Огляди політики управління ризиками ОЕСР

Ефективне управління для критичної інфраструктури Стійкість

Ця робота публікується під відповідальність Генерального секретаря OECD. Висловлені в ній думки та аргументи не обов'язково відображають офіційну позицію країн-членів OECD.

Цей документ, а також будь-які дані та будь-які карти, включені до нього, не впливають на статус або суверенітет будь-якої території, делімітацію міжнародних кордонів та меж, а також на назву будь-якої території, міста чи району.

Будь ласка, посилайтеся на цю публікацію як:
OECD (2019), *Належне врядування для забезпечення стійкості критичної інфраструктури*, Огляди політики управління ризиками OECD, Публікація OECD, Париж.
https://doi.org/10.1787/02f0e5a0-en

ISBN 978-92-64-53346-2 (друк)
ISBN 978-92-64-41050-3 (pdf)

Огляди політики управління ризиками
OECP ISSN 1993-4092 (друк)
ISSN 1993-4106 (онлайн)

Переглянута версія, липень 2019 р. Деталі змін доступні за посиланням:
http://www.oecd.org/about/publishing/Corrigendum_GoodGovernanceCriticalInfrastructureResilience.pdf

Статистичні дані по Ізраїлю надані відповідними ізраїльськими органами влади та під їхню відповідальність. Використання таких даних OECD не впливає на статус Голанських висот, Східного Єрусалиму та ізраїльських поселень на Західному березі річки Йордан відповідно до норм міжнародного права.

Авторські права на фото: Обкладинка © jamesteohart/Shutterstock.com

Виправлення до публікацій OECP можна знайти в Інтернеті за адресою: www.oecd.org/about/publishing/corrigenda.htm.

Передмова

Стихійні лиха та зловмисні атаки на об'єкти критичної інфраструктури становлять серйозні ризики для суспільства та економіки. Нещодавні шокові події - такі як Великий східнояпонський землетрус, ураган Харві в США, кібератаки на українську електромережу або обвал Генуезького мосту в Італії, демонструють, як перебої в роботі критично важливої інфраструктури та основних послуг можуть призвести до значних економічних збитків і людських жертв. Взаємопов'язаність ланцюгів поставок, технологічних і фінансових систем у світовій економіці збільшує вразливість критичної інфраструктури. Коли виникають потрясіння і перебої, їхній негативний вплив може виходити за межі секторів і кордонів і навіть мати глобальний резонанс.

Водночас глобальне зростання інвестицій в інфраструктуру та цифрова трансформація інфраструктурних послуг дають можливість переосмислити питання стійкості критичної інфраструктури. У цьому звіті проаналізовано мінливі умови для підвищення стійкості в країнах OECD, а також розглянуто варіанти політики та моделі управління, які сприяють авансовим інвестиціям у стійкість.

На основі дослідження, проведеного в різних країнах світу, у звіті аналізується поступовий зсув у політиці щодо критичної інфраструктури від захисту активів до забезпечення стійкості системи. Замість того, щоб зосереджуватися лише на захисті активів, системний підхід дозволяє урядам та операторам інфраструктури враховувати взаємозалежність активів і визначати пріоритети заходів з підвищення стійкості для критично важливих центрів і вузлів, вихід з ладу яких може завдати найбільшої шкоди.

Звіт також включає тематичне дослідження з електропостачання Фінляндії, яке ілюструє, як уряди можуть будувати партнерські відносини з операторами критичної інфраструктури для обміну інформацією та постановки цілей, зміцнюючи довіру та стійкість.

Нарешті, у "Політичному інструментарії з управління стійкістю критичної інфраструктури" визначено важливі кроки у розробці відповідної моделі управління для вирішення сучасних проблем стійкості критичноїінфраструктури. Цей посібник доповнює Рекомендації OECD з управління критичними ризиками, сприяє міжнародним дискусіям у рамках G20 щодо якісної інфраструктури та підтримує реалізацію Сендайської рамкової програми зі зниження ризиків катастроф.

Інструментарій покликаний підтримати зусилля урядів щодо оновлення політики у сфері критичної інфраструктури. Надалі OECD працюватиме з урядаминад розробкою контрольних показників та проведенням тематичних досліджень для порівняння прогресу та покращення міждержавного навчання у цій важливій сфері.

Подяки

Цей звіт був підготовлений під егідою Форуму OECD з питань ризиків високого рівня Директоратом OECD з питань державного управління на чолі з Маркосом Бонтурі (Marcos Bonturi).

У звіті представлено результати роботи Форуму з питань ризиків високого рівня OECD, спрямованої на посилення стійкості критичної інфраструктури шляхом удосконалення управління. Цей звіт координував і написав Чарльз Баубіон під керівництвом Джека Радіша і Стефана Якобзона. Розділи 1-3 ґрунтуються на Рамковій системі оцінки політики щодо управління стійкістю критичної інфраструктури, розробленій Мері Кейт Фішер і Кетрін Гампер в рамках проекту, який OECD проводила спільно з Міжамериканським банком розвитку. Аріадна Анісімов провела аналіз міжкраїнового дослідження OECD щодо стійкості критичної інфраструктури та надала цінну дослідницьку допомогу протягом усього проекту, особливо для тематичного дослідження щодо передачі та розподілу електроенергії у Фінляндії. Тереза Марія Деубеллі та Джон Рош зробили свій внесок у проект, поділившись своїми ідеями та відгуками. Ракель Паракено підготувала звіт до публікації. Команда дуже вдячна Елізабет Хаггард за допомогу, яку вона надавала протягом усього проекту.

Секретаріат висловлює подяку делегатам Форуму з питань ризиків високого рівня, які взяли участь в опитуванні OECD, і, зокрема, наступним колегам за їхні вдячні відгуки та коментарі: Райан Шварц і Трент Ебботт (Канада), Тіфен Боссан (Франція), Катрін Штольценбург (Німеччина), Георгіос Джаннопулос і Мацей Кушинський (Європейська комісія), Крістіан Фядер і Мікко Вяха-Сіпіля (Фінляндія), Дайго Ота (Японія), Пьотр Шуфнара (Польща), Стефан Брем (Швейцарія), Елізабет Лозі і Сьюзан Стівенс (США). Дуейн Вернер (Аргонська національна лабораторія), Марі-Валентин Флорін (Міжнародна рада з управління ризиками), Річард Сміт-Бінгем (компанії Marsh та McLennan) та Еліза Гастальді (Siemens) представили додаткові перспективи з боку дослідницького та приватного секторів.

Коментарі та відгуки, отримані від колег з OECD Лорана Берна, Лізи Даніельсон, Майкла Маллана та Лі Вольфрома, а також колеги з Агентства з ядерної енергії Ольвідо Гусмана, допомогли інтегрувати додаткові перспективи в аналіз.

Звіт ґрунтується на дискусіях, проведених під час семінару "Системне мислення для забезпечення стійкості та безпеки критичної інфраструктури", спільно організованого OECD та Об'єднаним дослідницьким центром Європейської Комісії (JRC) у вересні 2018 року. Особлива подяка спікерам та експертам за їхні цінні ідеї, а також JRC за підтримку в організації цього заходу.

Фінансова підтримка, отримана від Національного агентства з надзвичайних ситуацій Фінляндії (NESA), відіграла важливу роль у проведенні тематичного дослідження у Фінляндії, за що OECD висловлює подяку, так само як і за внесок Міжамериканського банку розвитку у проведення попереднього аналізу.

