Мапа процесу оцінки загроз та ризиків ядерним установкам та ядерним матеріалам

Бобро Дмитро
Провідний науковий співробітник
Відділ енергетичної та техногенної безпеки

м. Київ - 2015 р.

Чинники, які визначають небезпеку тероризму:

1) разом із прямою дією на КІ, цілеспрямований вибір терористів, направлений на завдання максимальної шкоди, зазвичай тягне за собою вторинні наслідки – каскад порушень в роботі інших об’єктів КІ;
2) відміну від терактів, ні технологічні, ні природні катаклізми не є заздалегідь спланованими спробами добитися максимальної дії на суспільство, спеціально розрахованого на його дестабілізацію; для терористів же цей вторинний ефект ширшої дестабілізації є важливішим;
3) крім прямого збитку і вторинної дії терористи можуть намагатися отримати контроль над ключовими вузлами або іншими об'єктами інфраструктури, що у подальшому призведе до ще більшої дестабілізації;
4) зростаюче розмаїття вразливих об’єктів КІ суттєво ускладнює визначення найбільш ймовірних мішеней для терактів та проведення відповідних антитерористичних заходів;
5) заходи з посилення безпеки на одних об’єктах та системах КІ (наприклад, на АЕС), водночас підвищують ймовірність переключення терористів на інші, менш захищені та більш вразливі цілі (наприклад, на ТЕЦ, що за умов низьких температур може дати не менш значущий дестабілізуючий ефект).

Мотиви та наміри терористів

Для усвідомлення ***привабливості*** об'єктів КІ для терористичних атак слід розуміти, чим **мотивуються** терористи у своєму виборі об'єкта для нападу. Найбільш характерними мотивами є:

- намагання викликати масову загибель людей;
- нанести економічну (екологічну, суспільно-політичну тощо) шкоду;
- викликати тривогу та невпевненість, розбрат у людей, невіру у спроможність влади ефективно захистити людей;
- отримати широкий суспільно-політичний резонанс.

Загалом, все це зводиться до намірів терористів щодо ***суспільно-політичної дестабілізації***. **Са́ме *дестабілізуючий ефект* і є головною метою та мірою успіху теракту.**

І хоча критична інфраструктура ставала об'єктом нападу для порівняно невеликої кількості терактів (до 10-15 %), в той час як основна кількість терактів була направлена проти людей та військових об'єктів, ***одну із найбільших загроз для критичної інфраструктури представляють дії диверсійних груп терористичних організацій***.

Сукупний ризик як кількісна міра загрози для держави

Для виключення різночитань далі ризик r_i від і-тої події визначимо як добуток частоти реалізації окремої події $a_i(\tau)$, що здійснилася за проміжок часу τ, на наслідки l_i від цієї події:

$$r_i = a_i(\tau) l_i \qquad (1)$$

Щодо терористичної загрози конкретизуємо формулу 1, представивши частоту $a_i(\tau)$ у виді двох множників:

$$a_i(\tau) = b_i(\tau) p_i \qquad (2)$$

де $b_i(\tau)$ – оцінка частоти прояву намірів порушників щодо об'єктів фізичного захисту; p_i – імовірність досягнення цілей порушників за умови прояву намірів, тобто частка від усіх протиправних дій (спроб несанкціонованого проникнення, нападів, тощо), які привели до наслідків (втрат) l_i.

Як видно, якщо втрати виражені в одних одиницях виміру для всіх розглянутих подій, то можливе підсумовування ризиків за всіма подіями. Тоді для k-того конкретного об'єкта ризик R_k можна виразити у виді суми:

$$R_k = \sum_{i=1}^{i=I(k)} b_{ik}(\tau) p_{ik} l_{ik} \qquad (3)$$

де підсумовування ведеться по всім загрозам для об'єкта k обсягом I(k).

Ризик для держави, що має K об'єктів, є:

$$R = \sum_{k=1}^{k=K} R_k \qquad (4)$$

Визначення частот подій

Якщо для К об'єктів у державі за час τ зафіксовано $N_i(\tau)$ намірів вчинити і-ту дію, оцінка середньої частоти $b_i(\tau)$ може бути визначена по формулі

$$b_i(\tau) = \frac{N_i(\tau) K_{Ii}}{K\tau} \qquad (5)$$

де $KI_i \geq 1$ – оцінений коефіцієнт пропуску і-того типу подій.

