УДК 323:342.5:005.1:001.8

УРАХУВАННЯ ПРОЕКТНИХ ЗАГРОЗ У РОЗБУДОВІ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Бобро Дмитро Геннадійович,
кандидат фізико-математичних наук

Проаналізовано сучасні методологічні підходи до оцінки загроз та небезпек об'єктам критичної інфраструктури. Продемонстровано, що досвід державної системи фізичного захисту (ядерних установок і матеріалів) щодо аналізу загроз, побудови моделі порушника та моделі загроз, визначення проектної загрози може бути використаний і при розбудові в Україні державної системи захисту критичної інфраструктури. Водночас необхідність захисту критичної інфраструктури від загроз будь-якого походження та спрямованості (*all hazards approach*) вимагає застосування моделі загроз, що, окрім моделі порушника, містить модель об'єкта та модель соціально-політичної обстановки, в якій цей об'єкт функціонує. Надано рекомендації щодо визначення проектної загрози об'єктам критичної інфраструктури та шляхів подальшої розбудови в Україні державної системи захисту критичної інфраструктури.

Ключові слова: критична інфраструктура, захист критичної інфраструктури, небезпека, загроза, модель загроз, проектна загроза, вразливість, ризик.

Bobro Dmytro

TREATMENT OF PROJECT THREATS IN DEVELOPMENT OF THE STATE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

The modern methodological approaches are analyzed to the estimation of hazards and threats to the infrastructure objects. It is shown, that experience of the State system of physical protection (for nuclear installations and materials) concerning the analysis of threats, building of violator's model and threat's model, definition of design basis threat can be used for construction of State system of critical infrastructure protection in Ukraine. At the same time, the necessity to protect critical infrastructure from the threats of any origin and directionality (all hazards approach) requires application of threats model, which must use not only the violator's model, but also the object's model and the model of socio-political situation. Recommendations are provide to determinate the design basis threat to critical infrastructure objects and ways of further construction of State system of critical infrastructure protection in Ukraine.

Keywords: critical infrastructure, critical infrastructure protection, hazard, threat, threat's model, design basis threat, vulnerability, risk.

Гібридна агресія Росії актуалізувала для України питання захисту інфраструктури, життєво важливої для безпеки людини, суспільства та держави, яка в світовій практиці визначається як критична[1].

Слід зазначити, що вперше на державному рівні в Україні термін «критична інфраструктура» (далі – *КІ*) згадується в Стратегії національної безпеки України (у редакції 2015 р.), де були визначені основні загрози та пріоритети забезпечення безпеки КІ. Підходи до розуміння сутності цього поняття були опрацьовані в Зеленій книзі з питань захисту критичної інфраструктури в Україні [1], підготовленій у Національному інституті стратегічних досліджень. У цій книзі

[1] У країнах світу, які для гарантування національної безпеки використовують поняття «критична інфраструктура», під нею розуміють об'єкти й системи, настільки важливі для забезпечення життєдіяльності людей і держави, що дестабілізація їхньої роботи, не кажучи вже про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків.

з урахуванням досвіду США, ЄС, країн – членів НАТО було систематизовано підходи до дефініції поняття «критична інфраструктура», визначено основні групи загроз КІ (техногенні аварії та технічні збої, спричинені, зокрема, людським фактором; природні лиха та небезпечні природні явища; зловмисні дії), надано пропозиції щодо основних принципів, на яких має здійснюватися подальша розбудова в Україні системи захисту критичної інфраструктури.

Заходи з подальшої розбудови системи захисту КІ були визначені рішеннями Ради національної безпеки і оборони України від 29 грудня 2016 р. та 16 лютого 2017 р. Метою цієї системи має стати гарантування спроможності критичної інфраструктури виконувати та, у разі переривання, у найкоротші терміни відновлювати функції із життєзабезпечення людей, суспільства, бізнесу і держави. При цьому слід враховувати необхідність забезпечення захисту критичної інфраструктури від усіх видів загроз (т. зв. підхід *all hazards approach*).

Водночас усвідомлення неможливості забезпечити однаково високий рівень захисту всієї критичної інфраструктури від усіх можливих загроз зумовило розвиток підходу, зосередженого на вибірковому захисті конкретного об'єкта КІ від обмеженого набору відомих та відносно прогнозованих загроз, при якому надається пріоритет тій або іншій інфраструктурі залежно від ступеня її «критичності», головною мірою якої є ризик [2]. Методологічно [3] це означає проведення:

- аналізу та класифікації загроз, оцінки ймовірності (точніше, частості) кожної загрози;
- оцінки вразливостей до кожного типу подій/атак (що з урахуванням частості загрози визначає ймовірність завдання шкоди);
- оцінки наслідків (для різних сценаріїв розвитку подій).

Саме проаналізувавши наявні загрози та небезпеки, зробивши їх відсів за результатами аналізу ризиків, можна сформувати перелік загроз (небезпек), на захист від яких має бути розрахована система захисту критичної інфраструктури. Цей перелік і буде т. зв. «проектною загрозою» – основою, яка визначатиме, від кого та від чого потрібно захищатися.

