неофіційний переклад

European Commission

JRC SCIENCE AND POLICY REPORT

Методології оцінки ризиків для захисту критичної інфраструктури. Частина II: Новий підхід

Маріанті Теохариду
Георгіос Джаннопулос

2015

Report EUR 27332 EN

Joint Research Centre

Європейська Комісія
Спільний дослідницький центр
Інститут захисту та безпеки громадянина

Контактна інформація
Георгіос Джаннопулос
Адреса Об'єднаний дослідницький центр, Via Enrico Fermi 2749, 21027, Ispra, Italy E-mail: Georgios.Giannopoulos@jrc.ec.europa.eu
Тел: +39 0332 78 6211

Науковий центр JRC https://ec.europa.eu/jrc

EUR 27332 EN

ISBN 978-92-79-49246-4

ISSN 1831-9424 doi:10.2788/621843

Люксембург: Видавничий офіс Європейського Союзу, 2015

Анотація

У цьому звіті описано процес оцінки ризиків для критичної інфраструктури (КІ) на основі робочого документа Генерального директорату з питань надзвичайних ситуацій (DG ECHO), а саме "Керівництва з оцінки ризиків та картографування для управління надзвичайними ситуаціями" та DG HOME "Про новий підхід до Європейської програми захисту критичної інфраструктури, що робить європейську критичну інфраструктуру більш захищеною". В результаті робочого документу співробітників DG ECHO, кілька держав-членів ЄС надали огляд ризиків, де ризик "втрати критичної інфраструктури" був визначений як антропогенний ризик.

Однак ми вважаємо, що в цьому процесі є багато можливостей для вдосконалення, головним чином тому, що критична інфраструктура ще не є ще одним ризиком на рівні держав-членів, але КІ, в свою чергу, підпадають під ризики, які були визначені в державах-членах. У цьому звіті ми визначаємо цю прогалину і пропонуємо методологію, яка базується на іншому підході до ризиків для КІ.

Зміст

Перелік рисунків

Перелік таблиць

Перелік скорочень

CBRN	Хімічна, біологічна, радіологічна та ядерна зброя
CI	Критична інфраструктура
CIP	Захист критичної інфраструктури
CIPRnet	Дослідницька мережа з питань готовності та стійкості критичної інфраструктури
CIPS	Запобігання, готовність та управління наслідками тероризму та інших ризиків, пов'язаних з безпекою
EC	Європейська комісія
ECI	Європейська критична інфраструктура
EISAC	Центр моделювання та аналізу європейських інфраструктур
EPCIP	Центр моделювання та аналізу європейських інфраструктур
EU	Європейський Союз
GIS	Географічні інформаційні системи
GRRASP	Платформа оцінки геопросторових ризиків та стійкості
ICT	Інформаційно-комунікаційні технології
ISO	Міжнародна організація зі стандартизації
MS	Держави-члени
NRA	Національні оцінки ризиків
RA	Оцінка ризиків
RVA	Аналіз ризиків та вразливостей
UNISDR	Управління ООН зі зменшення небезпеки стихійних лих

Висновки

Цей звіт описує методологію оцінки ризиків для критичної інфраструктури (КІ), засновану на двох робочих документах, підготовлених співробітниками DG ECHO "Оцінка ризиків і картографічні рекомендації для управління надзвичайними ситуаціями" [1] і DG HOME "Новий підхід до Європейської програми захисту критичної інфраструктури. Підвищення безпеки європейських об'єктів критичної інфраструктури". У результаті робочого документу співробітників DG ECHO кілька держав-членів ЄС надали огляд ризиків, де ризик "втрати критичної інфраструктури" був визначений як антропогенний ризик.

Однак ми вважаємо, що в цьому процесі є багато можливостей для вдосконалення, головним чином тому, що критична інфраструктура ще не є ще одним ризиком на рівні держав-членів, але КІ, в свою чергу, підпадають під ризики, які були визначені державами-членами. Безумовно, це є методологічною прогалиною, і, спираючись на результати звіту про огляд оцінки ризиків ([2]), ми пропонуємо тут методологію, яка підводить підсумки цих політик і надає ключові елементи, які дозволять запровадити подібний і порівнянний процес оцінки ризиків для КІ.

Звіт складається з п'яти розділів.

Перший розділ звіту є вступом до теми, в якому представлені законодавчі елементи, що вже існують, елементи спільної мови для CIP, а також способи подолання розриву між політиками ЄС. Другий розділ містить методологічні висновки національних оцінок ризиків, які були проведені відповідно до керівних принципів, наданих DG ECHO у Робочому документі для персоналу.

Третій розділ містить аналіз прогалин у цих оцінках ризиків, який потім використовується в четвертому розділі для розробки методології RA, запропонованої в цьому звіті.

Насамкінець, ми завершуємо цей звіт деякими політичними рекомендаціями та заходами щодо впровадження RA критично важливих об'єктів інфраструктури, які можуть бути застосовані як на національному, так і на міжнародному рівнях.

Розділ 1

Вступ

1.1 Передумови

У 2010 році Європейська Комісія видала керівні принципи з оцінки ризиків для підтримки держав-членів у підготовці національних оцінок ризиків для управління надзвичайними ситуаціями[1]. Після публікації цих керівних принципів та на основі результатів роботи держав-членів з оцінки ризиків у 2014 році Комісія підготувала огляд природних та техногенних ризиків в ЄС [3]. У деяких з цих перших, національних результатах оцінки ризиків, було виявлено ризик "втрати критичної інфраструктури". Втрата "основних" або "життєво важливих послуг", які надаються КІ, також враховується в кількох національних оцінках ризиків як індикатор впливу.

Директива ECI [4] підкреслює важливість оцінки ризиків для критичної інфраструктури на європейському рівні. Однак, в рамках цієї Директиви не було розроблено жодної методології RA, і держави-члени дотримуються своїх власних методологій. За винятком наскрізних критеріїв, тобто (a) жертв, (b) економічних наслідків і (c) суспільних наслідків, які слугують базовим орієнтиром для оцінки впливу, держави-члени не прийняли конкретної методології для оцінки ризиків для своєї критичної інфраструктури. Це означає, що порівняння результатів оцінки ризиків між державами-членами не є можливим. Це також стосується транскордонних оцінок ризиків, що включають декілька ризиків, які базуються на національних результатах. Крім того, Директива має галузеву сферу застосування, яка стосується лише енергетичного та транспортного секторів, що не дозволяє оцінити всі життєво важливі послуги, які надаються КІ.

У серпні 2013 року був опублікований робочий документ Комісії щодо нового підходу до Європейської програми захисту критичної інфраструктури "Зробити європейські критичні інфраструктури більш безпечними" [5]. У ньому викладено ініціативи Комісії щодо методологій оцінки ризиків, головним чином в рамках програми CIPS. Документ визначає межі галузевих методологій, коли необхідно розглядати міжгалузеві загрози, такі як ті, на які спрямовані керівні принципи DG-ECHO [1]. Натомість пропонується системний підхід, який передбачає спільну роботу з чотирма європейськими КІ: Євроконтролем, Galileo, мережею передачі електроенергії та газотранспортною мережею. Розробка інструментів для оцінки ризиків зосереджена на цих чотирьох пілотних проектах. Крім того, прогалиною є методології оцінки ризиків для подій з низькою ймовірністю і високими наслідками; такі методології можуть бути застосовані в майбутніх "стрес-тестах" для критично важливих об'єктів інфраструктури, як це розглянуто в роботі [6].

У Звіті Всесвітнього економічного форуму за 2015 рік [7] "Порушення критичної інформаційної інфраструктури" визнано 7-м у списку найбільших ризиків у світі з точки зору впливу. Це пов'язано з тенденцією "гіперзв'язності", яка асоціюється з технологічними ризиками, серед яких розглядається і втрата КІ. У звіті підкреслюється той факт, що ризики не можна оцінювати і розглядати ізольовано. Між ними існують причинно-наслідкові зв'язки, а в деяких випадках вони мають спільні основні тенденції (або вразливості). Така складність розгляду ризиків, ймовірності та потенційних наслідків піднімає питання про застосування підходу, що базується на множинних ризиках, а також про "завчасну готовність на глобальному, регіональному, національному та місцевому рівнях".