Акроніми та скорочення

BBK - Федеральне відомство Німеччини з питань цивільного захисту та допомоги у разі стихійних лих

BSI - Британський інститут стандартів

CI - Критична інфраструктура

CIP - Захист критичної інфраструктури

CIWIN - Інформаційна мережа попереджень про критичну інфраструктуру (Європейський Союз)

CPNI - Центр захисту національної інфраструктури (Великобританія)

CRISRRAM - Методологія оцінки ризиків і стійкості критичних інфраструктур і систем

DAFNI - Інструмент даних та аналітики для національної інфраструктури (Великобританія)

DC - Постійний струм

DHS - Міністерство внутрішньої безпеки (Сполучені Штати)

DSO - Оператор системи розподілу

EPCIP - Європейська програма захисту критичної інфраструктури

EU - Європейський Союз

FEMA - Федеральне агентство з управління надзвичайними ситуаціями (Сполучені Штати)

FERC - Федеральна комісія з регулювання енергетики (Сполучені Штати)

GDP - Зростання внутрішнього продукту

GPS - Глобальна система позиціонування

ICT - Інформаційно-комунікаційні технології

ISAC - Центр обміну та аналізу інформації

ISO - Міжнародна організація стандартів

IT - Інформаційні технології

JRC - Об'єднаний дослідницький центр (Європейська комісія)

NARUC - Національна асоціація уповноважених з питань регулювання комунальних послуг (Сполучені Штати)

NATS - Національна служба управління повітряним рухом

NCIPP - Національна програма захисту критичної інфраструктури (Польща)

NCTV - Національний координатор з питань безпеки та боротьби з тероризмом (Нідерланди)

NESA - Національне агентство екстреного постачання (Фінляндія)

NESO - Національна організація екстреного постачання (Фінляндія)

NIPP - Національний план захисту інфраструктури (Сполучені Штати)

OECD - Організація економічного співробітництва та розвитку

OT - Технологія експлуатації

PSA - Радник із захисту безпеки

PSC - Міністерство громадської безпеки Канади

RRAP - Регіональна програма оцінки стійкості (Сполучені Штати)

SARS - Важкий гострий респіраторний синдром

TEPCO - Токійська електроенергетична компаніяТокійська електроенергетична компанія

TISN - Довірена мережа обміну інформацією (Австралія)

TSO – Оператор системи передачі

Зміст

Таблиці

Цифри

Коробки

Виконавчий директор Резюме

Критична інфраструктура є основою нашої сучасної та взаємопов'язаної економіки. Порушення роботи критично важливих систем та основних послуг, таких як телекомунікації, енерго- та водопостачання, транспортні та фінансові системи, може призвести до значних економічних збитків. Ці системи є дуже вразливими до різноманітних потрясінь - від кліматичних і геологічних небезпек до промислових аварій, терористичних і кібератак, які можуть спричинити каскадний негативний вплив на місцевому і навіть глобальному рівнях.

Враховуючи гіперзв'язність цих основних інфраструктурних активів, що посилюється цифровою трансформацією, необхідна комплексна державна політика для посилення стійкості критичної інфраструктури. Мета полягає в тому, щоб обмежити ризик перебоїв у наданні основних послуг і підвищити здатність до швидкого відновлення після шоку. Забезпечення безперервності надання послуг критичної інфраструктури має бути невід'ємною частиною політики управління ризиками як в країнах-членах OECD, так і в країнах-партнерах, як зазначено в Рекомендаціях OECD щодо управління критичними ризиками.

У цьому звіті розглядається еволюція ландшафту ризиків та політичні корективи, необхідні для посилення стійкості критичної інфраструктури. Аналіз показує, що для ефективного подолання складності та взаємозалежності в інфраструктурі найкраще підходить послідовний, системний підхід. Партнерство між урядом та операторами інфраструктури також може сприяти більшому обміну інформацією та інвестиціям у стійкість. Інструментарій з управління стійкістю критичної інфраструктури надає конкретні рекомендації щодо реформ, зосереджуючи увагу на розбудові стійкості на випередження.

Основні висновки

З середини 2000-х років уряди розробляють і впроваджують державну політику на підтримку захисту критичної інфраструктури. Більшість країн OECD визначили сектори критичної інфраструктури, провели інвентаризацію активів і запровадили нормативно-правові акти, національні програми або механізми стимулювання для посилення стійкості критичної інфраструктури до шокових подій.

Однак, ці політики, які здебільшого визначалися порядком денним у сфері безпеки після 11 вересня, не завжди були ефективними у вирішенні проблем більш складного, взаємопов'язаного з цифровими технологіями середовища 21 століття. Сучасна політика забезпечення стійкості критичної інфраструктури повинна враховувати різноманітні і складні шокові події, більш взаємозалежні системи і країни, а також швидкий темп інновацій в інфраструктурних секторах. Старіння інфраструктури також становить зростаючий політичний виклик.

Інвестиції в інфраструктуру зростають у всьому світі, надаючи країнам можливість переглянути свою політику і підвищити стійкість, одночасно посилюючи стійкість і захист існуючої інфраструктури.

Системний підхід має очевидні переваги при розробці політики щодо критичної інфраструктури. Така політика повинна враховувати всі небезпеки та загрози, забезпечувати координацію між різними секторами (державним і приватним), охоплювати весь життєвий цикл інфраструктури та сприяти транскордонному

співробітництву.

Стійкість критичної інфраструктури залежить від співпраці урядів з операторами інфраструктури з державного та приватного секторів. Хоча оператори та уряди погоджуються з необхідністю захисту критично важливих активів і підтримки послуг, їхні погляди на рівень необхідної стійкості, засоби її досягнення та регуляторні вимоги, які повинні застосовуватися, можуть відрізнятися. Ці рішення мають фінансові наслідки і ставлять питання про те, хто буде нести додаткові витрати, пов'язані з інвестуванням в стійкість.

Державно-приватна співпраця між урядами та операторами з метою заохочення діалогу з цих питань є корисною для спільної розробки та впровадження політики забезпечення стійкості та безпеки критичної інфраструктури. Встановлення довіри, забезпечення безпечного обміну інформацією, розробка механізмів розподілу витрат і зміцнення міжнародного співробітництва є одними з ключових завдань, які необхідно вирішити при створенні таких партнерств, і вимагають відповідних механізмів управління.

Уряди можуть обирати з безлічі політичних інструментів для посилення стійкості критичної інфраструктури. Опитування OECD визначило двадцять два таких інструменти - від нормативно-правових актів і компенсаційних механізмів до добровільних механізмів, заснованих на партнерстві. Урядам важливо знайти правильний баланс між обов'язковими та добровільними механізмами, щоб посилити залучення зацікавлених сторін до цього процесу та забезпечити ефективне інвестування в стійкість.

Приклад фінської системи передачі та розподілу електроенергії ілюструє ефективну модель управління, яка сприяє інвестиціям у стійкість інфраструктури. Фінляндія розробляє рамки співпраці для посилення стійкості критичної інфраструктури, яка наголошує на державно-приватній співпраці, обміні інформацією та досягненні консенсусу щодо розробки політики та встановлення цілей Ця модель управління дала вражаючі результати в перші роки її впровадження. Тим не менш, з'явилися нові виклики, зокрема, вирішення проблем, пов'язаних з витратами для споживачів, різницею в можливостях великих і малих операторів, діджиталізацією та зміною клімату.

На шляху до більш структурованого підходу: сім кроків для політики стійкості критичної інфраструктури

У цьому звіті пропонується Інструментарій з управління стійкістю критичної інфраструктури, який пропонує урядам вирішити наступні сім взаємопов'язаних управлінських викликів:

1. **Створення міжгалузевої структури управління для забезпечення стійкості критичної інфраструктури**. Уряди повинні прийняти загальнодержавний підхід до забезпечення стійкості критичної інфраструктури, що охоплює різні ризики та сектори інфраструктури.
2. **Розуміння складних взаємозалежностей і вразливостей в інфраструктурних системах для визначення пріоритетності зусиль з розбудови стійкості**. Уряди повинні прийняти методології та метрики для визначення критично важливих функцій, систем та активів, які мають бути пріоритетними для інвестицій у розбудову стійкості.

3. **Встановлення довіри між урядом та операторами шляхом забезпечення обміну інформацією про ризики**. Уряди повинні створити платформи для обміну інформацією з операторами критичної інфраструктури для всебічного і спільного розуміння ризиків і вразливостей, забезпечуючи безпеку і конфіденційність інформації, якою вони обмінюються.

4. **Розбудова партнерств для вироблення спільного бачення та узгодження досяжних цілей у сфері стійкості.** Уряди повинні налагодити постійний діалог з операторами критичної інфраструктури з державного та приватного секторів, взявши за відправну точку очікування громадськості.