Питання захисту критичної інфраструктури за останні роки розглядалось у низці робіт, зокрема, А.О. Мороза, О.М. Євдіна, В.А. Заславського, В.Ф. Гречанінова, В.В. Бєгуна, С.І. Кондратова, Д.С. Бірюкова, О.М. Суходолі. Більшість цих робіт так чи інше стосувалася запровадження в управління безпекою ризик-орієнтованого підходу (який методологічно ґрунтується на аналізі загроз), проте питання визначення проектної загрози для критичної інфраструктури детально не опрацьовувалося (точніше, воно розглядалося лише в межах державної системи фізичного захисту (далі – *ФЗ*) та стосувалося лише загроз протиправних дій щодо ядерних установок та ядерних/радіоактивних матеріалів).

Мета статті – опрацювання підходів до визначення проектної загрози об'єктам критичної інфраструктури та можливості забезпечення адекватного захисту КІ від загроз різного походження та спрямованості, надання пропозицій щодо подальшої розбудови державної системи захисту критичної інфраструктури в Україні.

Модель порушника та модель загрози протиправних дій

У межах державної системи фізичного захисту передбачені заходи, що включають увесь ланцюжок дій: від оцінки загроз протиправних дій (у т. ч. визначення проектної загрози) та категоризації об'єктів системи до встановлення конкретних вимог щодо систем фізичного захисту, оцінки вразливості об'єктів, імовірності завдання шкоди, проведення перевірок систем фізичного захисту та планів взаємодії. Подібні підходи можуть бути використані також при розбудові в Україні державної системи захисту КІ.

Слід зазначити, що визначення проектної загрози ядерним установкам та ядерним матеріалам в Україні ґрунтується на рекомендаціях МАГАТЕ з фізичної ядерної безпеки [4] та аналізі сучасного безпекового середовища, яке враховує суттєві зміни безпекової ситуації внаслідок агресії РФ[2]. При цьому основою проектної загрози в системі ФЗ є «модель порушника», на основі якої будується «модель загрози». Обидві моделі є вихідною інформацією для

[2] Нині в Україні діє редакція Проектної загрози ядерним установкам, ядерним матеріалам, радіоактивним відходам, іншим джерелам іонізуючого випромінювання, схвалена рішенням РНБО України від 16 жовтня 2012 р. (зі змінами, внесеними Указом Президента України від 27 серпня 2015 р. № 521/2015). Цей документ є таємним.

розроблення політики безпеки і проектування будь-яких систем захисту.

Довідково. Відповідно до рекомендацій МАГАТЕ [4] проектна загроза (*design basis threat*) – це «ознаки та характеристики потенційних внутрішніх та/або зовнішніх порушників, що можуть вчинити спробу несанкціонованого вилучення або саботажу (диверсії), для протидії яким створюється та оцінюється система фізичного захисту». Закон України «Про фізичний захист ядерних установок…» дає практично аналогічне визначення: «Проектна загроза – властивості та характеристики потенційних правопорушників, дії яких можуть бути спрямовані на вчинення диверсії, крадіжки або будь-яке інше неправомірне вилучення радіоактивних матеріалів, для протидії яким створюється система фізичного захисту»[3]. Аналогічне визначення міститься й у Правилах фізичного захисту ядерних установок та ядерних матеріалів, розроблених Держатомрегулювання: «Проектна загроза – визначені в установленому порядку характеристики потенційних правопорушників, які могли б здійснити спробу несанкціонованого вилучення ядерних матеріалів або вчинення акту ядерного тероризму, для протидії яким визначається, створюється та оцінюється система фізичного захисту»[4].
Деякі відмінності згаданих визначень зумовлені дещо різним міжнародним трактуванням таких термінів, як «саботаж (диверсія)», «акт тероризму», та їх визначеннями в українському законодавстві.

Подібні підходи в оцінці загроз використовуються і в США. Зокрема, у документі «Політика Міністерства енергетики щодо базової проектної загрози» (*DOE O 470.3A, Design Basis Threat Polic*y)[5] визначено загрози, які стосуються аспектів захисту ядерної зброї (зміст зазначеного документа утаємничений), а в документі Комісії з ядерного регулювання США (*US NRC 10 CFR*)[6] у загальному вигляді (без конкретизації кількісних показників) визначено характеристики порушників щодо цивільних ядерних об'єктів та ядерних матеріалів. Так, у разі диверсії (в оригіналі – *sabotage*) використовується така модель порушника:
(i) Одиночна група, що атакує через одну точку входу; декілька груп, що атакують через декілька точок входу; комбінація груп та окремих нападників, що атакують через декілька точок входу з наступними атрибутами, підтримкою та оснащенням:
(A) добре підготовлені (включаючи військову підготовку та навички), віддані справі та готові убивати чи бути вбитими, з достатніми знаннями для визначення конкретного обладнання чи місць для успішного нападу;
(B) внутрішня допомога – активна (допомога для входу/виходу, відключення сигналів тривоги та засобів зв'язку, участь у нападі) чи пасивна (надання інформації) або те й інше;
(C) відповідна зброя, у т. ч. ручна автоматична зброя, оснащена глушниками та яка має ефективну дальність і точність;
(D) ручне оснащення, у т. ч. для нейтралізації (несмертельна зброя), вибухівка для входу або підриву реакторного обладнання;
(E) наземні та водні транспортні засоби;
а також:
(ii) Внутрішня загроза.
(iii) Напад із застосуванням замінованого транспортного засобу.
(iv) Напад із застосуванням замінованого водного транспортного засобу, які можуть бути скоординовані із зовнішнім нападом.
(v) Кібератака.