1.2 Усунення прогалин у політиці Комісії на технічному рівні

Як зазначалося вище, декілька держав-членів включили "втрату критичної інфраструктури" до переліку найбільших національних ризиків, що також підтверджується іншими світовими звітами. На нашу думку, це досить неоднозначно, оскільки багато з визначених ризиків становлять загрозу для КІ і можуть завдати прямої шкоди самій КІ, що опосередковано може призвести до порушення життєво важливих послуг. В огляді ризиків, пов'язаних з MS, втрата КІ визначена як антропогенний ризик (незловмисний), який має вплив на суспільство, хоча в принципі може виникнути через різні загрози. Це також може бути каскадним ефектом інших порушень КІ через загрози як природного, так і антропогенного характеру. Це лише незначною мірою зачіпається у звіті. Здається, що для небезпек, не пов'язаних з діяльністю людини, аспект втрати КІ не розглядається повністю, за винятком ризиків Natech для певних категорій інфраструктури (якщо тільки вони не включені в опосередкований вплив на суспільство). Таким чином, загальний вплив на суспільство через природні загрози, здається, недооцінюється. Крім того, методологічно не враховуються взаємозалежності, які мають відношення до КІ і можуть спричинити вторинні ефекти у випадку переривання надання послуг.

Метою запропонованої роботи є дослідження можливості об'єднання технічних елементів, описаних у цих політичних і законодавчих документах, для досягнення спільної методології. Такі зусилля дозволили б створити основу для оцінки ризиків для критично важливих інфраструктурних об'єктів, руйнування яких матиме вплив на європейське суспільство. Здається, що ці документи доповнюють один одного в тому сенсі, що:

- Директива ECI надає базові рекомендації щодо енергетичних і транспортних КІ та способів визначення найбільш важливих європейських КІ. Критерії стосуються впливу втрати інфраструктури як способу визначення їх пріоритетності. Ці керівні принципи не відповідають повній національній оцінці ризиків, але охоплюють ранні етапи управління ризиками шляхом "визначення контексту" (визначення сфери застосування) та "аналізу наслідків" (на етапі аналізу ризиків) [8]. По суті, директива рекомендує державам-членам спосіб визначення своїх активів (КІ), які потребують захисту, як перший крок до управління ризиками.

- Робочий документ співробітників DG HOME ([5]) не містить детальних методологічних міркувань щодо проведення оцінки ризиків КІ. Він пропагує системний підхід на противагу секторальному підходу та зосереджується на загрозах, які можуть спричинити значні наслідки для КІ.

- Політика DG HOME зосереджена на запобіганні, готовності та реагуванні в рамках захисту критичної інфраструктури. Однак для того, щоб мати обґрунтований підхід до цих елементів (головним чином, до запобігання та готовності), необхідно мати надійну методологію оцінки ризиків, яка б ставила загрози, вразливості і, нарешті, ризики в правильні рамки.

- Керівні принципи Генерального директорату з питань надзвичайних ситуацій ([1]) зосереджені на визначенні національних ризиків (небезпек). Ці настанови пропонують деякі методологічні елементи для оцінки ризиків. Однак вони не були адаптовані до критичної інфраструктури і не містили детальних рекомендацій щодо оцінки впливу.

Ми прагнемо використати методологічні елементи робочого документа для персоналу, виданого DG ECHO ще в 2010 році, і зіставити його з оцінкою ризиків критичної інфраструктури, збагативши його елементами, що мають відношення до КІ (наприклад, взаємозалежності). Поєднання цього звіту з "оглядом ризиків" дозволяє отримати більш чітке уявлення про те, як держави-члени інтерпретували та впроваджували рекомендації. Ми передбачаємо, що цей звіт також буде корисним для проведення оцінки ризиків у пілотних проектах переглянутого Плану дій, а також для майбутніх національних оцінок ризиків з більш чітким і сильним фокусом на КІ. Пілотні проекти зосереджені на секторі і мають дуже специфічний мандат, тоді як запропонована тут методологія RA поширює вплив інфраструктурних порушень на все суспільство. Як наслідок, ці два елементи є взаємодоповнюючими і, безумовно, не взаємовиключними.

Ключовим елементом, який випливає з огляду вищезазначених документів, є те, що, окрім відсутності спільної методології, держави-члени не мають спільної термінології, особливо щодо оцінки ризиків, пов'язаних з КІ. Різноманітність термінів та визначень чітко відображена в CIPedia, яка є колекцією термінів та визначень, пов'язаних з КІ1. Картина стає ще складнішою, коли визначення, пов'язані з КІ, повинні також відповідати термінології DG-ECHO або UNISDR2, яка в основному зосереджена на оцінці ризиків катастроф.

Ми усвідомлюємо, що все ще далекі від того, щоб запропонувати методологію, якої повинна дотримуватися кожна держава-член. З цієї причини ми прагнемо надати уявлення та рекомендації. Такі рекомендації на рівні ЄС могли б визначити необхідні компоненти, які мають бути включені в оцінку ризиків, або формат вихідних даних про ризики, щоб полегшити порівняння результатів.

Враховуючи рівень зрілості національних підходів до оцінки ризиків, що застосовуються країнами-членами ЄС, поки що неможливо обговорювати методи пом'якшення або обробки ризиків. Цей звіт буде зосереджений на методологічних міркуваннях національної оцінки ризиків стосовно КІ.

1.3 Визначення

У цьому розділі наведено визначення використаних термінів. В основному вони були отримані з CIPedia[3].

Критична інфраструктура - це об’єкт, система або її частина, розташована в державах-членах, яка має важливе значення для підтримки життєво важливих суспільних функцій, охорони здоров'я, безпеки, екологічного або соціального благополуччя людей, і переривання або руйнування якої матиме значний вплив на державу-члена в результаті нездатності підтримувати ці функції. [4].

Наслідок. Термін "наслідок" не є чітко визначеним у літературі з питань CIP. Хоча ISO визначає наслідок як "результат події, що впливає на цілі", це загальне визначення не робить різниці між наслідками для самої системи або критичної інфраструктури, для людей, для навколишнього середовища або для економіки. Таке розмежування необхідне, оскільки за змістом Директиви ECI [4] оцінка наслідків для людей, довкілля та економіки необхідна відповідно до наскрізних критеріїв. Крім того, наслідки каскадних впливів на інші інфраструктури також можуть потребувати розмежування та оцінки. З цієї причини в цьому документі ми спробуємо чітко розмежувати різні форми і типи наслідків

1CIPedia - це подібна до Вікіпедії онлайн-спільнота, що зосереджується на питаннях захисту критичної інфраструктури (ЗКІ) та стійкості, надана проектом ЄС 7РП CIPRNet, детальніше на http://www.cipedia.eu.

2Організація Об'єднаних Націй зі зменшення небезпеки стихійних лих, Термінологія зі зменшення небезпеки стихійних лих: http://www.unisdr.org/we/inform/terminology

[3]http://www.cipedia.eu

Ми також будемо називати **вплив** масштабом наслідків небезпеки або загрози. У цьому документі ми будемо розрізняти вплив на КІ (прямі наслідки для КІ), каскадний вплив на КІ (непрямі наслідки для КІ через вихід з ладу іншої КІ) та вплив на суспільство (наслідки для людей, довкілля та економіки).

Небезпека. Ми приймаємо визначення UNISDR, згідно з яким небезпека - це будь-яке "небезпечне явище, речовина, людська діяльність або стан, що може спричинити загибель людей, травми або інші наслідки для здоров'я, майнову шкоду, втрату засобів до існування та послуг, соціальну та економічну дезорганізацію або шкоду навколишньому середовищу" [9]. У цьому документі ми використовуємо цей термін як синонім поняття "загроза".

Стійкість. Термін "стійкість" означає здатність готуватися та адаптуватися до умов, що змінюються, а також витримувати та швидко відновлюватися після збоїв. Стійкість включає в себе здатність протистояти і відновлюватися після навмисних атак, нещасних випадків або природних загроз чи інцидентів [10]. Однак, стійкість все ще є відносно новим терміном, і тривають дебати щодо його точного визначення.

Ризик. Це проблематичний термін, оскільки він використовується або відповідно до традиційного визначення ISO, або як синонім небезпеки чи загрози. Ми будемо розглядати ризик як "поєднання наслідків події або небезпеки та пов'язаної з ними ймовірності її виникнення" [11].

