кількість однакових систем, і/або обчислити кількість специфічних подій, які відбулися, або реалізацій включених змінних.

Крім того, як вказано у роботі [4], необхідно враховувати, що терористи можуть дізнатися про розраховані ймовірності атаки того чи іншого об'єкта, і, відповідно, змінити свої пріоритети при виборі цілі.

Те саме можна сказати і про оцінювання ймовірнісних розподілів і очікувань випадкових величин, як, наприклад, кількість терористичних атак, або рівень загрози терористичної атаки. Також основна модель може складатися з причинно-наслідкових моделей і/або моделей впливу, в яких використовуються психологічні, психологічно-соціальні та культурні фактори. Але складність виконання таких обчислень зростає пропорційно задіяним ресурсам.

Оскільки ймовірність таких складних подій як терористичний акт є важкою для безпосереднього оцінювання, часто вона розкладається та аналізується по частинах, і лише потім обчислюється повна ймовірність. Для розкладу складних подій використовуються різні методи, які включають логічні дерева (дерева подій, дерева відмов, дерева рішень та ін.), діаграми впливу, Баєсовські мережі довіри та ін. Найпоширенішим є використання логічних дерев, за допомогою яких проводиться аналіз невизначених подій та визначення сценаріїв. Аналіз логічного дерева складається з визначення послідовності оцінок, і подальшого дослідження невизначеностей в кожній з цих оцінок. Наприклад, дерева подій представляють собою послідовність вершин з відгалуженнями, які індуктивно моделюють послідовності подій, що призводять до певних наслідків. Вони є корисним засобом у випадку, коли необхідно розділити великий всесвіт подій в структурований набір, і провести базову оцінку ризику тероризму, розглядаючи весь шлях від вибору зброї і цілі, до нападу і можливих наслідків. На Рис.1. наведене дерево подій, представлене у роботі [10], в якому змальовується шлях терористичної групи від придбання ядерного матеріалу до його доставки і вибуху.

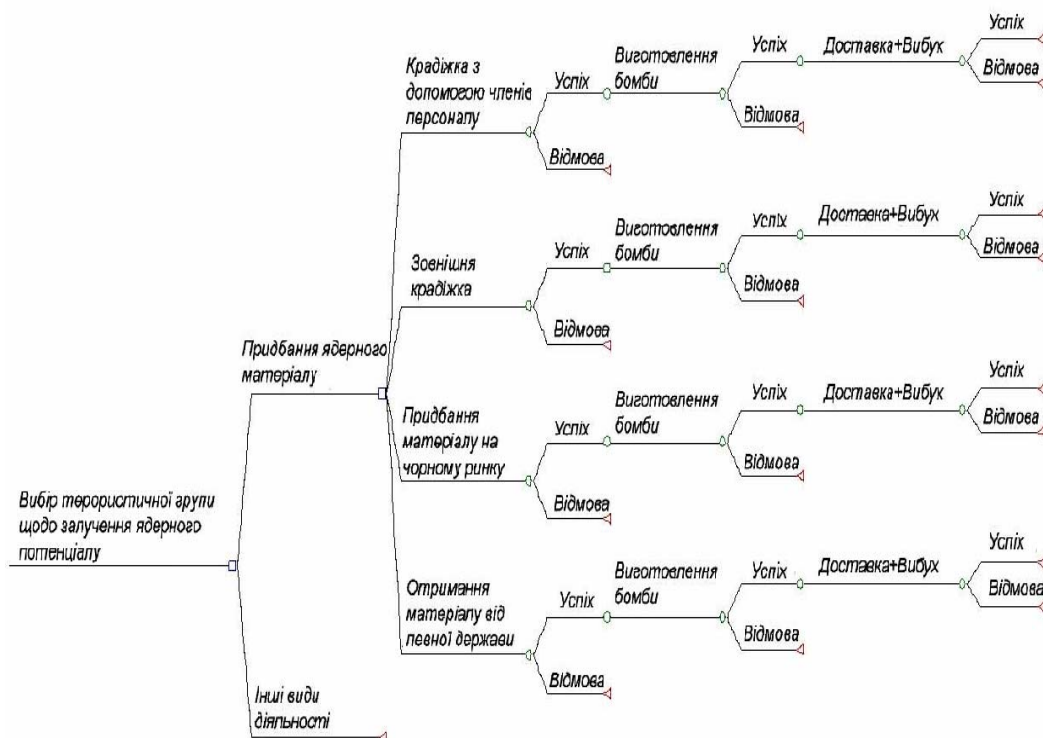


Рис.1. Дерево подій

До обмежень даного методу можна віднести те, що судження щодо розподілів ймовірностей є суб'єктивними, часто через обмеженість числових даних, а також вищезазначений факт, що вибір терористів не є випадковою подією, а залежить від поточної ситуації. Тому логічні дерева є лише статичним “знімком” загрози, вразливості і наслідків для конкретного періоду часу.