5. **Визначення комплексу політичних заходів для визначення пріоритетності економічно ефективних заходів з підвищення стійкості на всіх етапах життєвого циклу інфраструктури.** Уряди повинні визначити комплекс політичних інструментів на основі аналізу витрат і вигоди, щоб заохотити операторів інвестувати в забезпечення стійкості та досягти поставлених цілей.

6. **Забезпечення підзвітності та моніторингу впровадження політики стійкості критичної інфраструктури.** Уряд повинен здійснювати моніторинг впровадження та оцінювати прогрес у досягненні цілей щодо забезпечення стійкості, створивши чітку систему підзвітності для операторів.

7. **Врахування транскордонного виміру інфраструктурних систем.** Уряд повинен координувати національну політику стійкості критичної інфраструктури із сусідніми країнами та за її межами, щоб вирішувати питання транскордонної залежності.

1. Зробити стійкість критичної інфраструктури пріоритетом політики

У цьому розділі представлено огляд ризиків та інфраструктурних ландшафтів, а також висвітлено можливості інвестування у підвищення стійкості критичної інфраструктури. Оскільки кліматичні ризики та інші природні небезпеки, цифрові загрози і загрози безпеці можуть порушити роботу інфраструктурних послуг з далекосяжними соціально-економічними наслідками, аналіз у цьому розділі підкреслює важливість прийняття підходу до забезпечення стійкості критичної інфраструктури, що враховує всі небезпеки і загрози. У світлі зростаючої взаємозалежності між інфраструктурними системами, швидких темпів інноваційної трансформації інфраструктури та збільшення обсягів інвестицій в інфраструктуру в цьому розділі наводяться аргументи на користь коригування

Численні небезпеки та загрози можуть порушити роботу критично важливої інфраструктури

Критична інфраструктура є основою функціонування нашого сучасного взаємопов'язаного суспільства. Порушення телекомунікаційних послуг, водо- чи енергопостачання, транспортних чи фінансових систем може завдати значної шкоди добробуту громадян та спричинити негативні економічні наслідки, які матимуть резонанс за межами безпосередньо постраждалої території.

Різноманітні потрясіння - від стихійних лих до промислових аварій, терористичних або кібератак - продемонстрували вразливість цих критично важливих систем. Їх руйнування, збої або перебої в роботі можуть призвести до каскадних наслідків у різних секторах, а іноді й за межами національних кордонів. Таким чином, забезпечення безперервності обслуговування критично важливих об'єктів інфраструктури має бути невід'ємною частиною політики управління ризиками в країнах-членах OECD та країнах-партнерах.

Рекомендація OECD щодо управління критичними ризиками, прийнята міністрами країн-членів OECD у травні 2014 року, відображає цю важливість, закликаючи уряди визначити, де порушення роботи критичної інфраструктури може призвести до каскадних наслідків (OECD, 2014[1]). В опитуванні OECP щодо управління критичними ризиками, проведеному в 2016 році з метою моніторингу виконання Рекомендації, половина країн OECD вказали порушення роботи критичної інфраструктури як один з національних критичних ризиків (OECD, 2018[2]).

Стихійні лиха, промислові аварії та пандемії можуть спричинити серйозні перебої в роботі критично важливої інфраструктури

Критична інфраструктура є особливо вразливою до шокових подій, таких як стихійні лиха. Вітровали можуть призвести до падіння повітряних ліній електропередач і розподілу електроенергії, землетруси - до розриву водопроводів, руйнування мостів або тунелів, повені та інші стихійні лиха, пов'язані з водою, можуть мати значні наслідки для автомобільних доріг, залізниць, об'єктів водопостачання та водовідведення, а штормові припливи і цунамі впливають на гавані, енергетичні об'єкти та іншу інфраструктуру, розташовану в прибережних зонах. Космічні погодні явища, такі як сонячні бурі, також можуть поставити під загрозу відключення електромережі, а також поставити під загрозу супутники і системи геопозиціонування з потенційними наслідками для транспорту та інших видів діяльності (Krausmann et al., 2016[3]). Промислові аварії також можуть призвести до значних перебоїв. Пандемії, такі як атипова пневмонія у 2009 році, можуть перевантажити системи охорони здоров'я і вплинути на міжнародні авіаперевезення, якщо не буде запроваджена політика запобігання.

Коли об'єкт або мережа критичної інфраструктури зазнає впливу надзвичайної події, перебої в наданні послуг можуть швидко призвести до значних економічних або соціальних наслідків. Окрім прямих збитків від стихійного лиха, перебої в наданні послуг можуть мати більш тривалий характер і впливати на більшу територію, ніж сама катастрофа. Як наслідок, фірми та домогосподарства можуть постраждати від втрати послуг, що вплине на обсяги виробництва, попит та добробут. У деяких випадках безперервність діяльності уряду також може бути суттєво порушена, в тому числі під час реагування на надзвичайні ситуації, що може ще більше затримати економічне відновлення після стихійного лиха. Приклади, наведені у вставці 1, демонструють, наскільки масштабними можуть

бути такі наслідки нещодавніх катастроф, що вплинули на різні сектори економіки.

Очікується, що зміна клімату та пов'язані з нею ризики підвищення рівня моря підвищать вразливість багатьох систем критичної інфраструктури, розташованих на морському узбережжі та вздовж водних шляхів, особливо в енергетичному та транспортному секторах. В Оцінці ризиків, пов'язаних зі зміною клімату у Великій Британії, проведеної у 2017 році, було детально проаналізовано вплив зміни клімату на енергетичний сектор і підкреслено вразливість енергетичної інфраструктури країни до підвищення рівня моря (Уряд Великої Британії, 2017[4]).

Вставка 1.1. Наслідки порушень критичної інфраструктури під час окремих надзвичайних ситуацій

- **Великий східнояпонський землетрус** 2011 року та подальше цунамі суттєво вплинули на енергетичний сектор Японії. Аварія на атомній електростанції Фукусіма-1 і подальше закриття атомних електростанцій по всій країні призвели до скорочення виробництва електроенергії на 50 %, що спричинило значні перебої в енергопостачанні по всій країні.
- **Суперштторм "Сенді"** 2012 року **затопив** ключові дороги і тунелі, що з'єднують Бруклін і Манхеттен, а також лінії поїздів і метро у великому столичному регіоні Нью-Йорка і Нью-Джерсі. В результаті 5,4 мільйона пасажирів залишилися без засобів пересування, що порушило безперервність бізнесу в більшій мірі, ніж сам ураган. Крім того, приблизно 8,5 мільйонів домогосподарств постраждали від нестачі електроенергії.
- Закриття європейського повітряного простору після **виверження вулкану Ейяф'ятлайокудль** в Ісландії в 2010 році призвело до скасування понад 100 000 рейсів і зміни маршрутів по всьому світу. В результаті багато компаній, які залежать від авіаперевезень для доставки продукції та ключових компонентів, не змогли постачати продукцію на ринки та виробничі системи по всій Європі та за її межами.
- **Вибух небезпечних матеріалів у порту Тяньцзінь в** Китаї в 2015 році призвів до масштабної зміни маршрутів вантажів і танкерів, що прямувалидо 6 найбільшого порту в світі, на кілька тижнів.
- **Чилійський землетрус 2010** року спричинив серйозні перебої в роботі транспортної та телекомунікаційної систем.
- **Відключення електроенергії** на **північному сході США та в Канаді у** 2003 році було спричинене падінням дерев на високовольтну лінію електропередач у північному Огайо, що призвело до каскадних збоїв у південно-східній Канаді та восьми штатах на північному сході США, від чого постраждали 50 мільйонів людей у США та Канаді, а збитки оцінюються у 6 мільярдів доларів США.