Ризик менеджмент це систематичне застосування політик, процедур і практик управління до діяльності з інформування, консультування, встановлення контексту та ідентифікації, аналізу, оцінювання, лікування, моніторингу та перегляду ризиків (на основі Настанови ISO 73:2009 [12]).

Оцінка ризиків відноситься до загального процесу:

- *ідентифікації ризиків* - процес пошуку, визнання та опису ризиків,
- *аналіз ризиків* - процес розуміння природи ризику та визначення рівня ризику, та
- *оцінка ризиків* - процес порівняння результатів аналізу ризиків з критеріями ризику для визначення того, чи є ризик та/або його величина прийнятними або толерантними.

Лікування ризиків відноситься до будь-якого процесу, спрямованого на зміну ризику4 і може включати:

- уникнення ризику шляхом прийняття рішення не починати або не продовжувати діяльність, яка спричиняє ризик,
- прийняття або збільшення ризику для того, щоб скористатися можливістю,
- усунення джерела ризику,
- зміна ймовірності,

[4]У сфері CIP цей термін іноді називають "пом'якшенням ризиків", "усуненням ризиків", "запобіганням ризикам" і "зниженням ризиків".

- зміна наслідків,
- розподіл ризику з іншою стороною або сторонами (включаючи контракти та фінансування ризику), та
- утримання ризику шляхом прийняття обґрунтованого рішення.

Оцінка окремих ризиків - визначають одиничний ризик (тобто ймовірність і наслідки) однієї конкретної небезпеки (наприклад, повені) або одного конкретного типу небезпеки (наприклад, затоплення), що виникає в певній географічній зоні протягом певного періоду часу [1].

Оцінка множинних ризиків - визначити загальний ризик від декількох небезпек, що виникають одночасно або незабаром одна за одною, оскільки вони залежать одна від одної або спричинені однією і тією ж пусковою подією чи небезпекою; або просто загрожують одним і тим же елементам, що перебувають у зоні ризику (вразливим/ підданим впливу елементам), без хронологічного збігу [1].

Сценарій - гіпотетична ситуація, що складається з ідентифікованої загрози або небезпеки, об'єкта, на який впливає ця небезпека, та пов'язаних з нею умов, включаючи наслідки, коли це доречно [13].

Розділ 2

Національні оцінки ризиків: методологічні висновки

Для того, щоб виявити методологічні прогалини в оцінці ризиків КІ державами-членами, ми спочатку проаналізуємо, які загрози були визначені державами-членами та як вони були оцінені з точки зору ймовірності та впливу. У кількох випадках держави-члени використовували сценарний підхід, тому ми також прокоментуємо елементи, необхідні для проведення сценарного аналізу з більш повним відображенням та аналізом КІ.

2.1 Рекомендації щодо оцінки ризиків

Керівні принципи DG-ECHO 2010 року слідують стандартному підходу ISO31000, де ризик розглядається як "поєднання наслідків події або небезпеки та пов'язаної з ними ймовірності її виникнення" [11]. Коли при оцінці ризику розглядаються питання запобігання та готовності до небезпеки, то ризик може бути кількісно визначений як "функція ймовірності виникнення небезпеки, експозиції (загальна величина всіх елементів, що піддаються ризику) та вразливості (конкретний вплив на експозицію)".

Для візуалізації результатів у рекомендаціях обрано матрицю ризиків 5×5, наприклад, таку, що представлена на рисунку нижче.

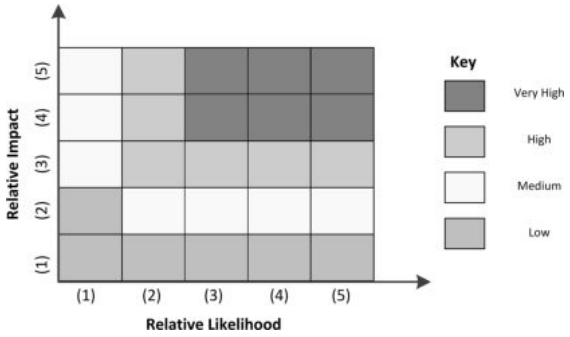

Рисунок 2.1: *Приклад матриці ризиків [1]*

Оцінка ризиків повинна проводитися на основі трьох різних критеріїв впливу: людські, економічні (включаючи екологічні) та політичні/соціальні наслідки; кількісно для перших двох категорій, наприклад, кількість смертей/поранень або витрати в євро, і з використанням якісної шкали для третьої категорії. Держави-члени повинні представити свої оцінки ризиків для кожного сценарію в неагрегованому вигляді, тобто у вигляді трьох різних матриць ризиків (див. Рис. 2.1) - по одній для кожної категорії наслідків. Часовий горизонт для оцінок було рекомендовано розробити від початкових 1-5 років, тоді як держави-члени можуть включати ризики, передбачені на найближчі 25-35 років.

Крім того, в настановах описується вимір транскордонних ризиків, здійснення багатовимірного аналізу ризиків або аналізу ризиків декількох інцидентів, які відбуваються незалежно або як наслідок інших інцидентів. Нарешті, в настановах описується важливість створення карт ризиків, що відображають просторовий розподіл основних загроз, активів, що підлягають захисту, та їхню відповідну вразливість, за допомогою географічних інформаційних систем (GIS). Ці карти можуть бути використані на більш пізньому етапі для створення агрегованих карт ризиків (транскордонних або мультиризикових).

Необхідність спільного розуміння термінології та методології ризиків в ЄС також підкреслюється в [14]. Цей документ також закликає країни-члени ЄС визначати, аналізувати та оцінювати сценарії з одним ризиком, а в якості наступного кроку - розглядати сценарії з декількома ризиками. Методологічно слід розглядати як якісні, так і кількісні методи.

2.2 Результати впровадження

Всі вищезазначені рекомендації створюють умови для більш уніфікованого підходу з боку держав-членів. Незважаючи на використання загальної матриці ризиків 5×5, порівняння результатів все ще залишається складним, оскільки після імплементації країни-члени застосовують різні шкали ймовірності та впливу, часові рамки, різну термінологію та сценарії ризиків. Хоча таке розмаїття підходів збагачує загальний рекомендований підхід, більш уніфікований підхід дозволив би оцінювати транскордонні ризики та краще координувати управління ризиками в межах ЄС. Крім того, питання втрати КІ та оцінки пов'язаних з цим ризиків не розглядаються державами-членами поглиблено, як ми побачимо в наступних розділах.

2.2.1 Небезпеки

Із загального переліку небезпек, визначених у NRA, найбільш важливими є наступні [3]:

- Природні небезпеки
  - Повені
  - Несприятливі погодні умови
  - Дикі/лісові пожежі
  - Землетруси
  - Пандемії/епідемії
  - Епідемії сільськогосподарських тварин
- Техногенні небезпеки
  - Не зловмисні
    - Аварії на виробництві
    - Ядерні/радіологічні аварії
    - Нещасні випадки на транспорті
    - **Втрата критичної інфраструктури**
  - Зловмисні
    - Кібер атаки
    - Терористичні атаки

Ми бачимо, що втрата або порушення роботи критичної інфраструктури розглядається окремо як техногенна небезпека (ненавмисна, аварія). Включення втрати КІ як окремого ризику підкреслює той факт, що держави-члени вважають ймовірність такої події важливою. Зокрема, цей ризик визначили сім держав-членів, а саме: Чеська Республіка, Німеччина, Ірландія, Нідерланди, Польща, Швеція та Велика Британія. Частково це можна пояснити існуванням Директиви EPCIP та Директиви ECI, які підвищили обізнаність щодо важливості порушення роботи КІ та потенційного впливу на суспільство.

Таблиця 2.1: *Виявлено ризики, пов'язані з КІ*

Країна	***Рівень ризику***	***Використані терміни***
CZ	Високий	Порушення роботи критичної інфраструктури
DE	-	Виведення з ладу критично важливої інфраструктури
IE	Високий	Втрата критично важливої інфраструктури
PL	Середній	Перебої з постачанням електроенергії, палива, природного газу
SE	Дуже Високий	Перебої з постачанням продовольства через дефіцит палива
UK	Високий	Атаки на інфраструктуру
NL	Дуже Високий	Збій у роботі IP-мережі, зловмисне тривале відключення електроенергії
	Високий	Національне відключення електроенергії, зловмисне відключення електроенергії
	Середній	Зловмисний збій газопостачання

Згідно зі звітом і як показано в таблиці вище, Німеччина, Ірландія та Чеська Республіка розглядають втрату КІ в загальних рисах, тоді як Польща, Нідерланди, Швеція та Велика Британія зосереджуються на перебоях в енергопостачанні, пов'язаних із втратою або пошкодженням інфраструктури, "необхідної для підтримання життєво важливих суспільних функцій". Нідерланди також посилаються на збої в роботі IP-мережі, беручи до уваги сектор ІКТ. Що стосується транспортного сектору (Директива ECI), було враховано кілька аварій, пов'язаних з транспортом (DK, EE, IE, NL, NO, SE, SI, UK), але без прямого посилання на КІ.