Щодо інших країн, то, наприклад, в Австралії у проектній загрозі ядерним об'єктам, окрім згаданих вище характеристик порушників, як оснащення розглядаються ще й дрони, а модель загроз включає ще й напад на ядерний об'єкт за допомогою літака, який може бути скерований на об'єкт як імпровізований вибуховий пристрій[7].

---

[3] Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» від 10 жовтня 2000 р. № 2064-III [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2064–14/page2

[4] Правила фізичного захисту ядерних установок та ядерних матеріалів, затверджені наказом Державного комітету ядерного регулювання України від 4 серпня 2006 р. № 116 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/z1067–06

[5] DOE O 470.3A, Design Basis Threat Policy (U) [Електронний ресурс] / U.A. Department of Energy. – Режим доступу : https://www.directives.doe.gov/directives-documents/400-series/0470.3-border-a

[6] Purpose and Score. NRS Regulations. Part Index [Електронний ресурс] / U.A. NRS. – Режим доступу : https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

[7] Australian National Design Basis Threat Approved Declassification [Електронний ресурс] / Australian Safeguards and Non-Proliferation Office. – Режим доступу : http://dfat.gov.au/international-relations/security/asno/Documents/design-basis-threat.pdf

У Російській Федерації формування базових проектних загроз об'єктам паливно-енергетичного комплексу (ПЕК) здійснюється відповідно до низки нормативно-правових актів, а сама базова проектна загроза [5] містить відомості про:

- цілі здійснення актів незаконного втручання – критичні елементи, що підлягають захисту, можливі засоби та способи їх пошкодження (руйнування);
- сценарії здійснення актів незаконного втручання, у т. ч. вживані тактики досягнення поставлених цілей, маршрути та часові характеристики дій порушника відносно кожного з критичних елементів об'єкта;
- розрахункові моделі порушника, у т. ч. чисельність, склад, розподіл нападників за елементами бойового ладу, озброєння, оснащення, екіпіровки; ступені обізнаності із виробничо-технологічним циклом і системами фізичного захисту об'єкта; спроможності санкціонованого доступу;
- виробничі особливості об'єкта, його географічне, соціальне та криміногенне оточення.

Зазначені дані в РФ включаються до паспорта безпеки об'єкта ПЕК, який відображає не лише характеристики цього об'єкта з точки зору його потенційної небезпеки (категорії небезпеки, отриманої з урахуванням властивостей небезпечних речовин, що використовуються на об'єкті, та за впливом вражаючих факторів, що можуть мати місце у разі аварії на об'єкті), але й можливі наслідки в результаті незаконного втручання у функціонування об'єкта, оцінку стану систем інженерно-технічного та фізичного захисту, заходи із забезпечення антитерористичної захищеності [6].

Таким чином, в аспекті фізичного захисту об'єктів модель загроз будується на моделі порушника та розробляється для того, щоб встановити:

- від кого захищатися;
- яка мета потенційного порушника (причини та мотиви, цілі на об'єкті);
- хто може бути потенційним порушником (одна людина чи група осіб), він є зовнішнім або внутрішнім порушником, чи, можливо, вони діють у зговорі;
- якими знаннями та навичками володіє порушник (як щодо об'єкта, включно із системою його фізичного захисту, так і щодо використання зброї, засобів зв'язку та розвідки, наприклад, дронів, транспорту тощо);
- якими методами та засобами користується порушник (озброєння, технічна оснащеність, засоби зв'язку, розвідки, пересування тощо);
- яку тактику дій може використати порушник (сценарії дій).

При цьому загрози критичній інфраструктурі слід розглядати також і з точки зору виокремлення елементів об'єкта захисту, на які ці загрози спрямовані [1; 3]:

- *фізичні елементи*, зокрема технологічне обладнання та ресурси об'єктів;
- *системи управління*, зокрема системи автоматичного управління та регулювання технологічними процесами, системи зв'язку, охорони (у т. ч. контролю доступу, інженерно-технічні засоби охорони тощо);
- *персонал* об'єктів, зокрема диспетчерський, оперативний, який безпосередньо забезпечує функціонування критичної інфраструктури, персонал охорони тощо.

Проте подібні моделі загроз та сформована на їх основі проектна загроза, заснована лише на моделі порушника, не дає можливості побудувати систему захисту критичної інфраструктури від загроз усіх типів – будь-якого походження та спрямованості.

Модель загроз та проектна загроза критичній інфраструктурі

Слід зазначити, що моделі загроз та порушника широко використовуються у світі також і в рамках захисту інформаційних ресурсів і кіберзахисту об'єктів КІ. Причому саме в цій сфері був здійснений перехід від розгляду лише загроз зловмисних (чи, точніше, протиправних) дій до більш ширшого кола загроз.