Розмірність величини $b_i(\tau)$ може бути прийнята 1/(рік·об'єкт).

Для невтілених у державі подій можуть застосовуватися методи порівняння з аналогами іноземних країн, експертні оцінки тощо. Зокрема, якщо імовірність подій розподілена за законом Пуассона і за період спостережень τ над К об'єктами не відбулося жодної події, то можна стверджувати, що така реалізація можлива з довірчою імовірністю 0,95, якщо прийняти $b_i(\tau) \approx 0{,}05/(\tau \cdot K)$

Оцінка імовірності досягнення цілей порушників

Виходячи з прийнятих підходів імовірність досягнення цілей порушників можна представити в наступному виді:

$$p_i = (1 - P_{Ii} P_{Ni}) \qquad (6)$$

де PI_i – імовірність своєчасного виявлення (перехоплення) порушників;
PN_i – імовірність нейтралізації порушників.

Наслідки загроз

Якщо підходити до оцінки наслідків реалізованих загроз атомним електростанціям в аспекті захисту критичної інфраструктури, то слід враховувати їх взаємозв’язок з іншими елементами критичної енергетичної інфраструктури та можливість каскадної аварії в об’єднаній енергетичній системі України.

З іншої сторони, наслідки стосуються й іншої шкоди, які можна звести у наступні основні групи:
збиток здоров’ю і життю людей (у т.ч. кількість постраждалих, загиблих, евакуйованих);
економічний збиток (розмір економічних втрат, як прямих, так і не прямих);
екологічні наслідки (вплив на населення та навколишнє природне середовище);
політичні та репутаційні збитки (суспільна тривога, втрата впевненості в дієздатності влади, розбрат, зниження авторитету влади, порушення державного управління тощо).

Звернемося далі до розгляду розмірності втрат (наслідків). Для можливості обліку втрат різного характеру і різної розмірності в одній функції ризику можна використовувати нормовані втрати, тобто замість абсолютної величини втрат вводяться відносні втрати, які визначаються для кожної групи подій з однаковою розмірністю втрат:

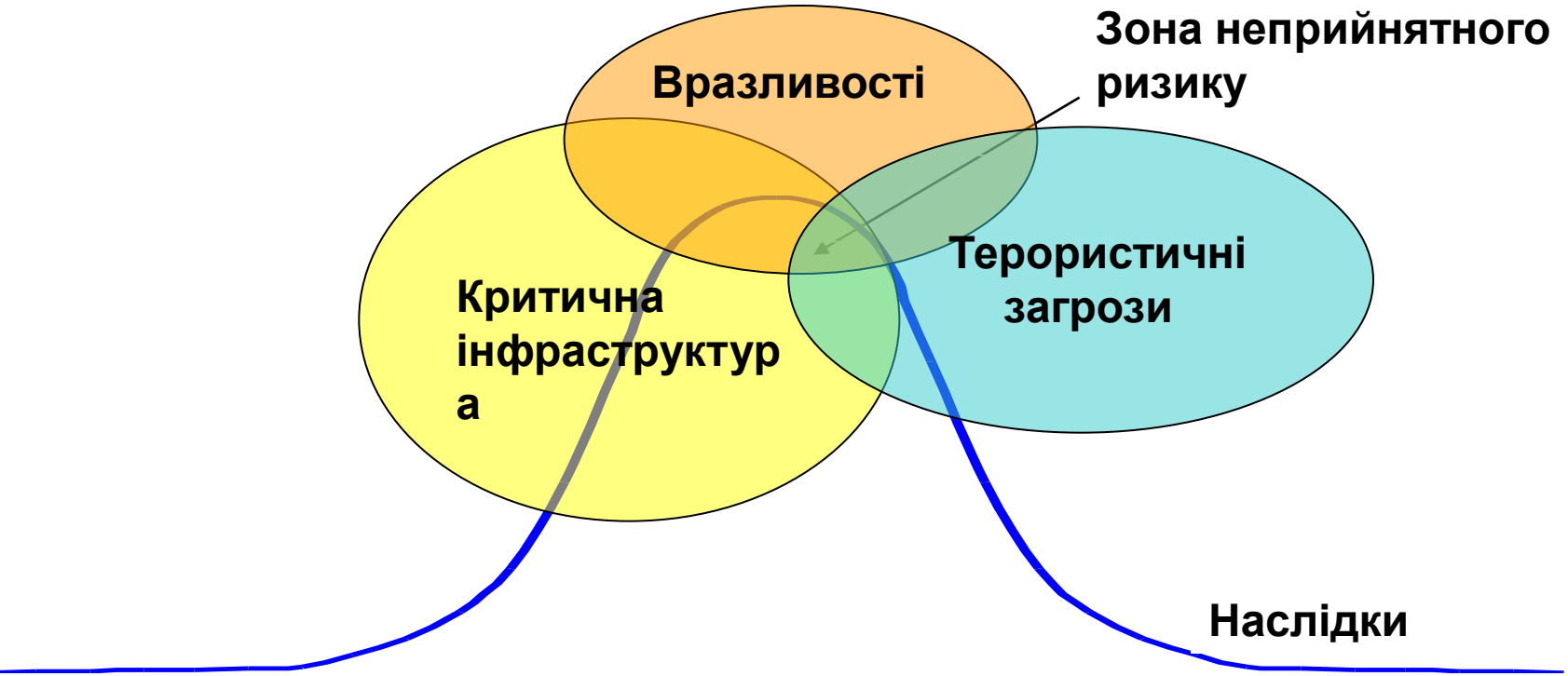
$$L_{0i} = Li / Lmax \qquad (7)$$

де lmax – втрати від реалізації події з максимальним збитком.

Такий підхід не виключає застосування експертної або іншої оцінки безпосередньо нормованих втрат для кожної події.

Оцінка терористичних загроз та ризиків

Не вдаючись до числових розрахунків, можна сказати, що ризик терористичного нападу на об’єкт КІ буде тим більший, чим вище рівень певної загрози цьому елементу, чим більше вразливість зазначеного елементу стосовно конкретної загрози і чим важчі наслідки у випадку реалізації загрози (здійснення нападу).