Наслідки для громадян, що виникають внаслідок переривання або пошкодження послуг, що надаються КІ, залежать від багатьох факторів (тривалості, часу виникнення, наявності засобів контролю для пом'якшення наслідків тощо), але потенційно можуть спричинити вплив на суспільство (добробут громадян, економічні наслідки та ін.). Однак термінологія, що використовується, залишається неоднозначною. Хоча технічний збій і подальша недоступність КІ може статися через технічну вразливість, використання терміну "втрата КІ" не обов'язково відображає однакове значення у всіх сценаріях, і це зауваження береться до уваги NRA Німеччини під час розробки сценаріїв.

Інша проблема полягає в тому, що відповідно до своїх національних політик, держави-члени не включають однакові типи КІ (сектори) до своїх оцінок, а також не приділяють однакової уваги всім типам порушень КІ.

Залежності небезпек. Залежність між природними загрозами враховують у своїх оцінках лише деякі держави-члени [3]. Як показано в Таблиці 2.2, держави-члени врахували підвищену ймовірність конкретних природних загроз через виникнення інших природних загроз.

Втрата КІ також може бути прямим наслідком кількох небезпек і може спричинити додатковий вплив на суспільство, який необхідно враховувати, але, водночас, не переоцінювати через подвійну кількісну оцінку.

Таблиця 2.2: *Залежність або кореляція між небезпеками*

Небезпека	***Каскадна або корельована небезпека***	***Країна***
Несприятливі погодні явища	Повінь	DK, NO, RO, HU, UK
	Зсуви грунту	IT
	Лісові пожежі	HU, IE, LT
	Забруднення, **втрата КІ**	DK, LT, SE, NO
	Нещасні випадки на транспорті	
Землетруси	Зсуви грунту	HU, IT
	Цунамі	EL
Landslides, Earthquakes, Volcanos	Нещасні випадки на транспорті	NO, IT, EL, UK
Ядерні, хімічні та транспортні аварії, **втрата КІ**	Зараження харчових продуктів, забруднення	DK, LT, UK, NO
	Терористичні та кібер атаки	NO, UK
втрата КІ	Повінь, забруднення, **втрата КІ**, Пандемії	UK, IE
		DK
Забруднення	Пандемії	EE, SE

Питання каскадних ефектів частково розглядається в деяких NRA. Насправді, вплив на критичну інфраструктуру та її послуги може розглядатися при оцінці ризиків інших природних і техногенних загроз як частина структури сценарію, як це має місце у випадку NRA, проведеної Німеччиною та Данією. Ми також спостерігаємо, що втрата КІ враховується при оцінці ризиків Natech. Наприклад, втрата КІ може відбутися з більшою ймовірністю через суворі погодні явища, зсуви, землетруси або виверження вулканів (див. Таблицю 2.2).

Більше того, деякі держави-члени виявляють кореляцію між втратою КІ та іншими ризиками. Приклади включають зв'язок між втратою КІ та підвищеним ризиком зараження, забрудненням навколишнього середовища, а також подальшим каскадним впливом на інші КІ в різних секторах. Втрата КІ також може бути пов'язана з підвищеним ризиком терористичних і кібератак. Нарешті, це може вплинути на ризики пандемії через нестачу робочої сили.

2.2.2 Критерії ймовірності/вірогідності

Якщо ми звернемося до детальних результатів огляду ризиків ЄС5 , то побачимо, що кілька держав-членів покладаються на напівкількісні шкали, тобто від "дуже низького/дуже рідкісного (1)" до "дуже високого/дуже ймовірного (5)", тоді як кілька держав-членів пов'язують шкалу з частотою виникнення. Приклади підходів включають частоту одного або декількох інцидентів у різних часових шкалах (CZ, IE, LT, NO, PL, HU) або ймовірність виникнення протягом 1 року (EE, EL). Норвегія також розглядає навмисні події і те, чи сприймається загроза як ймовірна чи ні, з точки зору мотивації.

Хоча ймовірність настання конкретної загрози оцінюється державою-членом (включаючи в деяких випадках ймовірність втрати КІ), цей показник відноситься до початкової ймовірності реалізації сценарію ризику. Однак ймовірність того, що подія завдасть шкоди (a) конкретному КІ або (b) залежним КІ, не оцінюється. Такий аналіз вимагає детального відображення потенційних ланцюгів залежності між КІ [15, 16]. Ймовірність пошкодження однієї або декількох КІ можна оцінити на основі попередніх інцидентів, рівня вразливості КІ до ініціюючої загрози та/або до втрати послуг іншої КІ.

Як варіант, можна припустити найгірший сценарій, коли всі залежні КІ та їхні послуги виходять з ладу, незважаючи на наявність механізмів стійкості. Тоді загальний ефект втрати можна оцінити з точки зору впливу.

[5] Додаток 4(b) of [3]

Це також вимагає детального зображення залежностей. Оцінка впливу не є простим процесом, оскільки вплив не повинен бути надмірно запізнілим (через подвійні розрахунки). Більше того, коли виникають взаємні залежності, загальний ефект початкової події може бути посилений, а процес відновлення - ускладнений.

2.2.3 Критерії впливу

Для цілей керівних принципів DG-ECHO було визначено три типи впливу:

- Вплив на людину (у цифрах);
- Економічні та екологічні впливи (в євро);
- Політичні/соціальні впливи.

Політичні/соціальні наслідки, як правило, оцінюються за напівкількісною шкалою, що складається з кількох класів, наприклад, (1) обмежений/незначний, (2) незначний/значний, (3) помірний/серйозний, (4) значні/ дуже серйозні, (5) катастрофічні. Для того, щоб зробити класифікацію таких впливів вимірюваною, країни-члени ЄС прийняли власні набори критеріїв, тоді як інші частково імплементували ці керівні принципи. Наприклад, кілька держав-членів не пропонують оцінки впливу своїх сценаріїв або опускають конкретні критерії, особливо політичні/соціальні, які важче піддаються кількісній оцінці.

Рекомендований підхід відповідає наскрізним критеріям Директиви ECI, а саме:

(a) критерій людських жертв (оцінюється з точки зору потенційної кількості смертельних випадків або поранень);

(b) критерій економічних наслідків (оцінюється з точки зору значущості економічних втрат та/або погіршення якості продукції або послуг; включаючи потенційний вплив на навколишнє середовище);

(c) критерій суспільних наслідків (оцінюється з точки зору впливу на довіру громадськості, фізичного страждання та порушення повсякденного життя, включаючи втрату основних послуг).

По суті, рекомендації щодо оцінки впливу є сумісними і дуже схожими. Однак їх виконання чітко демонструє неоднозначність термінології [3]. Лише декілька держав-членів (EE, EL, LT, IE) намагаються врахувати вплив втрати КІ двома основними способами:

- як засіб вимірювання політичних або соціальних наслідків (наприклад, втрата "життєво важливих послуг"):
  - для різних рівнів роботи (часткове або повне порушення),
  - для різних часових рамок,
  - для різних географічних діапазонів,
- або як засіб вимірювання економічних втрат (наприклад, IE перейменовує критерій на "інфраструктура").

По суті, втрата КІ безпосередньо призводить до втрати життєво важливих послуг і впливає на громадян. Однак, необхідно оцінювати не тільки соціальні наслідки небезпеки, але й шкоду, завдану КІ, а також подальшу втрату послуг (і відповідні наслідки для громадян).