Так, у Російській Федерації при аналізі джерел загроз безпеці інформації аналізуються як антропогенні джерела (особи, що здійснюють протиправну діяльність), так і природні та техногенні джерела [7]. Модель порушника включає їхні типи (зовнішній/внутрішній) та види (спецслужби держав, терористичні чи екстремістські угруповання, кримінальні структури, конкуренти, розробники, адміністратори, обслуговуючий персонал, користувачі тощо),

можливі цілі та мотивацію порушників, їхній потенціал.

В Україні відповідно до Типового положення про службу захисту інформації в автоматизованій системі (АС) [8] також передбачено створення моделі порушника та моделі загроз. Під моделлю порушника розуміється «абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії та т. ін. Стосовно АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, які знаходяться за межами контрольованої зони)». Модель порушника має визначити:

- можливу мету порушника;
- категорії осіб, з числа яких може бути порушник;
- припущення щодо кваліфікації порушника;
- припущення щодо характеру його дій.

У моделі загроз інформації в автоматизованій системі, окрім навмисних дій (спроб) потенційних порушників, мають бути враховані такі події:

- зміна умов фізичного середовища (стихійні лиха й аварії, як-от: землетрус, повінь, пожежа тощо);
- збої та відмови в роботі обладнання та технічних засобів АС;
- наслідки помилок під час проектування та розробки компонентів АС;
- помилки персоналу (користувачів) АС під час експлуатації.

Якщо звернутися до досвіду західних країн, то, наприклад, під час аналізу загроз електроенергетичному сектору США [9; 10] бачимо, що відповідна модель включає:

- загрози природного характеру (торнадо, повені, землетруси тощо);
- людські помилки та інші техногенні аварії;
- протиправні дії (кримінальні та терористичні угруповання, активісти екстремістських груп різного спрямування, хакери тощо).

Загалом же при розгляді моделей загроз критичній інфраструктурі США на національному рівні в рамках підходу *all hazards approach* розглядається низка загроз природного та техногенного характеру, а також зловмисних дій, пов'язаних у т. ч. з використанням як зброї літаків, актів ядерного, радіологічного, хімічного та біологічного тероризму [11].

Таким чином, в аспекті захисту критичної інфраструктури модель загроз КІ є більш широким (відносно моделі в системі ФЗ) поняттям та базується на пошуку відповіді на питання: «Які фактори можуть завдати шкоди функціонуванню об'єкта КІ?» А це означає необхідність аналізу не тільки потенційних порушників, а й самого об'єкта критичної інфраструктури – де він розташований (у т. ч. географічні, кліматичні умови, сейсмічні показники); які потенційно-небезпечні технології на цьому об'єкті використовуються; де та як розміщено обладнання, як до нього можна дістатися, що може вплинути на його роботу; які інші об'єкти розташовані поряд із об'єктом, який аналізується, та можуть потрапити під дію вражаючих факторів; яке місце цей об'єкт займає у виробничих ланцюжках; хто є споживачем його продукції (тобто взаємозалежність з іншими господарськими об'єктами) тощо.

Водночас модель загроз буде неповною без моделювання соціально-політичної обстановки, в якій об'єкт КІ функціонує, оскільки від цього залежить можливість реалізації низки загроз воєнного та соціально-політичного характеру.