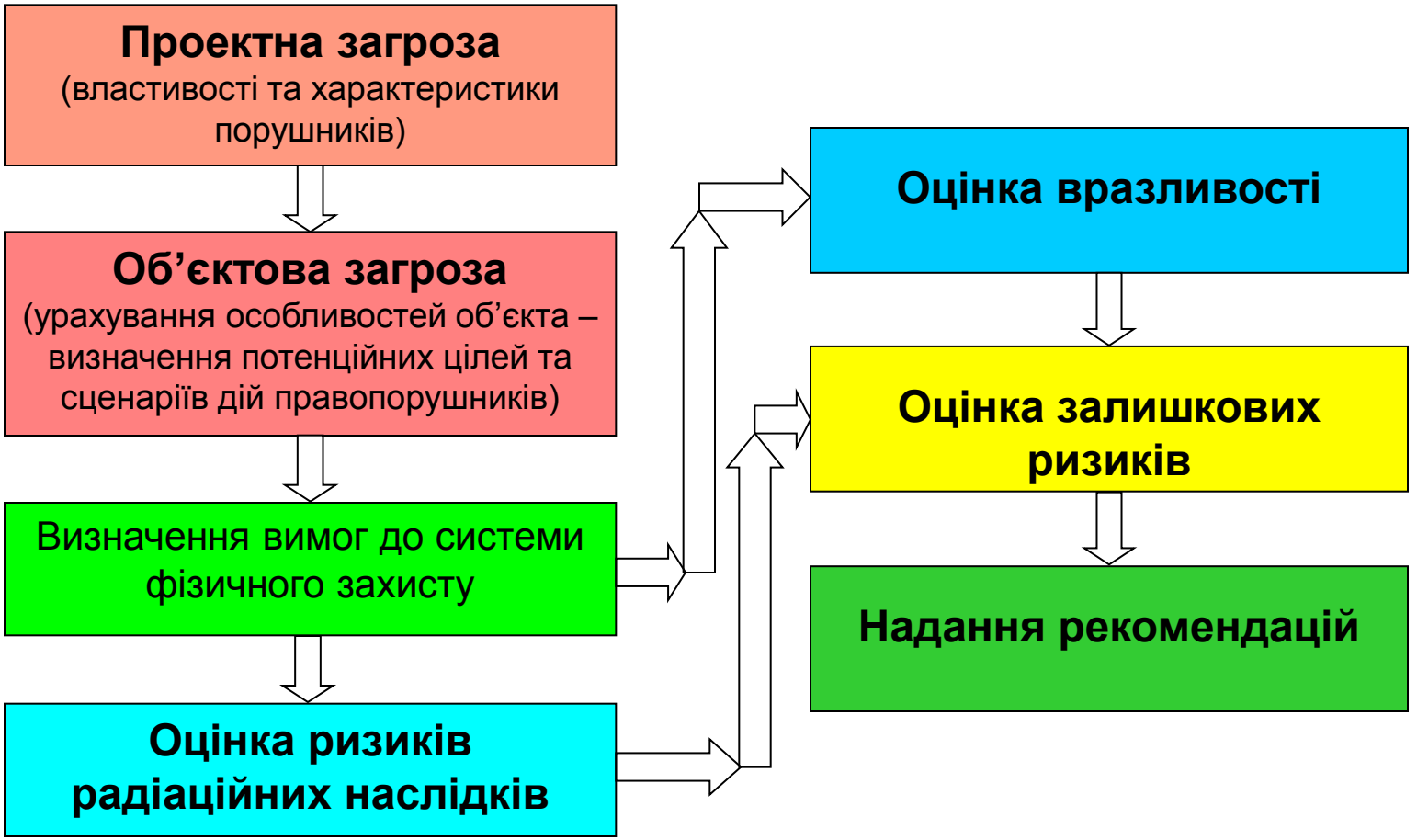


Фактор невизначеності у процесі оцінки терористичних загроз

Слід зазначити, що наведений «класичний» методологічний підхід оцінки терористичних загроз та ризиків не завжди є таким, що може бути реалізованим на практиці. При цьому, якщо для певних категорій подій можна отримати їхні ймовірнісні характеристики (точніше, частоти подій, які можна вирахувати за даними, що зберігаються у базі даних Global Terrorism Database ***[1]***, чи базі даних американської неурядової неприбуткової дослідної організації RAND ***[2]***), то для інших подій можна зробити лише припущення щодо їх частоти. Тобто, для процесу оцінки терористичних ризиків характерна суттєва невизначеність. Важливо відмітити, що **найбільший внесок у цю невизначеність дає саме етап оцінки терористичної загрози конкретному об’єкту КІ**.

[1] Global Terrorism Database, http://www.start.umd.edu/gtd/
[2] RAND Database of Worldwide Terrorism Incidents, http://www.rand.org/nsrd/projects/terrorism-incidents.html

Мапа оцінки терористичних ризиків і загроз - фізична ядерна безпека



Загальний підхід до оцінки ризиків – експертна оцінка

Як свідчать результати використання **методу Дельфі**, у разі залучення до експертної оцінки компетентних у справі людей, **отримана усереднена оцінка буде точною не менш ніж на 80%.** При цьому, якщо провести декілька раундів оцінки, попередньо ознайомивши експертів з результатами попередніх раундів, то достовірність оцінки буде ще вищою.

Водночас, якісна експертна оцінка вимагає чіткого розуміння експертами усіх термінів, що використовуються, та процесів, що аналізуються, обґрунтування та розуміння шкал, що використовуються для оцінки загроз, вразливостей та наслідків. При цьому, найбільшу похибку дає не різниця у кваліфікації експертів та можливість впливу одних експертів на інших, а *психологія сприйняття ризику*. Так, люди (і експерти тут не є виключенням) перебільшують одні ризики та недооцінюють інші.