Якщо ми також розглянемо залежності між КІ, то цей процес включає не один крок, а декілька, пов'язаних з непрямими втратами КІ та додатковими соціальними наслідками. З квітня 2015 року Нідерланди оновили дві категорії впливу, що використовуються для NRA [17]:

- Категорія А: щонайменше вплив на одну з наступних чотирьох категорій впливу:
  - Фізичний вплив: > 10 000 загиблих, важкопоранених або хронічно хворих
  - Економічний вплив: > 50 000 млн. євро збитків або 5,0% зниження реального доходу
  - соціально-психологічний вплив: > 1 мільйон людей зазнають емоційного впливу або мають серйозні проблеми з виживанням у суспільстві
  - ***каскадний вплив***: цей збій спричиняє збій у роботі щонайменше двох інших (критичних) секторів [6]

- Категорія В: щонайменше вплив на одну з наступних трьох категорій впливу:
  - Фізичний вплив: > 1.000 загиблих, важкопоранених або хронічно хворих
  - Економічний вплив: > 5.000 євро збитків або 1.0% зниження реального доходу
  - Соціально-психологічний вплив: > 100.000 мільйон людей зазнають емоційного впливу або мають серйозні проблеми з виживанням у суспільстві

Ми бачимо, що за критерієм високого рівня (категорія А) оцінюються каскадні впливи з точки зору секторів, на які вони впливають. Це свідчить про те, що принаймні одна держава-член розглянула вищезазначений аргумент щодо оцінки каскадних впливів.

[6] Зауважте, що умови, за яких сектор вважається провальним, залишаються незрозумілими в цьому документі [17].

Розділ 3

Виявлені прогалини

У цьому розділі ми наводимо наші спостереження щодо поточних методів та результатів NRA, про які повідомляють країни-члени ЄС [3], з особливим акцентом на КІ. Ми передбачаємо національну оцінку ризиків із сильним акцентом на CIP, а саме CI-rich NRA. Такий підхід дозволить встановити тісніші зв'язки на рівні ЄС у сфері управління надзвичайними ситуаціями (DG-ECHO) та захисту критичної інфраструктури (DG-HOME).

Розмежування термінів. Однією з основних проблем існуючих підходів є те, що втрата КІ розглядається і як загроза, і як наслідок. Це призводить до відсутності ясності, коли йдеться про оцінку ризиків, як з точки зору результатів, так і з точки зору їх представлення. Це вказує на те, що потрібен більш чіткий перелік загроз.

Непорівнянність результатів. Загалом, при порівнянні різних загроз і відповідних сценаріїв ризику кількісне порівняння не завжди можливе через різну природу аналізованих ризиків. При розгляді подібних сценаріїв ризику в різних державах-членах та їхніх методологій NRA можна провести деякі порівняння. З цією метою було б корисно, якби держави-члени використовували подібні методи, особливо щодо кількісної оцінки ймовірності/впливу загрози. У попередньому розділі ми визначили декілька підходів щодо типу та масштабу впливів, часових рамок тощо.

Наведене вище спостереження є загальним; воно стосується оцінок, орієнтованих на катастрофи, навіть без урахування конкретних елементів критичної інфраструктури. При розгляді CI-rich NRA, відсутність сумісності між методологіями посилюється, оскільки це є невід'ємною складнішою проблемою для розв'язання.

Відсутність моделювання та аналізу залежностей. Якщо ми хочемо застосувати метод оцінки ризику, який враховує як залежності між КІ, так і прямі чи опосередковані наслідки загроз, то метод аналізу сценарію ризику повинен включати більше кроків та ітерацій, як показано на Рисунку 3.1.

Ми бачимо, що після імплементації керівних принципів DG-ECHO державам-членам довелося вирішувати складну проблему залежності як між загрозами, так і між ураженими КІ. Це чітко представлено в Таблиці 2.2, де лише декілька держав-членів намагалися врахувати такі кореляції між виникненням загроз, у тому числі втратою КІ.

"Слабкий аналіз наслідків". В ідеалі аналіз наслідків повинен враховувати як прямі, так і непрямі наслідки. Як приклад прямих наслідків, при розгляді сценарію небезпеки повені, можна виділити наступні можливі порушення [18]:

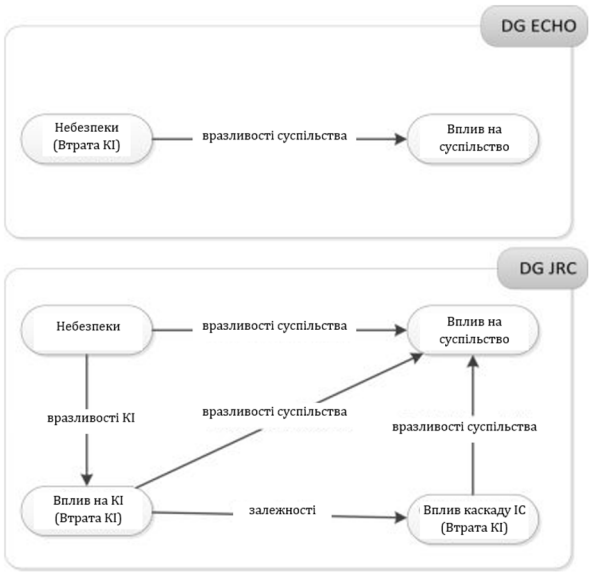

Рисунок 3.1: *Порівняння підходів з одним ризиком*

- транспортні перебої через аварії, пов'язані з повенями (сходження з рейок, зіткнення автотранспорту, зіткнення морських суден, обвалення або переповнення структурних елементів, наприклад, тунелів, мостів, аеропортів і т.д.),
- перебої в транспортному сполученні через масштабну евакуацію цивільного населення, що спричиняє затори на дорогах,
- перебої у водопостачанні або забруднення питної води чи інші загрози для здоров'я,
- інциденти з небезпечними речовинами (CBRN) через пошкодження конструкцій/підтоплення об'єктів,
- інциденти з небезпечними речовинами (CBRN) внаслідок аварій на транспортних засобах, що їх перевозять,
- аварії на каналізаційних системах,
- перебої в електропостачанні
- перебої в роботі телекомунікацій,
- перебої в роботі медичних закладів через нестачу електроенергії, затоплення, збільшення кількості пацієнтів або нездатність персоналу чи медикаментів дістатися до місця події,
- перебої в роботі промисловості чи бізнесу через перебої з електропостачанням чи зв'язком.

Ми бачимо, що повінь може завдати численних прямих збитків КІ різних секторів (наприклад, транспорт, ІКТ, енергетика тощо), окрім безпосередніх соціальних наслідків. Хоча цей перелік не є вичерпним, і ці порушення навряд чи відбудуться одночасно, він демонструє складність відображення прямого і непрямого впливу сценарію на національну критичну інфраструктуру. Розрахунок загального впливу сценарію на суспільство є складним процесом, оскільки наслідки можуть посилюватися через паралельні порушення або через те, що нелегко уникнути подвійних розрахунків очікуваних наслідків. Випадок попередніх інцидентів може дозволити отримати більш реалістичні оцінки, але це не завжди так, коли розглядаються невідомі національні ризики.

Відсутність оцінки вразливостей. Вразливості можуть бути пов'язані з фізичними (наприклад, відсутність бар'єрів або сигналізації), кібернетичними (наприклад, відсутність брандмауера) або людськими (наприклад, непідготовлені охоронці) факторами [13]. Оцінка вразливості має бути частиною повної оцінки ризиків. Вона включає оцінку конкретних загроз або небезпек на різних рівнях аналізу: на рівні КІ або активів, на рівні системи або мережі (наявність залежностей або ймовірність каскаду) або на рівні суспільства (ступінь вразливості до небезпеки).

Відсутність транскордонних сценаріїв. КІ є складними, взаємозалежними системами (або системами систем), і наслідки їх порушень можуть виходити за межі географічних кордонів держави-члена. У звіті [3] представлено загальноєвропейський сценарій та матрицю для кожної з розглянутих загроз. Такі загальноєвропейські сценарії можуть ґрунтуватися на підході до побудови сценаріїв, застосованому в національних оцінках, і дозволять зосередити увагу в цьому огляді на ризиках, що мають транскордонний вимір. Однак вищезгадані прогалини (порівнянність результатів, неоднозначність термінів, необхідність аналізу залежностей) ще більше ускладнюють розробку таких сценаріїв.

Також слід враховувати, що "включення декількох сценаріїв, які містять одну й ту саму подію, може призвести до подвійного підрахунку ризику"[13]. Крім того, деякі інші інфраструктури можуть зіткнутися з загальними причинами або каскадними збоями, які посилюють вплив і складність сценарію.