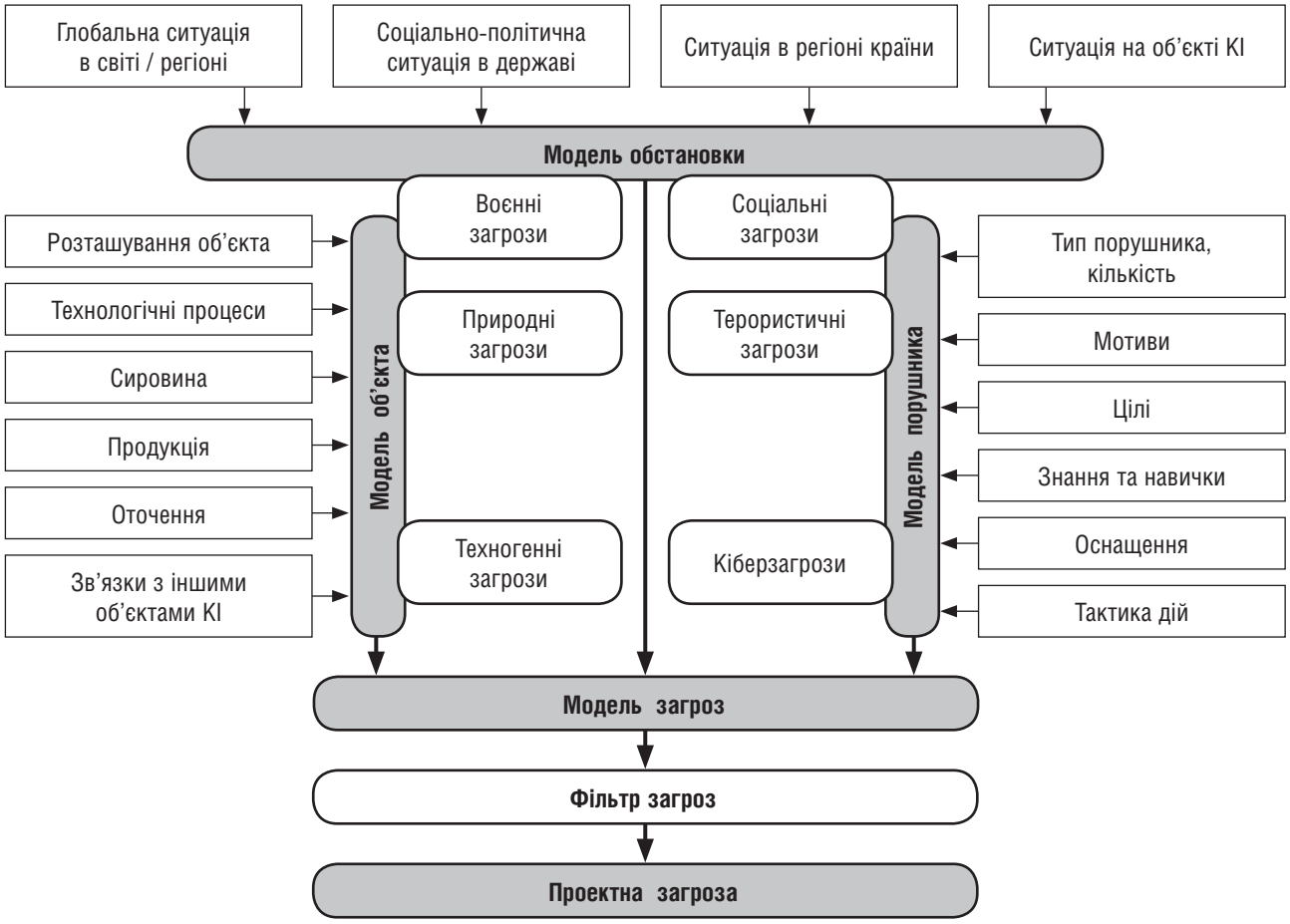
Отже, адекватна модель загроз об'єкта КІ має включати модель порушника, модель об'єкта та модель обстановки [12; 13; 14]. Зважаючи на зазначене, модель загроз можна представити графічно (*рис. 1*).

У цій моделі відповідно до підходу *all hazards approach* враховано загрози (небезпеки) будь-якого походження: природного й техногенного характеру (ураховуються при опрацюванні моделі об'єкта); соціально-політичного та воєнного характеру (ураховуються при опрацюванні моделі обстановки); протиправні дії – кіберзагрози та загрози диверсійно-терористичного характеру (ураховуються в моделях порушника).

Однак варто враховувати, що ці моделі (обстановки, об'єкта, порушника) є взаємопов'язаними та взаємозалежними. Так, наприклад, модель об'єкта є основою для визначення потенційних цілей порушника (у т. ч. щодо кібератак), а соціально-політична ситуація в державі, регіоні та на об'єкті впливає на мотиви (протестні настрої тощо) та дії (наприклад, перекриття доріг тощо) порушників.

Завдяки моделюванню формується *модель загроз*, яка містить перелік можливих загроз (небезпек) об'єкта критичної інфраструктури, що впливають

Рис. 1. **Модель загроз та проектна загроза об'єктам критичної інфраструктури**



Джерело: розроблено автором.

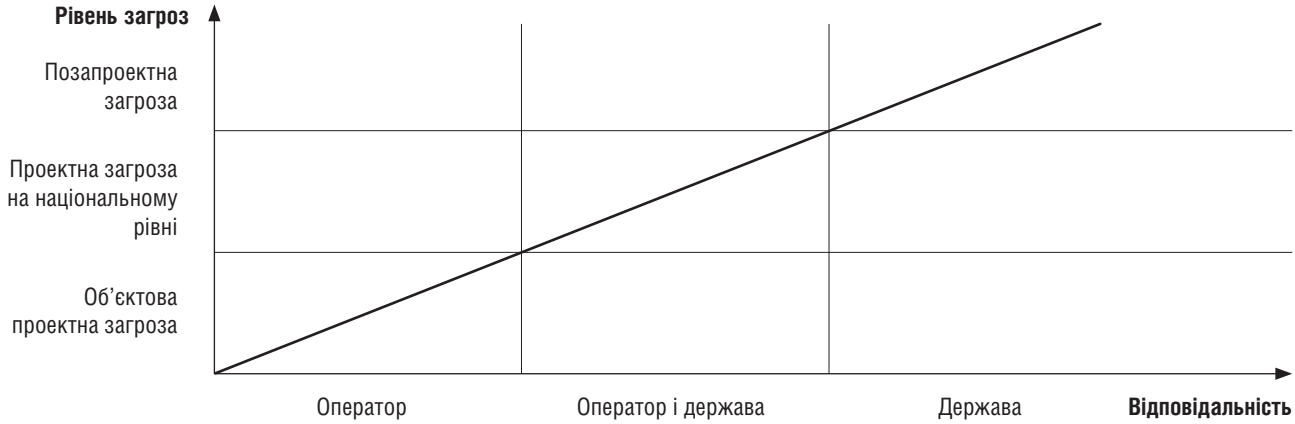
на його безпечне функціонування[8]. Проте, як уже згадувалося, забезпечити однаково високий рівень захисту всієї критичної інфраструктури від усіх імовірних загроз неможливо. Потрібно провести фільтрацію та ранжування загроз. Дослідники [12] пропонують для цього використовувати їх імовірність (відсів малоймовірних), величину (відсів тих, вплив яких на функціонування об'єкта КІ не виходить за припустимі межі) та потенційні втрати (відсів тих загроз, втрати від реалізації яких є прийнятними). Вважаємо, що ці підходи є слушними, проте більш коректно здійснювати відсів загроз за ризиками, оскільки саме ризик, оцінений для різних сценаріїв розвитку подій, є мірою «критичності» об'єкта КІ [2; 15]. При цьому навіть малоймовірні події (з частістю 10^{-5} на рік і нижче) мають ураховуватися в моделі загроз, якщо їх наслідки (а з урахуванням вразливості об'єкта вони й становитимуть ризик) є суттєвими.