Якщо ціль дослідження полягає в обґрунтуванні прийняття терористами рішень, чи вибору тої чи іншої цілі для атаки, то найдоцільнішим є використання методів теорії ігор, згідно з якою проблема уявляється як стратегічна гра, в якій нападник намагається максимізувати, а захисник намагається мінімізувати наслідки нападу.

В якості прикладу такого підходу може слугувати стаття [9].

Автори даної роботи наводять наступну модель:

- є ряд цілей (проіндексованих літерою i , пронумерованих від 1 до N), кожна з яких має цінність V_i ;
- нападник, з повними ресурсами A_T , повинен вибрати ціль і кількість призначеного їй ресурсу A_i .
- захисник, з повними ресурсами D_T , має вирішити, як розподілити ресурси D_i серед цілей.
- повне знищення цілі i відбувається з ймовірністю, заданою функцією $p(V_i, A_i, D_i)$.
- нападник хоче максимізувати і захисник хоче мінімізувати очікувані втрати EL , котрі задаються формулою:

$$EL = \sum_i V_i \cdot p(V_i, A_i, D_i);$$

в свою чергу функція $p(V_i, A_i, D_i)$ обчислюється як

$$p(V_i, A_i, D_i) = \exp\left(-\frac{A_i \cdot D_i}{\sqrt{V_i}}\right) \cdot \left(\frac{A_i^2}{A_i^2 + V_i}\right);$$

де перший множник-ймовірність того, що запланована атака пройде невиявленою, і другий представляє ймовірність, що запланована, невиявлена атака буде успішною.

До беззаперечних переваг даного підходу можна віднести можливість наочного спостереження наслідків можливих рішень. Але в таких моделях робиться припущення, що і нападник, і захисник є досить обізнаними, і будуть діяти раціонально для досягнення своїх цілей. Дане припущення є обмежуючим, наприклад, одна із сторін може бути менш обізнаною, ніж передбачалося, і може через це недооцінити наслідки своїх дій, або вибрати хибний, з точки зору гри, шлях. Через це застосування теорії ігор можна назвати “нормативним” методом, тобто таким, що демонструє як ПОВИННА проходити гра, а не як вона ДІЙСНО буде відбуватися.

Були спроби вирішити проблему невизначеності та неточності, пов'язаної з ризиком за допомогою теорії нечітких множин [3]. Але до цього часу вона не застосовувалася для прогнозування терористичних актів.

Автор роботи [6] пропонує комплексний підхід для визначення ризику тероризму і визначає п'ять, на його погляд, ключових припущень, щодо оцінювання цього ризику:

1. Існує взаємозалежність між загрозою терористичного нападу і станом досліджуваної системи, який представлений вразливістю, стійкістю і критичним впливом.

2. Конкретна загроза, її ймовірність, її строки, стан досліджуваної системи і ймовірність наслідків можуть бути взаємозалежними.

3. Два питання, що виникають в процесі оцінювання ризику: “Яка ймовірність”, і “Які наслідки”, можуть бути взаємозалежними.

4. За допомогою стратегічних варіантів управління ризиками можна зменшити як ймовірність загрози певній системі так і пов’язану ймовірність наслідків, змінюючи стани системи (включаючи вразливість і стійкість).

5. Визначення ризику для вразливої системи від певної загрози повинне базуватися на системному та повторюваному процесі моделювання, з визнанням того факту, що стани системи являють собою важливий момент для визначення кількісних значень наслідків, заснованих на зборі інформації, дослідних доказах та іншій якісній інформації. Факт, що стани всіх систем є функціями часу (серед інших змінних) робить період часу основним на кожному етапі процесу оцінки ступеня ризику. Таким чином, ризик системи, викликаний ініціюючою подією (наприклад, погрозою), є багатовимірною функцією певної загрози, її ймовірності і періоду часу, станів системи (що представляють уразливість і стійкість), і ймовірнісних багатовимірних наслідків.

Велика кількість дослідників визнає колосальну невизначеність при ідентифікації та обчисленні ризику тероризму і тому надає перевагу менш точним аналітичним методам, що відносяться до якісних [11].