Розділ 4

Новий підхід: Методологія оцінки ризиків та стійкості критично важливих інфраструктур та систем (CRISRRAM)

У цьому розділі ми прагнемо запропонувати методологію, яка враховує методологічні висновки та прогалини, визначені в попередніх розділах. Основними характеристиками запропонованої методології є те, що вона використовує системний підхід і спрямована на вирішення проблем на рівні активів, системному рівні та рівні суспільства. Крім того, вона дотримується підходу до всіх видів небезпек, що є важливим елементом, враховуючи, що політика DG ECHO більше зосереджена на стихійних лихах, тоді як політика DG HOME - на безпеці та техногенних загрозах.

Те, що описано на Рисунку 4.1, - це підхід, заснований на одній загрозі та сценарії, який, безумовно, можна застосувати для проведення NRA, але з акцентом на КІ. Рівень суспільства відповідає вимогам керівних принципів DG-ECHO, але він йде далі і включає в себе більш надійний і послідовний аспект порушення роботи критичної інфраструктури, який є ключовим елементом EPCIP. Згідно з методологією, небезпека може мати безпосередній вплив на суспільство, а може також впливати на ключові об'єкти і системи, що, в свою чергу, може вплинути на громадян, навколишнє середовище або економіку.

Ці різні прямі або непрямі впливи відображені в запропонованому багаторівневому підході.

- **Громадський рівень.** Запропонована методологія починається з визначення сценарію небезпеки, який може безпосередньо вплинути на суспільство (наприклад, повінь, землетрус), але в той же час може вплинути на критично важливу інфраструктуру. Цей рівень відповідає національним керівним принципам оцінки ризиків, оскільки ризик розраховується відповідно до матриці ризиків, що базується на оцінці ймовірності загрози та (суспільного) впливу. Однак цей підхід також враховує вплив, спричинений виходом з ладу КІ або інших залежних КІ (каскадний вплив). Вони оцінюються на основі прямого впливу загрози на КІ (рівень активів) або через непрямий вплив небезпеки на інші КІ (системний рівень).
- **Рівень об'єкта.** На основі історичних даних, результатів оцінки вразливості КІ або наявності механізмів забезпечення стійкості можна надати оцінку прямого впливу на одну або декілька безпосередньо постраждалих КІ, виходячи з історичних даних, результатів оцінки вразливості КІ або наявності механізмів забезпечення стійкості. Зазвичай це оцінюється з точки зору рівня непрацездатності або економічних втрат для кожного активу. Цей прямий вплив на кожну КІ - погіршення якості послуг, перебої або збої - пов'язаний з впливом на суспільному рівні. Якщо це не так, то ця інфраструктура не повинна розглядатися як КІ в першу чергу. Ця оцінка пов'язує перебої на рівні активів з впливом на суспільство.
- **Системний рівень.** Якщо обраний сценарій загрози опосередковано впливає на інші КІ,

ми повинні враховувати взаємозалежності між цими КІ. Взаємозалежності є ключовим питанням для сучасної критичної інфраструктури. Як наслідок, оцінка залежностей повинна бути включена в нашу систему оцінки ризиків. Інструменти моделювання, імітації та аналізу дають гарне уявлення про ефекти пульсації у взаємопов'язаних системах, які, зрештою, призводять до впливу на суспільство через ці непрямі ефекти. Однак це може бути безперервний цикл, оскільки взаємозалежність між інфраструктурами може призвести до циклічного збільшення непрямих ефектів. Зрозуміло, що це може призвести до посилення впливу на рівні суспільства.

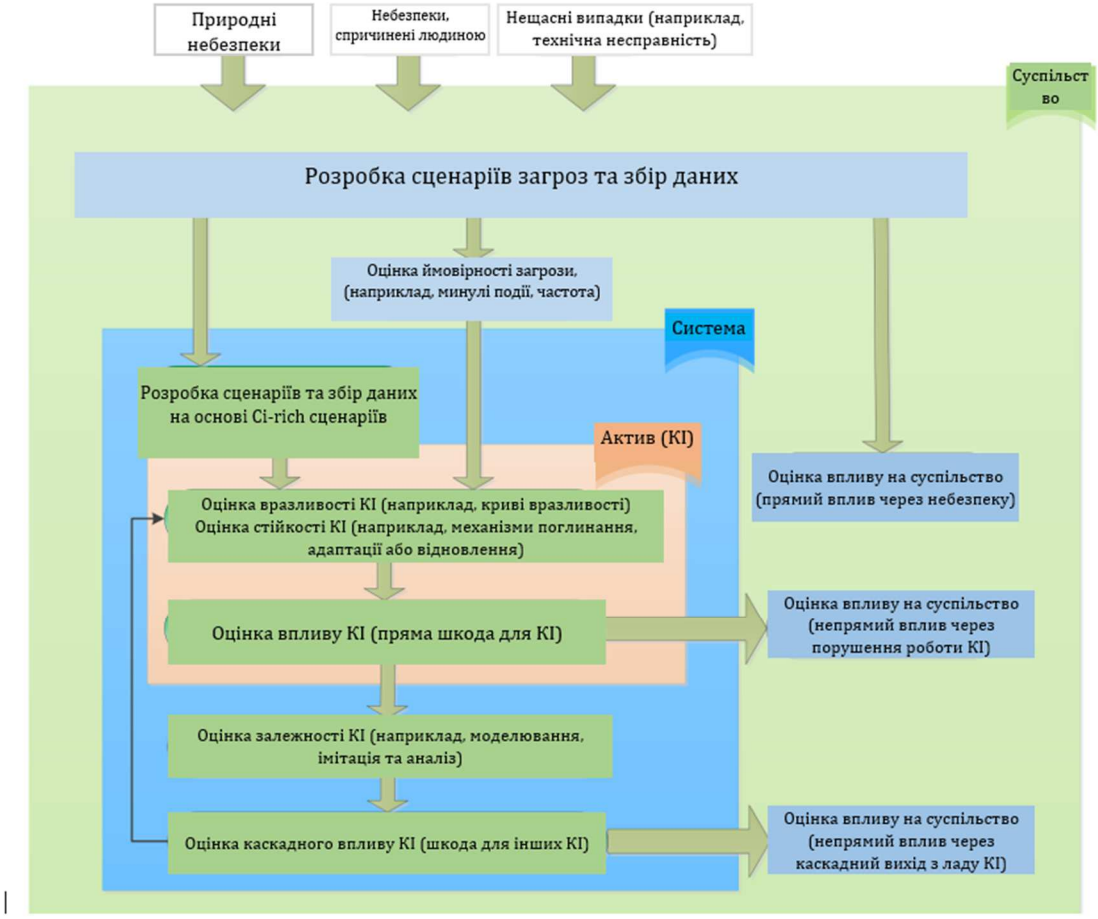

Рисунок 4.1: *Запропонована методологія CI-rich NRA*

The risk assessment layers and steps of this methodology are partially covered by ex- isting risk assessment methodologies identified in [2]. Several of them cover the overall risk management process (not only the risk assessment step). Risk treatment is achieved through various mitigation strategies, countermeasures or resilience mechanisms, but this methodolog-ical step is considered out of scope for this report.

Ми бачимо, що лише обмежена кількість цих методів та інструментів зосереджується на розробці сценаріїв. Прикладом може слугувати аналіз ризиків та вразливостей (RVA) від DEMA, в якому розробці сценаріїв присвячено окремий етап.

Більшість методів зазвичай зосереджені на конкретному, заздалегідь визначеному сценарії загрози або застосовують однакову методологію для обраних сценаріїв. Лише в обмежених випадках включається оцінка ймовірності загрози (наприклад, COUNTERACT, DECRIS, EURACOM, BMI, CIPDSS тощо). Що стосується оцінки вразливості, то метод BIRR вводить поняття VI (індекс вразливості) та PMI (індекс захисних заходів), CARVER оцінює доступність до фізичного розташування, COUNTERACT оцінює наявні засоби захисту від відповідних ризиків для різних активів, DECRIS використовує етап аналізу вразливості для визначення того, які загрози слід вивчати далі, а RVA використовує якісну п'ятибальну шкалу для оцінки вразливості. Методологія оцінки ризиків Sandia враховує ефективність системи захисту, яка виражається в зниженні ймовірності успішної реалізації загрози. Що стосується стійкості, BIRR вводить RI (Індекс стійкості), який забезпечує оцінку того, наскільки стійким є актив на основі механізмів надійності, винахідливості та відновлення. CARVER2 аналогічно розглядає наявність механізмів резервування, навіть якщо стійкість не згадується чітко. RAMCAP-Plus включає крок під назвою "Управління ризиками та стійкістю", який підкреслює, наскільки цей елемент є центральним у методології. Взаємозалежності охоплюються більшістю методик, оскільки це ключовий елемент для КІ, але методи, що використовуються, та рівень деталізації значно різняться між цими методиками.