Примітка: У Додатку 1 більш детально описано наслідки цих окремих подій, що призвели до порушення роботи критичної інфраструктури, а також уроки, винесені з них.
Джерело: Додаток 1

Ці перебої можуть призвести до значних економічних збитків і втрат

Оцінити економічні та соціальні наслідки руйнування критично важливої інфраструктури досить складно. Ці непрямі наслідки надзвичайних ситуацій не так просто виміряти або змоделювати, як прямі збитки, для яких у країнах OECD все частіше застосовуються класичні методи (OECD, 2018[5]). Тим не менш, під час великих катастроф економічний вплив цих порушень зазвичай занадто великий, щоб його ігнорувати (Rose та ін., 2012[6]).

Аналіз OECD щодо ризику повеней на річці Сена в Парижі дає уявлення про масштаби економічних втрат, пов'язаних з критично важливою інфраструктурою. На основі сценаріїв повеней різної величини, зосереджених навколо події з періодом повторюваності 100 років, потенційні збитки, завдані критично важливій інфраструктурі, такій як транспортні, енергетичні або водні об'єкти та мережі,

становлять від 35% до 55% від загального обсягу прямих збитків, спричинених повенями. Ще важливіше те, що втрати бізнесу, спричинені перебоями в роботі електроенергетичного і транспортного секторів у мегаполісі Парижа, можуть сягати85% від загальних втрат бізнесу, змодельованих для всієї території (OECD, 2014 рік[7]).

Критична інфраструктура може бути мішенню для зловмисних атак - від тероризму до цифрових загроз безпеці

Зловмисники також визначили об'єкти критичної інфраструктури як потенційні цілі з огляду на значний вплив, який може спричинити їхнє руйнування. Це стосується як терористичних актів, так і цифрових загроз. Новий ризик гібридних загроз, що характеризується тим, що зловмисники використовують вразливі місця цивільної діяльності, такі як життєзабезпечення, щоб вплинути на довіру суспільства до відкритих і демократичних суспільств, також привертає підвищену увагу ризик- менеджерів у країнах OECD (OECD, 2018[8]).

Як показано у Вставці 1.2, цифрові загрози можуть впливати на критичну інфраструктуру різними способами - від програмного до апаратного забезпечення, а також через вплив на попит. Швидкий розвиток технологій і зростаюча цифровізація багатьох процесів у критично важливій інфраструктурі вимагають постійного відстеження цифрових загроз безпеці та регулярної оцінки нових можливостей зловмисників.

Що стосується ризику тероризму, то транспортна інфраструктура - від повітряного і морського сполучення до залізниць і метро - є дуже вразливими об'єктами для терористичних атак, захистити які може бути дуже складно. У разі нападу негативні наслідки можуть вийти далеко за рамки людських жертв, оскільки системи можуть бути виведені з ладу на кілька тижнів, а довіру громадян буде важко відновити. Хімічні заводи і ядерні реактори також можуть бути об'єктами терористичних атак, що призводить до масштабних розливів, які можуть зробити територію непридатною для проживання на тривалий час. Терористи також можуть атакувати системи водопостачання з бактеріологічним або хімічним забрудненням.

Для операторів критичної інфраструктури внутрішні загрози є важливим питанням як з точки зору ризиків для цифрової безпеки, так і тероризму. Доступ до об'єктів та знання заходів безпеки надають значну перевагу зловмисникам, які бажають вчинити такі дії.

На шляху до підходу до ризиків критичної інфраструктури, що враховує всінебезпеки та загрози

У цьому динамічному ландшафті ризиків портфель ризиків, на які повинні реагувати політики, щоб побудувати більш стійку країну, постійно змінюється. Вразливість критичної інфраструктури до цього спектру небезпек і загроз вимагає підвищеної уваги до безпеки та стійкості критичної інфраструктури. Ризики катастроф, посилені зміною клімату, створюють низку викликів для стійкості інфраструктури. Крім того, зростання гібридних загроз і пов'язаних з ними ризиків цифрової безпеки вимагає підвищення стійкості критичної інфраструктури до інцидентів у сфері цифрової безпеки. Заходи безпеки проти терористичних ризиків також повинні включати стійкість інфраструктури. Різноманітність загроз, з якими стикається критична інфраструктура, вимагає підходу до забезпечення стійкостікритичної інфраструктури, що враховує всі небезпеки і загрози.

Вставка 1.2. Цифрові загрози для критичної інфраструктури

Цифрові загрози можуть впливати на критичну інфраструктуру по-різному:

Шкідливе програмне забезпечення, що впливає на системи управління та контролю: Шкідливе програмне забезпечення Stuxnet, виявлене у 2010 році, продемонструвало, наприклад, вразливість систем управління складними промисловими процесами, такими як функціонування електростанцій, водо- і нафторозподільчих мереж. Безпосередній контроль над складними промисловими і технічними процесами, пов'язаними з об'єктами критичної інфраструктури, вимагає потужного технічного потенціалу. Атака на українську електромережу у 2015 році стала попереджувальним сигналом, який підкреслив витонченість атак та наявність інструментів для часткового контролю і порушення енергопостачання.

Програми-здирники, що вражають велику кількість комп'ютерів, можуть так само блокувати системи та впливати на операторів критичної інфраструктури в їхній повсякденній діяльності, що може мати потенційні наслідки для їхньої роботи. У 2017 році віруси-здирники Wannacry та NotPetya призвели до серйозних збоїв у роботі низки систем критичної інфраструктури в Європі, зокрема Національної служби охорони здоров'я Великої Британії, телекомунікаційної компанії Telefonica в Іспанії, німецької залізничної компанії Deutsche Bahn абоданської судноплавної компанії Maersk.

Розподілений контроль на пристроях Інтернету речей впливає на попит: Зростає занепокоєння щодо вразливості пристроїв Інтернету речей, які зазвичай мають низький рівень захисту від цифрових загроз. Контроль над великою кількістю пристроїв може бути використаний для створення шоку попиту на послуги комунальних підприємств. Наприклад, одночасне ввімкнення пристроїв може спричинити пік попиту на електроенергію, порушивши баланс між виробництвом та споживанням електроенергії, що вплине на стабільністьмережі.

Бекдори в апаратних компонентах критичної інфраструктури: Окрім програмного забезпечення, цифрові загрози можуть також походити від апаратних компонентів. Ланцюги постачання критично важливих галузей стали основною сферою уваги для політиків, наприклад, у зв'язку з постійним розгортанням технологій 5G. У контексті гібридних загроз зростає занепокоєння тим, що постачальники інформаційних технологій можуть навмисно вбудовувати апаратні та програмні бекдори в системи IT/OT, які використовуються для роботи критично важливої інфраструктури.

Джерело: Презентації та обговорення на семінарі ОЕСР з системного мислення для забезпечення стійкості та безпеки критичної інфраструктури (2018), доступне за посиланням: http://oe.cd/critinf

Новий ландшафт для інвестицій у критичну інфраструктуру стійкість

Окрім еволюції факторів ризику, сам сектор інфраструктури зазнає значних змін та еволюції, що може вплинути на його стійкість. По-перше, взаємозв'язок і взаємозалежність між інфраструктурними системами та між країнами значно зросли з глобалізацією, що збільшило потенціал для каскадного розвитку шокових подій.