З їх точки зору точні, строгі та статичні методи моделювання є неефективним використанням ресурсів, а невідомі події пов’язані з тероризмом, наприклад, наявність терористичних груп з намірами атаки, або здатність таких груп змінювати стратегію в залежності від надходження інформації, являють собою серйозний виклик для методів моделювання, заснованих на кількісному підході. Набагато важливішим є розгляд питань, що стоять за формуванням картини ризику тероризму, до яких відносяться:

- потенційні терористичні загрози
- засоби перешкодження терористичним актам та їх ефективність
- можливі антизаходи на всіх етапах підготовки терористичного акту
- вразливість критичних систем
- наслідки терористичних актів
- включені вірогідності намірів терористичних груп, їх можливостей та ефектів антитерористичних заходів.

Висновки можуть бути зроблені шляхом зведення результатів аналізу в матрицю, що представляє картину ризику з інтервалами вірогідності та наслідків. Але навіть отримавши ці результати, важко знайти правильне розуміння того, що дійсно ці інтервали означають, і які оцінки характеризують терористичну загрозу як помірну, а які як значну.

Висновки

З огляду на вищезазначене, можна зробити висновок, що дослідження ризиків ядерного тероризму є порівняно новим напрямом, актуальність якого з точки зору підвищення національної безпеки держави є високою. Розробка надійної методики оцінювання ризиків ядерного тероризму для попередження нападів та спроб крадіжки ядерних матеріалів є пріоритетним, але досить важким завданням, через велику кількість невизначеностей при оцінюванні відповідних параметрів. Актуальним питанням є створення такої методики, моделі якої мінімізували б кількість параметрів, що привносять невизначеність в результат, але які водночас враховували б максимальну кількість параметрів, що впливають на ризик.

1. Лисиченко Г.В., Забулонов Ю.Л., Хміль Г.А.. Природний, техногенний та екологічний ризики: аналіз, оцінка, управління – К.: Наук. думка. – 2008. – 543 с.
2. Ліпкан В.А., Нікіфорчук Д.Й., Руденко М.М. Боротьба з тероризмом – Знання України. – 2002. – 254 с.
3. Akgun I., Kandakoglu A., Ozok A. F. Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism // Expert Syst Appl. – 2010. – V. 37, №5. – P. 3561-3573.
4. Cox L.A. Some limitations of “risk = threat x vulnerability x consequence” for risk analysis of terrorist attacks // Risk Analysis. – 2008. – V. 28, № 6. – P. 1749-1761.
5. Ezell, Barry C., Bennet S., Detlof von Winterfeldt, Sokolowski J., Collins A., Probabilistic Risk Analysis and Terrorism Risk // Risk Analysis. – 2010. – V. 30, № 4. – P. 575-589.
6. Haime Y.Y. On the Complex Quantification of Risk: Systems-Based Perspective on Terrorism // Risk Analysis. – 2011. – V. 31, №8. – P. 1175-1186.
7. Hausken K. Probabilistic risk analysis and game theory // Risk Analysis. – 2002. – V.22, №1. – P. 17-27.
8. Kaplan S., Garrick BJ. On the quantitative definition of risk // Risk Analysis. – 1981. – V. 1, №1. – P. 11-27.
9. Major J., Advanced techniques for modeling terrorism risk // Journal of Risk Finance. – 2002. – V.4, №1. – P.15-24.
10. Matthew Bunn. Guardians at the Gates of Hell: Estimating the Risk of Nuclear Theft and Terrorism - and Identifying the Highest-Priority Risks of Nuclear Theft. PhD dissertation, (Massachusetts Institute of Technology, 2007). – 466 p.
11. Sissel H. Jore, Ove Njå. Risk of Terrorism: A Scientifically Valid Phenomenon or a Wild Guess? The Impact of Different Approaches to Risk Assesment // Critical Approaches to Discourse Analysis across Disciplines. – 2010. – V. 4, № 2. – P. 197-216.
12. Willis H., Morral A., Kelly T., Medby J., Estimating terrorism risk // RAND Center for Terrorism Risk Management Policy. – 2005. – 94 p.

Г.В. Лисиченко, Ю.Л. Забулонов, В.М. Буртняк, Ю.О. Медведєв

СОВРЕМЕННЫЕ ПОДХОДЫ К ОЦЕНКЕ ТЕРРОРИСТИЧЕСКИХ РИСКОВ

В статье рассматриваются современные подходы к оценке рисков терроризма. Описаны сложности оценки рисков терроризма и связанные с этим неопределенности. Раскрыта необходимость в надежной методологии оценивания рисков.

G. Lysychenko, Y. Zabulonov, V. Burtnyak, Y. Medvedev

MODERN APPROACHES TO THE ASSESSMENT OF THE TERRORISM RISK

The article considers modern approaches to the modeling of terrorism risk. Are described the complexities of the terrorism risk assessment and related uncertainties. The need in reliable assessment methodology is revealed.