4.1 Вимоги до розробки сценаріїв CI-rich, та збору даних

Сценарний підхід до NRA був рекомендований як DG-ECHO [1], так і застосований кількома державами-членами [3]. Він також підтримується настановами DHS щодо управління національними ризиками КІ [13]. Використання сценаріїв вважається засобом подолання складності проблеми; сценарії використовуються для того, щоб "розділити виявлені ризики на окремі частини, які можна оцінити та проаналізувати індивідуально" [13]. Використання таких сценаріїв має визначити, які об'єкти інфраструктури є найбільш критичними (потенційні наслідки будуть найвищими), а потім, де саме на цих вузлах слід зосередити заходи з безпеки та стійкості.

Під час проєкту CIPRNet FP7 Об'єднаний дослідницький центр у співпраці з Fraunhofer та CEA вивчив вимоги таких транскордонних сценаріїв [18]. Швидко стало очевидним, що визначення ключових активів (інфраструктур) та їх експлуатаційного стану є важливим при проведенні транскордонних навчань, заснованих на сценаріях.

У проекті CIPRNet кожна фаза сценарію описується відповідно до певного шаблону, який охоплює наступну інформацію [18]:

- **Часові рамки / тривалість:** Це може бути позначено конкретними моментами часу або конкретними подіями;
- **Опис інциденту:** Відображає поточну ситуацію, пов'язану з явищем/загрозою, що вивчається;
- **Постраждала інфраструктура(и):** Інформація, яка повинна бути включена, - це назва, сектор, місцезнаходження, оперативний статус і режим роботи (наприклад, нормальний, напружений, відновлення і т.д.) для кожної ураженої інфраструктури;
- **Карти:** Це необхідно для того, щоб візуально відобразити стан кожної фази;
- **Наслідки:** Прямі збитки, завдані інфраструктурі, також необхідні для кожної фази, оскільки це дозволить оцінити загальні соціальні наслідки всього сценарію.

Ми вважаємо, що підхід, представлений у цьому звіті, безумовно, може бути застосований до транскордонних регіонів і сценаріїв. Однак його застосування не є простим, і це пов'язано з моделями управління, які існують у різних регіонах.

Необхідно зробити кілька кроків, які можна узагальнити в наступних пунктах:

- Узгодження спільного глосарію термінів з метою полегшення комунікації та узгодженого визначення сценаріїв
- Визначення критичної інфраструктури або елементів КІ, які становлять спільний інтерес
- Визначення спільного сценарію загроз

Після того, як ці кроки будуть виконані, методологію RA, представлену тут, можна застосовувати так само, як це було б у випадку з національними КІ. Іншими словами, методологія RA, представлена тут, є ядром, навколо якого певні функції повинні бути додані або опущені залежно від конкретного дослідження (національний, транскордонний аналіз або аналіз на рівні ЄС).

4.2 Оцінка множинних ризиків

Якщо розглядати сценарії з декількома ризиками, проблема стає ще складнішою, оскільки численні загрози можуть несподівано змінити пропускну спроможність інфраструктури. Якщо ми розглянемо сценарії перехресних загроз, така складність ще більше зростає. Оцінка ймовірності загрози (див. Рисунок 4.1) повинна враховувати кореляцію між загрозами. Як наслідок, це виклик, який ще належить вирішити, головним чином, через його внутрішню складність. Певні загрози (наприклад, повені) можуть спричинити інші стихійні лиха (наприклад, зсуви), які можуть посилити негативний вплив як на КІ, так і на суспільство. Один з підходів може полягати в тому, що це вже враховано у визначенні сценарію, а потім слідувати всій методології RA, як це вже було описано. Однак, необхідна надійна методологія для визначення сценаріїв з декількома небезпеками, що враховує кореляції між небезпеками.

4.3 Управління ризиками та стійкістю

Хоча цей звіт зосереджений переважно на оцінці ризиків, він може стати основою для вивчення альтернативних варіантів управління ризиками. Оскільки підхід базується на сценаріях, він розглядає відомі або передбачувані загрози. Однак управління ризиками також має враховувати невідомі загрози, що більше відповідає сучасному підходу, який зосереджується на підходах, орієнтованих на забезпечення стійкості. Це означає, що контрзаходи повинні бути спрямовані не лише на запобігання загрозі або захист активу, але й на підвищення стійкості активу, тобто на посилення здатності до поглинання, адаптації та відновлення КІ [19] або комбінації КІ, які надають життєво важливі послуги громаді.

Розділ 5

Висновки та рекомендації

Мета цього звіту - надати огляд стану RA в державах-членах ЄС і показати, як його можна пов'язати з роботою та політикою щодо критичної інфраструктури (EPCIP), щоб запропонувати елементи, які можуть бути корисними для формування майбутньої політики у сфері захисту та стійкості критичної інфраструктури, враховуючи існуючі зусилля та законодавство. Стійкість, безумовно, повинна розглядатися як елемент, що може доповнити традиційну оцінку ризиків.

Для того, щоб впровадити систему оцінки ризиків, представлену в попередніх розділах, необхідно доопрацювати низку елементів. У наступних параграфах вони перераховані, а також представлені рекомендації щодо дій на рівні політик.

Потреба в моделюванні та симуляції

Власники та оператори об'єктів критичної інфраструктури неодноразово наголошували на важливості розробки інструментів і методологій для моделювання та симуляцій в сфері КІ. Дійсно, за останні роки було розроблено значну кількість інструментів, які можуть бути використані для оцінки широкого спектру руйнівних сценаріїв. Однак, здається, що більшості з цих інструментів не вистачає функцій для того, щоб їх можна було використовувати по всій Європі і зробити стандартом у цій галузі. В принципі, вони являють собою спеціальні зусилля, пристосовані до потреб конкретного регіону/штату, і, як наслідок, не мають можливості масштабуватися на міжнародному рівні. Необхідно створити спільний репозиторій або набір інструментів, що включає методології оцінки ризиків та інструменти, необхідні для проведення аналізу ризиків (наприклад, контрольні списки, сценарії, шаблони, моделі і т.д.). Крім того, для реалізації цілісного підходу необхідні інструменти, здатні боротися з численними загрозами, при цьому враховуючи об’єкти, системи та суспільні аспекти, а також взаємозалежності.

У Європі проводяться кілька зусиль, спрямованих на досягнення цієї мети. Важливим прикладом є ініціатива CIPRnet EISAC, спрямована на створення центру для розвитку компетенцій та інструментів для моделювання порушень критичної інфраструктури на різних рівнях. Такі зусилля повинні бути оцінені і належним чином розглянуті на рівні політики ЄС. JRC також робить свій внесок у цьому напрямку, розробляючи GRRASP (Платформу оцінки геопросторових ризиків та стійкості), яка має на меті надати Державам-членам ЄС можливості для аналізу порушень критичної інфраструктури. Для подальшої підтримки необхідності розробки інструментів з більш абстрактним підходом, цитуємо [13]: "Рівень деталізації та специфічності, що досягається за допомогою найскладніших моделей оцінки ризиків та симуляцій, може не бути практичним або необхідним для всіх об’єктів, систем або мереж. За таких обставин спрощений аналіз залежностей і взаємозалежностей, заснований на експертних оцінках, може забезпечити достатнє розуміння для своєчасного прийняття обґрунтованих рішень з управління ризиками".

Потреба в гармонізованій шкалі впливу

У ході дослідження, представленого в цьому звіті, ми виявили, що для полегшення розробки міжнародних або транскордонних оцінок ризиків необхідні гармонізовані шкали впливу. Важливим питанням є розмежування прямого та непрямого впливу, оскільки таким чином можна уникнути подвійного врахування впливу. Мета полягає в тому, щоб мати можливість представляти порівнянні результати і обмінюватися досвідом між державами-членами ЄС.