По-друге, інновації та технологічний прогрес призводять до появи нових форм і типів інфраструктурних систем - від "розумних міст" до автономних транспортних засобів. Ці нові види "розумної інфраструктури" в основному використовують інновації, спрямовані на зниження витрат і підвищення ефективності, що може мати вплив на ризики і стійкість, які все ще необхідно враховувати та правильно розуміти. Паралельно з появою нової інфраструктури, у багатьох

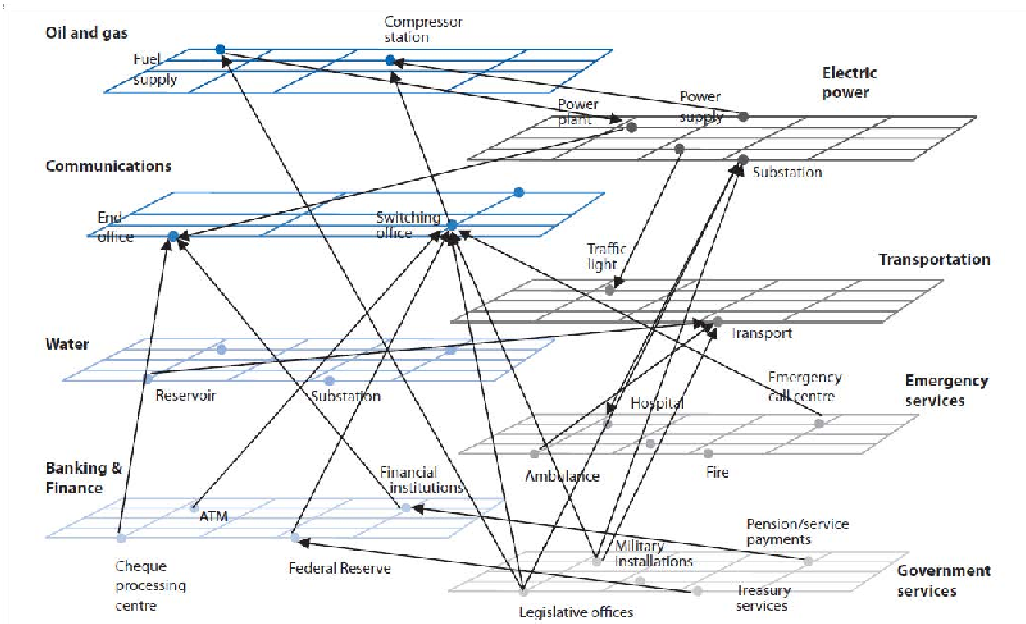
країнах OECD старіюча інфраструктура створює вразливі місця.

По-третє, інвестиції в інфраструктуру зростають у всьому світі, що створює ключову можливість для посилення стійкості з самого початку, за умови, що ці інвестиції інтегрують стійкість у свій дизайн.

Взаємозв'язок і взаємозалежність інфраструктурних активів і системзростає

Глобальні інвестиції в інфраструктуру, розгортання глобальних ланцюгів доданої вартості, а також розвиток інформаційно-комунікаційних технологій посилили взаємозв'язок і взаємозалежність між секторами та країнами по всьому світу. Збільшення потоків даних, товарів, людей та енергії живить глобальні ланцюги доданої вартості та підтримує економічне зростання. Критична інфраструктура - це центри, вузли і мережі дедалі складнішої павутини взаємозалежностей і взаємозв'язків, через які агенти загроз можуть переміщатися, а наслідки збоїв можуть бути каскадними. Тому збій або порушення роботи однієї системи критичної інфраструктури може мати далекосяжні наслідки в інших секторах або в інших місцях, іноді в глобальному масштабі (OECD, 2011[9]).

Рисунок 1.1. Взаємозалежності між утилітами та мережею



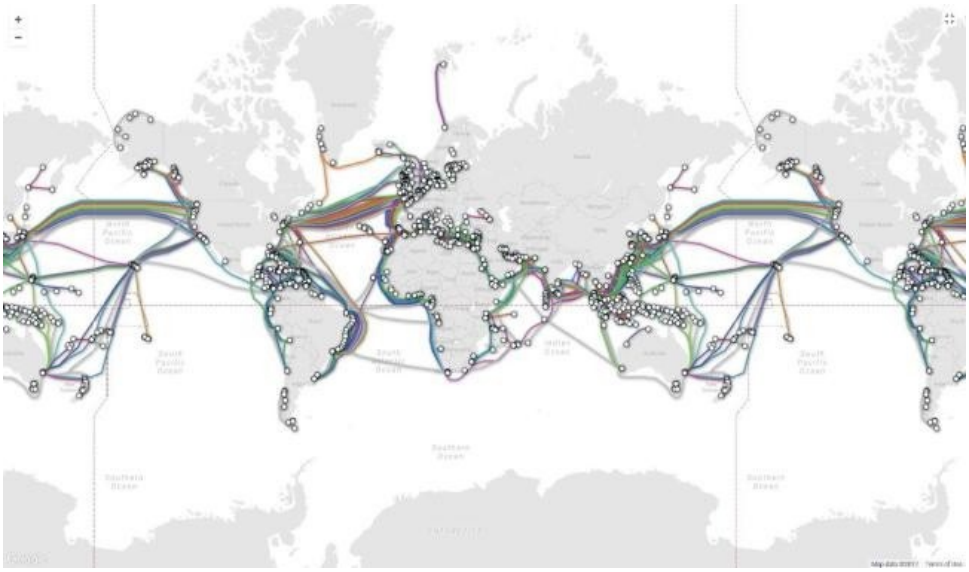
Джерело: NARUC (Національна асоціація регуляторних комісій у сфері комунальних послуг), (2005), Короткий огляд технічної допомоги з питань захисту критичної інфраструктури "Взаємозалежності між комунальними підприємствами та мережами: Що потрібно знати державним регуляторам", США, доступно за посиланням: www.naruc.org/Publications/CIP_Interdependencies_2.pdf

Наприклад, масштабні повені 2011 року в Бангкоку суттєво вплинули на автомобільну промисловість Японії, оскільки постачальники, розташовані в зоні затоплення, були виведені з ладу. Транскордонні інфраструктури, такі як високовольтні електромережі, є ще одним способом поширення збоїв. Збої в роботі електроенергетичних або телекомунікаційних систем можуть мати наслідки дляінших критично важливих секторів, які залежать від енергопостачання аботелекомунікаційних систем, від водоочищення до критично важливих галузей промисловості або державних систем (рис. 1.1).

Деякі сектори майже повністю залежать від ключової критичної інфраструктури: наприклад, авіаційний сектор залежить від Глобальної системи позиціонування (GPS) для управління маршрутами літаків по всьому світу; глобальний обмін
даними залежить від обмеженої кількості підводних кабелів, через які проходить

понад 90% світового трафіку даних (рис. 1.2).

Малюнок 1.2. Глобальна карта підводної кабельної системи



Джерело: Global Bandwidth Research Service, (2017), безкоштовна інтерактивна карта підводних кабелів TeleGeography,
доступний за посиланням https://www.telegeography.com/telecom-resources/submarine-cable-map/index.html

Інновації та діджиталізація трансформують інфраструктуру

Інновації трансформують інфраструктурні системи швидкими темпами, що має наслідки для ризиків і вразливостей, які мають бути інтегровані в політику стійкості та безпеки критичної інфраструктури. Від енергетичного до інформаційного та транспортного секторів відбуваються великі трансформації. Енергетичний сектор надає можливості для значних інновацій завдяки зростаючій частці відновлюваних ресурсів, розвитку інтелектуальних мереж, а також більш децентралізованим і локалізованим підходам до виробництва і споживання енергії. Стрімкий розвиток автономних транспортних засобів разом із прогресом у сфері штучного інтелекту обіцяє докорінно змінити транспортний сектор. Інформаційно- комунікаційні технології суттєво змінили спосіб обміну даними та спілкування у нашому повсякденному житті. Розумні міста, що керуються підходом, орієнтованим на дані, мають на меті поєднати інформаційну революцію зінноваційними та взаємопов'язаними міськими послугами, змінюючи вигляд мегаполісів, де проживає більшість населення планети.

Оскільки темпи інновацій продовжують прискорюватися, це має вплив на управління ризиками. Загалом, сучасні інноваційні тенденції свідчать про те, що більш децентралізовані системи та автономні механізми поступово замінюватимуть централізовані мережі з автоматизацією управління та контролю. Такі характеристики можуть посилити стійкість за рахунок надмірності та гнучкості. Однак це також може призвести до появи нових форм вразливостей: збільшення кількості слабких місць у децентралізованих системах і поширеного ризику більш руйнівних кібератак на ці системи, які все більше покладаються напотоки даних і кодування.

Зростаючі інвестиції в інфраструктуру створюють можливості для забезпечення стійкості

На наступні десятиліття заплановані значні інвестиції в нові об'єкти інфраструктури, і це є цінною можливістю забезпечити інтеграцію питань стійкості з самого початку.