Водночас, ризики, які мали місце в житті експерта (особливо недавно чи були пов’язані зі смертельною небезпекою), для нього часто мають більшу вагу, ніж ті, з якими він ніколи не зіштовхувався. А звідси виникає його зашореність та налаштованість на боротьбу з минулими типами загроз, ніж здатність передбачити їх нові типи.

Загальний підхід до оцінки ризиків та захисту КІ

Загалом, все це укладається в поняття «***моделі загроз***», яка включає:

- опис можливих **загроз КІ**, їх джерел, мотивів, засобів, що використовуються, та методів реалізації (для терористичної загрози – «***модель порушника***»);
- опис об’єктів, придатних для реалізації загроз, визначення **вразливостей** цих об’єктів до загроз, що аналізуються;
- опис можливих **втрат**, масштабу потенційної шкоди, її ймовірності.

Таке моделювання ризику на системному рівні сприяє не лише ідентифікації потенційних небезпек, але й більш глибокому розумінню устрою та функціонування об’єкта/системи КІ, виявленню «слабких ланок» в системі, а, загалом, *адекватному ранжуванню ризиків*.

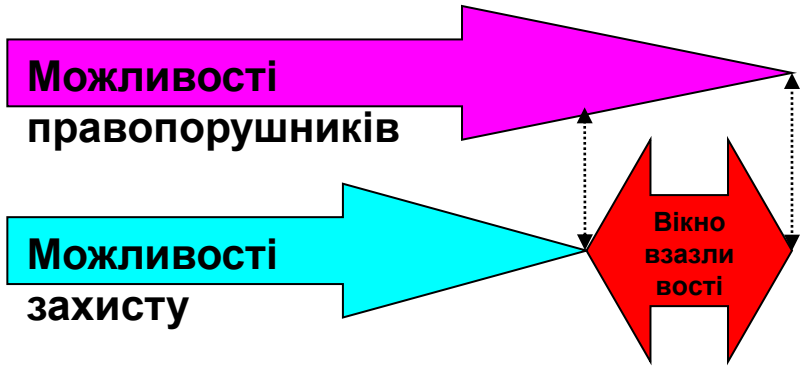
При цьому слід пам’ятати, що оцінка ризику – це «моментальний знімок» стану справ на даний момент, який має переглядатися на регулярній основі.

Загальний підхід до оцінки ризиків та захисту КІ

Виходячи з такого розуміння основних складових ризику можна визначити й основні **шляхи зменшення ризиків КІ**:

- **зниження рівня загроз** (наприклад, шляхом перехоплення порушників до завдання ними удару по об’єкту КІ, посилення охорони кордонів тощо);
- **зниження вразливості** об’єкта КІ (створення системи фізичного захисту, яка здатна протистояти правопорушникам);
- **мінімізація можливої шкоди** (захист населення тощо);
- **підвищення стійкості** (підвищення технічної надійності та забезпечення можливості як скорішого відновлення функцій КІ).

Фактично, з одного боку потрібно закрити **вікно вразливості** – адаптувати систему фізичного захисту об’єктів КІ до чинних загроз, а з іншого – на державному рівні мати розвинену систему запобігання і реагування на надзвичайні ситуації та передбачити заходи з відновлення функцій цих об’єктів (у т.ч. за рахунок резервування та диверсифікації).



Висновки та рекомендації

Створення та функціонування *моделі загроз* об’єктам КІ, зокрема, терористичних загроз, становить безперервний високотехнологічний цикл, реалізація якого вимагає від держави належного інформаційно-аналітичного, організаційно-правового, кадрового та науково-технічного забезпечення.

Застосування методів оцінки ризиків на державному рівні дозволить мати кількісні, а для терористичних загроз – адекватні якісні оцінки очікуваної небезпеки у випадках реалізації загроз критичній інфраструктурі.

Це дасть можливість одержати необхідний баланс між вимогами забезпечення захисту КІ і наявних ресурсів – зокрема, визначити пріоритетність захисту об’єктів, вимоги до систем фізичного захисту, до резервування тощо.