Відкритим питанням залишається невизначеність оцінок ([13]). Навіть коли сценарій з обґрунтованими найгіршими умовами чітко сформульований і послідовно застосовується, існує цілий ряд результатів, які можуть мати місце. Для деяких інцидентів діапазон наслідків невеликий, і проста оцінка може надати достатньо інформації для прийняття рішень. Якщо діапазон наслідків великий, сценарій може вимагати більшої конкретизації умов для отримання відповідних оцінок наслідків. Однак, якщо сценарій розбитий на частини з достатнім рівнем деталізації, але все одно залишається значна невизначеність, оцінка повинна супроводжуватися діапазоном невизначеності для підтримки прийняття більш обґрунтованих рішень. Найкращий спосіб повідомлення про невизначеність буде залежати від факторів, які роблять результат невизначеним, а також від обсягу і типу наявної інформації.

Визначення спільних або транскордонних сценаріїв

Прийняття спільної методології RA у різних країнах і транскордонних регіонах відкриває шлях до тіснішої співпраці з питань, що становлять спільний інтерес. Кордони накладають обмеження на безперервність управління, але це не стосується деяких загроз. Крім того, багато транскордонних регіонів функціонують і залежать від інфраструктури, яка знаходиться по обидва боки кордонів, і, як наслідок, можуть знадобитися скоординовані та узгоджені дії. У цьому контексті розробка навчань має вирішальне значення, а прийняття гармонізованого процесу RA допомагає у визначенні загальних або спільних сценаріїв.

Залучення приватного сектору (операторів КІ)

Через розвинену модель управління сучасною критичною інфраструктурою необхідно залучати операторів КІ до проведення оцінки ризиків. Оператори мають набагато краще уявлення про ризики, з якими може зіткнутися їхня інфраструктура, а також про те, яким буде їхній вплив (на рівні об’єктів). Необхідна тісна співпраця та обмін інформацією з органами влади для того, щоб вносити цю інформацію в систему RA, яка може дозволити визначити вплив на рівні системи з урахуванням взаємозалежностей і, зрештою, отримати загальну картину економічного впливу.

Потрібен динамічний аналіз

Відповідно до звіту [3] можна розробити загальноєвропейський сценарій і матрицю для кожної загрози. Це той момент, коли елемент CIP повинен бути ідентифікований і відповідним чином вирішений. Всі заходи з моделювання та симуляції, які будуть необхідні як для відображення сценарію, так і для об’єктів (КІ), що зазнають впливу, повинні дозволяти проводити аналіз у часі, оскільки як рівні працездатності кожної ураженої КІ, так і залежності між ними можуть змінюватися з плином часу.

Подяки

Ця робота була підтримана програмою "Запобігання, готовність і подолання наслідків тероризму та інших ризиків, пов'язаних з безпекою (CIPS)" в рамках адміністративної домовленості (контракт № HOME/2011/CIPS/AA/001-A1). Ми дуже вдячні за цю підтримку.

Список використаних джерел

[1] Е. Комісія, "Робочий документ співробітників Комісії: Керівництво з оцінки ризиків та картографування для управління надзвичайними ситуаціями". 21.12.2010, sEC(2010) 1626 final.

[2] Г. Джаннопулос, Р. Філіппіні та М. Шиммер, "Методології оцінки ризиків для захисту критичної інфраструктури: Сучасний стан", Європейська Комісія, Tech. Rep. EUR 25286, 2012.

[3] Європейська Комісія, "Огляд робочого документу співробітників Комісії щодо ризиків природних і техногенних катастроф в ЄС", Брюссель, 8.4.2014, sWD(2014) 134 final.

[4] Є. Рада, "Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію та призначення європейських об'єктів критичної інфраструктури та оцінку необхідності покращення їх захисту". 2008.

[5] Є. Комісія, "Робочий документ співробітників Комісії щодо нового підходу до європейської програми захисту критичної інфраструктури - підвищення безпеки європейської критичної інфраструктури", 28.8.2013, sWD(2013) 318 final.

[6] Л. Гальбузера, Г. Джаннопулос і Д. Уорд, "Розробка стрес-тестів для підвищення стійкості критичної інфраструктури: техніко-економічний аналіз", Люксембург: Офіс публікацій Європейського Союзу, JRC Science and Policy Reports JRC91129, 2014.

[7] "Глобальні ризики 2015: 10-е видання", Всесвітній економічний форум, Tech. Rep. REF: 090115, 2015.

[8] "ISO31010:2009 - Управління ризиками - Методи оцінки ризиків", Міжнародна організація зі стандартизації, 2009.

[9] МСУОБ ООН. (2009, травень) 2009 Термінологія МСУОБ ООН щодо зменшення ризику стихійних лих, Міжнародна стратегія ООН зі зменшення небезпеки стихійних лих. [Онлайн]. Доступно: http://www.unisdr.org/files/ 7817 UNISDRTerminologyEnglish.pdf

[10] "Президентська політична директива - Безпека та стійкість критичної інфраструктури, PPD-21, Білий дім, Офіс прес-секретаря, США". Білий дім, Офіс прес-секретаря, лютий 2013 року.

[11] "ISO31000:2009 - Управління ризиками - Принципи та настанови", Міжнародна організація зі стандартизації, 2009.

[12] "ISO Guide 73:2009 - Управління ризиками - Принципи та настанови", Міжнародна організація зі стандартизації, 2009.

[13] "Додатковий інструмент: Реалізація підходу до управління ризиками критичної інфраструктури", Міністерство внутрішньої безпеки США, Tech. Rep., 2013. [Онлайн]. Режим доступу: http://www.dhs.gov/sites/default/files/ publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

[14] К. Європейського Союзу, "Висновки Ради щодо подальшого розвитку оцінки ризиків для управління катастрофами в Європейському Союзі", 11 і 12 квітня 2011 року, 3081-е засідання Ради з питань юстиції та внутрішніх справ.

[15] "Оцінювання залежностей n-го порядку між критичними інфраструктурами", Міжнародний журнал критичної інфраструктури, т. 9, № 1, с. 93-110, 2013.

[16] Міністерство безпеки та правосуддя, "Короткий огляд кризових ситуацій в Нідерландах", 09-04-2015. [Онлайн]. Доступно за посиланням: https://www.nctv.nl/Images/voortgangsbrief-150415 tcm126-590874.pdf

[17] Y. Barbarin, M. Theocharidou, and E. Rome, "CIPRNet deliverable deliverable D6.2: Application scenario", CEA, JRC, Fraunhofer IAIS, Tech. Rep., травень 2014. [Онлайн]. Доступно: https://www.ciprnet.eu/

[18] Р. Френсіс і Б. Бекера, "Метрика і рамки для аналізу стійкості інженерних та інфраструктурних систем", Reliability Engineering & System Safety, vol. 121, pp. 90-103, 2014.

Europe Direct - це сервіс, який допоможе вам знайти відповіді на ваші запитання про безкоштовний номер Європейського Союзу (*): 00 800 6 7 8 9 10 11

(*) Деякі оператори мобільного зв'язку не надають доступ до номерів 00 800 або ці дзвінки можуть бути платними.

Багато додаткової інформації про Європейський Союз можна знайти в Інтернеті. Доступ до неї можна отримати через сервер Europa http://europa.eu.

Як отримати публікації ЄС

Наші публікації можна придбати в книгарні ЄС (http://publications.europa.eu/howto/index_en.htm), де ви можете зробити замовлення у обраного вами агента з продажу.

Офіс публікацій має всесвітню мережу агентів з продажу.

Ви можете отримати їхні контактні дані, надіславши факс на номер (352) 29 29-42758.

LB-NA-27332-EN-N

JRC Mission

Місія Об'єднаного дослідницького центру як внутрішньої наукової служби Комісії полягає в тому, щоб надавати політикам ЄС незалежну, науково обґрунтовану науково-технічну підтримку протягом усього політичного циклу.

Працюючи у тісній співпраці з генеральними директоратами, Об'єднаний дослідницький центр вирішує ключові суспільні виклики, стимулюючи інновації шляхом розробки нових методів, інструментів і стандартів, а також ділиться своїми ноу-хау з державами-членами, науковою спільнотою та міжнародними партнерами.

Служіння суспільству
Стимулювання інновацій
Підтримка законодавства

Publications Office

doi:10.2788/621843
ISBN 978-92-79-49246-4