Слід зазначити, що означений підхід до відсіву загроз є відсівом «знизу», а потрібно провести ще й відсів «зверху» – тобто розподілити загрози на ті, що включаються до проектної загрози, та на позапроектні загрози, нейтралізація яких є відповідальністю держави (наприклад, загрози бойових дій). Такий підхід (щодо розподілення відповідальності між оператором КІ та державою) є одним із основоположних принципів МАГАТЕ щодо встановлення та підтримки режиму фізичного захисту[9]. Це розмежування

[8] Слід зазначити, що, окрім відомих (прогнозованих) загроз (небезпек), існує ще й безліч інших загроз, а для відомих загроз – безліч можливих сценаріїв їх реалізації. Тому побудувати абсолютну систему захисту КІ неможливо. Проте і за цих умов невизначеності та реалізації неврахованих загроз є можливість забезпечити стійкість критичної інфраструктури шляхом швидкого відновлення її функцій, у т. ч. за рахунок диверсифікації та резервів.

[9] Відповідно до рекомендацій МАГАТЕ [4] визначено низку основоположних принципів щодо встановлення та підтримки режиму фізичного захисту, зокрема щодо відповідальності: держави (принципи *A* та *B*), органу регулювання безпеки (принцип *D*), операторів (принцип *E*), проведення державою оцінки загрози (принцип *G*) тощо.

Рис. 2. **Схема розподілення відповідальності між оператором КІ та державою**



Джерело: розроблено автором.

щодо захисту КІ можна представити у вигляді схеми (*рис. 2*).

Можна навести такий приклад класифікації розмежування відповідальності, яка залежить від характеристик моделювання порушника та загроз:

- відповідальність оператора – внутрішній порушник, що діє через образу на керівництво об'єкта, не має зброї чи інших активних засобів впливу (вибухівки тощо), але може втрутитись у керування технологічними процесами на об'єкті, через що може статися збій у функціонуванні об'єкта КІ або аварія;
- відповідальність держави та оператора – внутрішній порушник, що діє на критично- чи життєво-важливому об'єкті КІ[10] у зговорі з диверсійно-терористичною групою, оснащення якої не перевищує показників, встановлених проектною загрозою на національному рівні;
- відповідальність держави – незаконне збройне формування, що має на озброєнні важку військову техніку (позапроектна загроза).

При цьому роль держави полягає не тільки в нейтралізації позапроектних загроз чи участі в нейтралізації проектних загроз критичній інфраструктурі, а й у:

- розробці та впровадженні єдиних методологічних підходів, на основі яких мають бути проаналізовані загрози критичній інфраструктурі, сформована модель загроз, підготовлена проектна загроза критичній інфраструктурі на національному рівні (залежно від категорії критичності об'єктів інфраструктури [16]);
- наданні методологічної підтримки операторам критичної інфраструктури в розробці об'єктових проектних загроз, планів їх попередження та нейтралізації;
- оцінці ефективності діяльності у сфері захисту критичної інфраструктури.

Так, у США цими питаннями, як і іншими методологічними питаннями захисту КІ, опікується Національний координаційний центр інфраструктури Офісу захисту інфраструктури Міністерства внутрішньої безпеки (*Department of Homeland Security, Office of Infrastructure Protection, National Infrastructure Coordinating Center*)[11]. Проте наразі в Україні подібний центр відсутній.

Висновки та рекомендації

Державна система фізичного захисту (щодо ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання), яка існує в Україні, в організаційному плані є однією з найбільш просунутих державних систем реагування та захисту, оскільки передбачає весь ланцюжок дій щодо забезпечення захисту: від оцінки загроз, визначення проектної загрози, категоризації об'єктів системи до встановлення конкретних вимог щодо систем фізичного захисту, оцінки вразливості об'єктів, імовірності завдання шкоди, проведення перевірок систем фізичного захисту та планів взаємодії. Подібні підходи можуть бути використані при розбудові в Україні державної системи захисту КІ, зокрема під час розробки проектної загрози як основи,

[10] Категорії об'єктів КІ наведені відповідно до [16].