Нещодавній аналіз ОЕСР свідчить про те, що для покриття потреб в інвестиціях в інфраструктуру на період 2016-2030 років необхідно 95трильйонів доларів США (OECD, 2017[10]). У багатьох країнах ОЕСР застаріла інфраструктура потребує інвестицій, а інновації надають можливості для того, щоб ці інвестиції сприяли підвищенню продуктивності.

Для того, щоб такі інвестиції в інфраструктуру були не лише правильними, але й стійкими, необхідно переглянути основні моделі управління інфраструктурою. ОЕСР розробила концепцію кращого управління інфраструктурою (OECD, 2017[11]), яка спрямована на реалізацію правильних проєктів у спосіб, що є економічно ефективним, доступним і викликає довіру у користувачів та громадян. Ця концепція наголошує на необхідності інтегрувати питання стійкості на початковому етапі при розробці цих інвестицій, щоб не лише захистити ці інвестиції від небезпек і загроз, але й забезпечити їхню безперебійну роботу під час стихійних лих.

Зміна клімату вимагатиме також проектування стійкої інфраструктури, адаптації або модернізації існуючої та розбудови захисної інфраструктури, причому деякі з них вважаються критично важливими. Робота ОЕСР щодо кліматично стійкої інфраструктури (OECD, 2018[12]) містить рекомендації щодо того, як забезпечити кліматичну стійкість за допомогою конкретних проектів, зміцнення сприятливого середовища для кліматичної стійкості та мобілізації державних і приватних інвестицій.

Посилання

Актон, Д. і М. Хіббс (2012), *Чому Фукісіму можна було попередити*, http://www.CarnegieEndowment.org/pubs. (дата перегляду: 25 лютого 2019 року). [24]

Александер, Д. (2013), "Вулканічний попіл в атмосфері та ризики для цивільної авіації: Дослідження в європейському кризовому менеджменті", *Міжнародний журнал науки про ризики стихійних лих*, Том 4/1, с. 9-19, http://dx.doi.org/10.1007/s13753-013-0003-0. [31]

Бах, К. та ін. (2013), "Додавання цінності дослідженням критичної інфраструктури та управлінню ризиками катастроф: концепція стійкості", *http://journals.openedition.org/sapiens* 6.1, https://journals.openedition.org/sapiens/1626 (дата звернення: 25 лютого 2019 р.). [25]

Critical Five (2014), *Формування спільного розуміння наративу щодо критичної інфраструктури*, https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative- critical-infrastructure-2014-508.pdf (дата перегляду: 25 лютого 2019 р.). [34]

Євроконтроль (2010), Попеляста хмара у *квітні та травні 2010 року: Вплив на повітряний рух*, https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/facts- and-figures/statfor/ash-impact-air-traffic-2010.pdf (станом на 25 лютого 2019 року). [29]

FEMA (2013), *Hurricane Sandy FEMA After-Action Report*, https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf (дата перегляду 25 лютого 2019 року). [22]

Фермандуа, А. (2011), *Чилі та землетрус: готовність, реагування та уроки*, http://dels.nas.edu/resources/static-assets/materials-based-on-reports/presentations/AmbassadorFermandois.pdf (дата перегляду: 25 лютого 2019 року). [27]

Флінн, С. (2015), *Підвищення стійкості критичної інфраструктури після буревію Сенді: Уроки для Нью-Йорка та нації*, Північно-Східний університет, Бостон, Массачусетс, http://dx.doi.org/10.17760/D20241717. [19]

Фу, Г., Дж. Ван і М. Ян (2016), "Анатомія пожежі та вибуху в порту Тяньцзінь: Процес і причини", *Process Safety Progress*, Vol. 35/3, pp. 216-220, http://dx.doi.org/10.1002/prs.11837. [16]

Гордон В., Фейрхолл А. і Ландман А. (2017), "Загрози інформаційній безпеці - наслідки для громадського здоров'я", *New England Journal of Medicine*, Vol. 377/8, с. 707-709, http://dx.doi.org/10.1056/NEJMp1707212. [15]

Хуан, П. і Дж. Чжан (2015), "Факти, пов'язані з вибухом 12 серпня 2015 року в Тяньцзіні, Китай", *Process Safety Progress*, Vol. 34/4, с. 313-314, http://dx.doi.org/10.1002/prs.11789. [17]

Hurricane Sandy Rebuilding Task Force (2013), *Стратегія відновлення після* урагану Сенді "*Сильніші громади, стійкий регіон"*, Міністерство житлового будівництва та міського розвитку США, https://archives.hud.gov/news/2013/HSRebuildingStrategy.pdf (дата перегляду: 25 лютого 2019 р.). [21]

IATA (2010), *IATA Economic Briefing Chart 1: Поширення і зсув шлейфу*, http://www.iata.org/economics (дата перегляду: 25 лютого 2019 року). [30]

Краусманн Е. та ін. (2016), *Космічна погода і критична інфраструктура: висновки і перспективи*, Об'єднаний дослідницький центр Європейської комісії, https://ec.europa.eu/jrc/en/publication/eur- scientific-and-technical-research-reports/space-weather-critical-infrastructures-findings-and- outlook (станом на 25 лютого 2019 року). [3]

Маттей, Т. (2017), "Приватність, конфіденційність та безпека медичної інформації: Lessons from the Recent WannaCry Cyberattack", *World Neurosurgery*, Vol. 104, pp. 972-974, http://dx.doi.org/10.1016/j.wneu.2017.06.104. [13]

Mazzocchi, M., F. Hansstein та M. Ragona (2010), *Хмара вулканічного попелу 2010 року та її фінансовий вплив на європейську авіаційну галузь*, Форум CESifo № 2, https://www.cesifo- group.de/DocDL/forum2-10-focus11.pdf (дата перегляду: 25 лютого 2019 року). [28]

МакГі, С. та ін. (2014), Взаємозв'язок *ризиків та каскадні ефекти в критичній інфраструктурі: Наслідки для структури Jyogo,* https://www.preventionweb.net/english/hyogo/gar/2015/en/bgdocs/McGee%20et%20al.,%202014.pdf (дата перегляду: 25 лютого 2019 року). [23]

Мінкель, Д. (2008), *Північно-східне відключення електроенергії 2003 року - п'ять років потому - Scientific American*, https://www.scientificamerican.com/article/2003-blackout-five-years-later/ (дата звернення: 25 лютого 2019 р.). [32]

Muir-Wood, R. (2011), *Розробка оптимальних механізмів пом'якшення та передачі ризиків для покращення управління ризиком землетрусів у Чилі,* Робочі документи ОЕСР з фінансів, страхування та приватного пенсійного забезпечення NO. 12, http://www.oecd.org/daf/fin/wp (дата перегляду: 25 лютого 2019 року). [26]

O'Dowd, A. (2017), "Велика глобальна кібератака вражає NHS і затримує лікування", *BMJ (Clinical research ed.),* Vol. 357, p. j2357, http://dx.doi.org/10.1136/bmj.j2357. [14]

ОЕСР (2018*)*, *Оцінка глобального прогресу в управлінні критичними ризиками*, Огляди ОЕСР щодо політики управління ризиками, Публікація ОЕСР, Париж, https://dx.doi.org/10.1787/9789264309272-en. [2]

ОЕСР (2018), *Оцінка реальної вартості катастроф: Потреба у кращих доказах*, Огляди політики управління ризиками ОЕСР, ОЕСР, Париж, https://dx.doi.org/10.1787/9789264298798-en. [5]

ОЕСР (2018), "Кліматостійка інфраструктура"*, Документ з екологічної політики ОЕСР*, № 14, ОЕСР, Париж, http://www.oecd.org/environment/cc/policy-perspectives-climate-resilient- infrastructure.pdf (дата перегляду: 25 лютого 2019 р.). [12]

ОЕСР (2018), *Протидія гібридним загрозам*, https://www.oecd.org/gov/risk/strategic-crisis- management-helsinki-agenda-2018.pdf (дата перегляду: 25 лютого 2019 року). [8]

ОЕСР (2017), *Правильне управління інфраструктурою: Рамки для кращого управління*, OECD Publishing, Париж, https://dx.doi.org/10.1787/9789264272453-en. [11]