[11] Детальна інформація – за посиланням: https://www.dhs.gov/national-infrastructure-coordinating-center

спираючись на яку потрібно визначити, від кого та від чого необхідно захищати об'єкти КІ, на які загрози (небезпеки) має бути розрахована державна система захисту критичної інфраструктури.

Проте для подальшої розбудови системи захисту КІ потрібно мати апарат, який координуватиме розробку правових, організаційних, науково-методологічних та інших інструментів захисту КІ, проводитиме оперативний аналіз наявних загроз, небезпек і ризиків. З огляду на комплексність питання та широкий спектр завдань подібної структури, це означає, що необхідно створити Національний центр захисту критичної інфраструктури, який має бути сформований як державний орган виконавчої влади (як урядовий центр) [16].

Серед першочергових науково-методологічних завдань цього Центру слід вказати такі: аналіз та оцінка загроз, небезпек та ризиків; визначення проектної загрози об'єктам КІ на державному рівні; формування переліку об'єктів критичної інфраструктури, відповідальність за захист яких лежить і на державі включно.

Водночас при аналізі загроз і ризиків постає низка питань, як-от: які загрози мають обов'язково включатися до проектної загрози; як у проектній загрозі мають ураховуватися несуттєві загрози (тобто загрози, наслідки реалізації яких є прийнятними з точки зору забезпечення безперервності функціонування КІ); як коректно розмежувати проектну та позапроектну загрози (а значить, відповідальність оператора та держави); як адекватно зіставити різні ризики; який ризик можна вважати прийнятним[12] тощо. Відтак автор планує присвятити свої майбутні дослідження пошуку відповідей на ці питання.

[12] Відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» (*див. :* http://zakon2.rada.gov.ua/laws/show/877-16) прийнятний ризик – соціально, економічно, технічно і політично обґрунтований ризик, який не перевищує гранично допустимого рівня. Подібні підходи використовуються й у РФ, зокрема, у документі «ГОСТ Р 53195.1-2008: Безопасность функциональная связанных с безопасностью зданий и сооружений систем» зазначено, що прийнятний ризик (*tolerable risk*) – це «риск, который считается обычным при данных обстоятельствах, на основе существующих в текущий период времени ценностей и возможностей общества и государства». Проте єдиної кількісної характеристики прийнятного ризику немає.

Список використаних джерел

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов ; за заг. ред. О.М. Суходолі. – К. : НІСД, 2016. – 176 с.
2. Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art / G. Giannopoulos, R. Filippini, M. Schimmer. – Luxembourg : Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.
3. Бобро Д.Г. Методологія оцінки рівня критичності об'єктів інфраструктури [Електронний ресурс] // Стратегічні пріоритети. – 2016. – № 3 (40). – С. 77–85. – Режим доступу : http://sp.niss.gov.ua/content/articles/files/11-1485776127.pdf
4. Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Revision 5) [Електронний ресурс] / Серия изданий МАГАТЭ по физической ядерной безопасности, № 13. – Режим доступу : http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481r_web.pdf
5. Обоснование базовой проектной угрозы объекту [Електронний ресурс]. – Режим доступу : http://iteration.su/danger.html#section_2
6. Проблеми оцінки терористичної вразливості та формування паспортів безпеки об'єктів енергетики : аналіт. записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/content/articles/files/pasport_bezpeki-3d468.pdf
7. ФСТЭК России. Методика определения угроз безопасности информации в информационных системах [Електронний ресурс]. – Режим доступу : http://fstec.ru/component/attachments/download/812
8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 4 грудня 2000 р. № 53 (із змінами згідно з наказом Адміністрації Держспецзв'язку від 28 грудня 2012 р. № 806) [Електронний ресурс]. – Режим доступу : www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341
9. Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology. EPRI. 3002001181. December 2013. [Електронний ресурс]. – Режим доступу : https://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf

10. Electric Grid Security and Resilience. Establishing a Baseline for Adversarial Threats. June 2016. [Електронний ресурс]. – Режим доступу : https://energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience – Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf
11. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
12. Бояринцев Александр, Редькин Владимир. Центр анализа уязвимости ЗАО «НПП «ИСТА-Системс». Определение и ранжирование угроз объектам [Електронний ресурс]. – Режим доступу : http://mx1.algoritm.org/arch/71/71_5.pdf
13. Мошкова Р.А. Критерии системы управления экономической безопасностью предприятия железнодорожного транспорта [Електронний ресурс]. – Режим доступу : http://publishing-vak.ru/file/archive-economy-2016-6/6-moshkova.pdf
14. Петрищев И.О., Смагин А.А. Построение моделей угроз и расчетных показателей эффективности комплексной системы безопасности при анализе уязвимости складов нефтепродуктов [Електронний ресурс]. – Режим доступу : http://www.apu.npomars.com/images/pdf/21_4.pdf
15. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі [Електронний ресурс] // Стратегічні пріоритети. – 2015. – № 4 (37). – С. 83–93. – Режим доступу : http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf
16. Суходоля О.М. Щодо створення державної системи захисту критичної інфраструктури : аналіт. записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/content/articles/files/infrastrukt-86de2.pdf