ОЕСР (2017), *Інвестиції в клімат, інвестиції в зростання*, Публікація ОЕСР, Париж, https://dx.doi.org/10.1787/9789264273528-en. [10]

ОЕСР (2014), *Підвищення стійкості через інноваційне управління ризиками*, Огляди ОЕСР щодо політики управління ризиками, Публікація ОЕСР, Париж, https://dx.doi.org/10.1787/9789264209114- en. [20]

ОЕСР (2014), *Рекомендація Ради з управління критичними ризиками*, http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf (дата перегляду: 25 лютого 2019 року). [1]

ОЕСР (2014), *Басейн Сени, О-де-Франс, 2014: Стійкість до великих повеней*, Огляди політики управління ризиками ОЕСР, Публікація ОЕСР, Париж, https://dx.doi.org/10.1787/9789264208728-en. [7]

ОЕСР (2011), *Майбутні глобальні шоки: Покращення управління ризиками*, Огляди ОЕСР щодо політики управління ризиками, ОЕСР Publishing, Париж, https://dx.doi.org/10.1787/9789264114586- en. [9]

ОЕСР та EU JRC (2018), *Системне мислення для забезпечення стійкості та безпеки критичної інфраструктури - семінар ОЕСР/ JRC - ОЕСР*, http://www.oecd.org/gov/risk/workshop-oecd-jrc-system- thinking-for-critical-infrastructure-resilience-and-security.htm (дата звернення 25 лютого 2019 року). [41]

Роуз, А. та ін. (2012), *Загальні регіональні економічні втрати від перебоїв у водопостачанні для економіки округу Лос-Анджелес*, https://www.laedc.org/reports/WaterSupplyDisruptionStudy_November2012.pdf (дата звернення: 25 лютого 2019 р.). [6]

Swiss Re (2016), *Аналіз вибуху в порту Тяньцзіня | Swiss Re - провідний світовий перестраховик*, https://www.swissre.com/china/Analysis_of_Tianjin_Port_Explosion.html (дата звернення: 25 лютого 2019 року). [18]

U.S.-Canada Power System Outage Task Force (2004), Заключний *звіт про відключення електроенергії 14 серпня 2003 року в США та Канаді: Причини та рекомендації*, https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf (станом на 25 лютого 2019 року). [33]

Уряд Великої Британії (2017), *Зміна клімату у Великій Британії - оцінка ризиків у 2017 році*, http://www.gov.uk/ (дата звернення: 25 лютого 2019 року). [4]

Додаток 1.А. Уроки, винесені з минулих збоїв у роботі критичної інфраструктури

Атака програми-вимагача Wannacry 2017

Подія та її наслідки: Програма-вимагач Wannacry була поширена хакерами 13 травня 2017 року і заразила понад 200 000 комп'ютерів у 150 країнах (Mattei, 2017[13]). Wannacry - це шкідливе програмне забезпечення, яке блокує доступ користувачів і блокує файли в заражених системах, тому вимагають у жертв заплатити викуп у розмірі від 300 до 600 доларів США в обмін на ключ для дешифрування, щоб повернути зашифровані файли. Кібератака порушила рутинні операції і спричинила хаос у великих комерційних і державних установах, включаючи FedEx, Deutsche Bahn, Megafon, Telefonica і Російський центральний банк. Найбільше постраждала Національна служба охорони здоров'я Великої Британії (NHS), коли кібератака досягла інформаційно-технологічних систем у лікарнях. Як наслідок, лікарні та медичні заклади були змушені скасовувати операції, відкладати лікування та оголошувати про переведення в режим очікування в Англії та Шотландії (O'Dowd, 2017[14]). Система охорони здоров'я у Великій Британії була підірвана, і було висловлено велике занепокоєння щодо загроз конфіденційності та безпеки даних і записів пацієнтів.

Винесені уроки: Кібератака програма-вимагач Wannacry у 2017 році виявила вразливості та ризики для систем інформаційної безпеки, а також каскадні ефекти взаємозалежних і взаємопов'язаних систем критичної інфраструктури. Інформаційно-комунікаційні технології є основою для багатьох галузей, і цей кейс висвітлює наслідки кібератаки, що порушила нормальну роботу кількох комерційних і державних установ по всьому світу. Зокрема, він демонструє необхідність посилення безпеки інформаційних систем у сфері охорони здоров'я - секторі, що належить до критичної інфраструктури у більшості країн (O'Dowd, 2017[14]). Необхідно впроваджувати безперервність бізнес-планів, щоб забезпечити безперервність надання лікування та послуг під час збоїв. Найсучасніші технології можуть створити системи раннього попередження та забезпечити конфіденційність і безпеку даних і записів пацієнтів (Gordon, Fairhall and Landman, 2017[15]). Кібербезпека і захист інформаційно-комунікаційних технологій все частіше займають провідне місце в стратегіях безпеки критичної інфраструктури. Вони повинні враховувати розвиток технологій і потенційні нові вразливості та ризики, а також взаємозалежності нашого сучасного суспільства, яке значною мірою залежить від інформаційних систем. Безпека медичної інформації повинна бути першочерговим пріоритетом національної безпеки.

Вибух у порту Тяньцзіня, 2015

Подія та її наслідки: 12 серпня 2015 року в порту Тяньцзіня вибухнув склад небезпечних матеріалів. Це була станція нагляду за небезпечними матеріалами та ліцензований підрозділ Муніципальної транспортної комісії міста Тяньцзінь, що здійснював операції з небезпечними матеріалами в порту. Основним товаром у цьому складському бізнесі є небезпечні та токсичні матеріали і гази. Криза виникла внаслідок низки подій, починаючи з пожежної сигналізації о 22:50 і дзвінків до місцевої пожежної служби (Fu, Wang and Yan, 2016[16]). Пожежні бригади прибули швидко, але їм було важко отримати доступ до місця через численні високі штабелі контейнерів.

Близько 23:13 поліція та пожежники розпочали евакуацію людей з місця пожежі. Після пожеж з інтервалом у кілька секунд один за одним пролунали два вибухи, що спричинили підземні поштовхи, еквівалентні землетрусам магнітудою 2,2 і 2,9 балів, і призвели до утворення вогняних куль. Вибухи і пожежі призвели до госпіталізації 233 осіб, у тому числі трьох в тяжкому стані і трьох у вкрай важкому стані (Huang and Zhang, 2015[17]). Кількість загиблих сягнула 173 осіб, а страхові збитки сягнули $2,4 млрд, що зробило цю катастрофу найгіршою промисловою катастрофою в Китаї за останні роки (Swiss Re, 2016[18]). У понад 17 000 домогосподарств вибухом було вибито двері та вікна, а 779 підприємств зазнали збитків. Місце вибуху було розташоване поруч зі складом імпортних автомобілів компаній Volkswagen, Renault, Land Rover та інших, що призвело до того, що, за оцінками, згоріли тисячі імпортних нових автомобілів на суму понад 31 мільйон доларів.

Винесені уроки: Аварія в Тяньцзіні викликала занепокоєння щодо виробництва, зберігання, транспортування та використання небезпечних хімічних речовин - сектору, який вважається критичною інфраструктурою. Цей випадок виявив багато проблем, пов'язаних з недоліками контролю ризиків і порушеннями національних або галузевих стандартів (Swiss Re, 2016[18]). По-перше, правильна ідентифікація та розуміння небезпечних хімічних речовин, а також наукове управління ними стали першочерговим пріоритетом в управлінні ризиками та контролі. Щоб забезпечити безпеку і захист виробництва, зберігання і транспортування небезпечних хімічних речовин, необхідно проводити регулярні оцінки безпеки і перевірки на відповідність вимогам безпеки. Цей кейс також демонструє важливість обміну знаннями про небезпечні хімічні речовини, включаючи: класифікацію та визначення того, в яких галузях промисловості використовуються небезпечні хімічні речовини. Підприємства, які здійснюють діяльність, пов'язану з небезпечними хімічними речовинами, повинні бути зобов'язані визначити свої основні джерела небезпеки та провести оцінку безпеки джерел ризику. Крім того, сусідні підприємства повинні бути поінформовані та мати плани кризових ситуацій та евакуації на випадок аварійпоблизу.