References

1. Sukhodolia, O., Biriukov, D., & Kondratov, S. (Eds.) (2015). *Zelena knyha z pytan zahystu crytychnoi infrastructury v Ukraini [The Green Book on Critical Infrastructure Protection]*. Kyiv: NISS [in Ukrainian].
2. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen [in English].
3. Bobro, D.G. (2015). Metodolohiia otsinky rivnia krytychnosti obiektiv infrastruktury [Methodology of Estimation of Infrastructure Objects Criticality Level]. *Stratehichni priorytety – Strategic Priorities, 3 (40)*, 77–85. *sp.niss.gov.ua*. Retrieved from http://sp.niss.gov.ua/content/articles/files/11-1485776127.pdf [in Ukrainian].
4. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). *IAEA Nuclear Security Series, No. 13*. (n. d.). *pub.iaea.org*. Retrieved from http://www.pub.iaea.org/MTCD/Publications/PDF/Pub1481r_web.pdf [in Russian].
5. Obosnovaniye bazovoy proektnoy ugrozy objektu [Substantiation of Base Design Threat to the Object]. (n. d.). *iteration.su*. Retrieved from http://iteration.su/danger.html#section_2 [in Russian].
6. Problemy otsinky terorystychnoi vrazlyvosti ta formuvannia pasportiv bezpeky obiektiv enerhetyky [Problems of Estimation of Terrorist Vulnerability and Forming of Safety and Security Passports of Energy Objects]. (n. d.). *niss.gov.ua*. Retrieved from http://www.niss.gov.ua/content/articles/files/pasport_bezpeki-3d468.pdf [in Ukrainian].
7. FSTEK Rossii. Metodika opredelenija ugroz bezopasnosti informatsii v informatsionnyh sistemah [FSTEC of Russia. Methodology of Determination of Threats to Safety of Information in the Informative Systems]. (n. d.). *fstec.ru*. Retrieved from http://fstec.ru/component/attachments/download/812 [in Russian].
8. ND TZI 1.4-001-2000. Typove polozhennia pro sluzhbu zahystu informatsii v avtomatyzovanii systemi, zatverdzhene nakazom Departamentu spetsialnyh telekomunikatsiynyh system ta zahystu informatsii Sluzhby bezpeky Ukrainy vid 4 hrudnia 2000 r. № 53 (iz zminamy zhidno z nakazom Administratsii Derzhspetszviazku vid 28 hrudnia 2012 r. № 806) [ND TZI 1.4-001-2000. Typical position about information protection service, ratified by the order of Department of the special telecommunication systems and information protection of Security Service of Ukraine from 2000, December 4, № 53 with changes in obedience to the order of Administration of the special state communication from 2012, Dec. 28 № 806]. (n. d.). *dsszzi.gov.ua*. Retrieved from www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341 [in Ukrainian].
9. Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology. EPRI. 3002001181. December 2013. *energy.gov*. Retrieved from https://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf [in English].
10. Electric Grid Security and Resilience. Establishing a Baseline for Adversarial Threats. June 2016. *energy.gov*. Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf [in English].

11. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. (n. d.). *dhs.gov*. Retrieved from https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf [in English].

12. Boyarintsev, Aleksandr, & Redkin, Vladimir. Tsentr analiza uyazvimosti ZAO «NPP „ISTA-Sistems"». Opredelenje i ranzhirovanje ugroz objektam [Center of analysis of vulnerability JSC «NPP «ISTA-Sistems». Determination and ranging of threats to the objects]. (n. d.). *mx1.algoritm.org*. Retrieved from http://mx1.algoritm.org/arch/71/71_5.pdf [in Russian].

13. Moshkova, R.A. (2016). Kriterii sistemy upravleniya ekonomicheskoy bezopasnostyu predpriyatiya zheleznodorozhnogo transporta [Criteria's of Control System by Economic Security of Railway Transport Enterprise]. *publishing-vak.ru*. Retrieved from http://publishing-vak.ru/file/archive-economy-2016-6/6-moshkova.pdf [in Russian].

14. Petrischev, I.O., & Smagin, A.A. Postroenye modeley ugroz i raschetnyh pokazateley effektivnosti kompleksnoy sistemy bezopasnosti pri analize ujazvimosti skladov nefteproduktov [Construction of Threats Models and Calculation Indexes of Efficiency of the Complex Safety System under the Vulnerability Analysis of Oil Products Storages]. (n. d.). *apu.npomars.com*. Retrieved from http://www.apu.npomars.com/images/pdf/21_4.pdf [in Russian].

15. Bobro, D.G. (2015). Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastruktury [Definition of Evaluation Criteria and Threats to Critical Infrastructure]. *Stratehichni priorytety – Strategic Priorities, 4 (37)*, 83–93. *sp.niss.gov.ua*. Retrieved from http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf [in Ukrainian].

16. Sukhodolia, O. (2017). Schodo stvorennia derzhavnoi systemy zahystu krytychnoi infrastruktury [About Construction of State System of Critical Infrastructure Protection]. *niss.gov.ua*. Retrieved from http://www.niss.gov.ua/content/articles/files/infrastrukt-86de2.pdf [in Ukrainian].