Ураган Сенді, США 2012

Подія та її наслідки: Наприкінці жовтня 2012 року на Нью-Джерсі і Нью-Йорк обрушився буревій "Сенді", який завдав збитків на суму близько 68 мільярдів доларів США і серйозно вплинув на енергетику, транспорт, зв'язок, водопостачання та охорону здоров'я у великому столичному регіоні Нью-Йорка і Нью-Джерсі (Flynn, 2015[19]). За оцінками, 8,5 мільйона домогосподарств постраждали від нестачі електроенергії, а 5,4 мільйона людей постраждали від припинення роботи метрополітену. Збитки, завдані лише транспортним послугам, оцінюються у понад 10 мільярдів доларів США (OECP, 2014[20]). Після виходу на сушу стала очевидною взаємозалежність високорозгалуженої системи постачання і розподілу палива та електроенергетики на східному узбережжі Сполучених Штатів. На відміну від попередніх перебоїв у постачанні палива після ураганів у Сполучених Штатах, ця подія в першу чергу вплинула на споживачів, а не на виробників. Деякі з найбільш постраждалих районів вже були в невигідному становищі ще до приходу урагану, оскільки на їхніх автозаправних станціях не вистачало пального або ж запаси були повністю вичерпані через сплеск попиту на пальне в результаті підготовки населення до шторму. Після урагану Сенді багато автозаправних станцій, які мали запаси пального, не працювали, оскільки їхні насоси не працювали через перебої в електропостачанні. Водночас, автозаправні станції, які не мали запасів пального, не могли його поповнити, оскільки компресорні станції не мали допоміжних потужностей, необхідних для підтримання роботи міждержавних трубопроводів. Така взаємозалежність між паливним сектором та електроенергетикою, а також потенціал пов'язаних з нею каскадних впливів були непередбачуваними.

Винесені уроки: Було визначено чотири ключові сфери, відповідальні за збої в роботі критично важливої інфраструктури (Flynn, 2015[19]). По-перше, зацікавлені сторони мали слабке розуміння взаємозалежності критичної інфраструктури та потенціалу каскадних впливів

пов'язаних з перебоями в роботі системи (наприклад, зв'язок між мережею розподілу та роздрібної торгівлі, паливом та енергетичним сектором). По-друге, будівельні стандарти не еволюціонували з розвитком більш сучасних інженерних проектів, інструментів і практик, які здатні підвищити стійкість взаємозалежних систем. Критично важливі елементи транспортної системи, такі як тунелі, мости, залізничнілінії та станції метрополітену Нью-Джерсі/Нью-Йорку, які слугують основним засобом переміщення людей і товарів у регіоні, розташовані в низинних районах і в багатьох випадках не були побудовані таким чином, щоб протистояти повеням. По-третє, існуючі організаційні структури управління та регіональне управління не були достатньою мірою розвинені для вирішення питань взаємозалежності секторів життєзабезпечення - палива, електроенергії, води, транспорту, зв'язку та охорони здоров'я - від інших секторів. Наприклад, плани евакуації медичних закладів призвели до того, що всі пацієнти, окрім тих, хто перебував у найтяжчому стані, були вивезені до громади, яка зрештою не мала електроенергії, необхідної для роботи медичного обладнання в домашніх умовах, або доступу до транспорту, щоб доглядачі могли дістатися до пацієнтів, прив'язаних до дому. По-четверте, недостатньо економічних та/або політичних стимулів для розвитку стійкості, а в багатьох випадках інституційні та фінансові перешкоди стримують інвестиції в стійкість. Наприклад, багато державних і приватних операторів воліють приймати федеральну фінансову допомогу на випадок катастроф, а не покладатися на власні кошти для інвестування в заходи з підвищення стійкості. Недостатня регіональна координація та співпраця в метрополіях Нью-Йорка та Нью-Джерсі в управлінні ризиками, які катастрофи створюють для регіональної інфраструктури життєзабезпечення, є ще одним фактором, що посилює вплив катастроф.

Визнаючи масштабність відновлювальних робіт, Президент Сполучених Штатів створив Робочу групу з відновлення після урагану Сенді, якій було доручено "виявляти і працювати над усуненням перешкод на шляху до стійкої відбудови, беручи до уваги існуючі та майбутні ризики і сприяючи довгостроковій стійкості громад та екосистем у регіоні, що постраждав від урагану Сенді" (Hurricane Sandy Rebuilding Task Force, 2013[21]). У своєму звіті Робоча група відзначила особливо руйнівний вплив урагану на енергетичну, комунікаційну, транспортну, водопровідно-каналізаційну та медичну інфраструктуру регіону, а також пов'язані з ним значні затримки у реагуванні та відновленні і втрати в економічній діяльності. На основі уроків, отриманих під час процесу відновлення, Робоча група розробила 69 рекомендацій, майже половина з яких містила заклик до розвитку стійкості під час процесу відновлення. У відповідь на масове відключення електроенергії після урагану Сенді в Нью-Йорку і Нью-Джерсі Федеральне агентство з надзвичайних ситуацій (FEMA) на прохання президента створило Цільову групу з відновлення енергетики. Робоча група підтримала масові приватні зусилля з відновлення енергопостачання, в рамках яких електричні компанії уклали угоди про взаємодопомогу і направили понад 70 000 робітників до постраждалих районів. Це дозволило доставити повітрям 229 автомобілів для відновлення електропостачання і 487 осіб для допомоги Нью-Йорку і Нью-Джерсі у відновленні електропостачання ((FEMA, 2013[22])).

Великий східнояпонський землетрус, 2011

Подія та її наслідки: У 2011 році землетрус біля узбережжя Японії спричинив значні руйнування на суші і викликав серію великих хвиль цунамі, які серйозно вплинули на північно-східне узбережжя. Затоплення внутрішніх територій внаслідок цунамі, в свою чергу, призвело до великої ядерної аварії на атомній електростанції Фукусіма Дайічі (McGee та ін., 2014[23]). Хоча АЕС "Фукусіма-1" пережила землетрус відносно неушкодженою і навіть належним чином розпочала процедури аварійного вимкнення, конструкція майданчика була недостатньою для запобігання затопленню від цунамі, яке значно перевищувало висоту бар'єрів на майданчику. В результаті землетрусу було виведено з ладу електромережу, а коли цунамі пробило стіни об'єкту, подальша аварійна ситуація

призвела до затоплення резервних дизельних енергоблоків станції та вторинних резервних батарей постійного струму (Acton and Hibbs, 2012[24]). Без електроенергії станція не змогла забезпечити достатнє охолодження трьох своїх реакторів, які зрештою зазнали повного розплавлення 7-го рівня (за Міжнародною шкалою ядерних подій від 1 до 7), що перевищило навіть Чорнобильську катастрофу 1986 року (McGee et al., 2014[23]). За оцінками, 4,4 мільйона домогосподарств постраждали від скорочення електропостачання, яке забезпечувала Токійська електроенергетична компанія TEPCO Company. Швидкісна залізниця Сінкансен була закрита протягом двох тижнів (OECD, 2014[20]).

Винесені уроки: Аналіз, проведений після події, показав, що розплавлення можна було певною мірою запобігти. Інцидент міг би спричинити менше наслідків, якби електростанція врахувала концепцію стійкості при проектуванні. Наприклад, система охолодження станції функціонально залежала від гарантованого електропостачання, а реакція пожежної бригади могла б бути більш своєчасною і зменшити наслідки, якби не були заблоковані транспортні шляхи (Bach та ін., 2013[25]). Хоча японська ядерна промисловість мала найвищі у світі стандарти ядерної безпеки з точки зору управління сейсмічними ризиками, це могло статисяна шкоду врахуванню ширшого спектру потенційних (побічних) ризиків. Ці фактори демонструють критичну роль ефективних регулюючих органів і необхідність регулярних перевірок безпеки, які враховують і ведуть до включення як динамічного і мінливого ландшафту загроз, так і сучасних передових практик (Acton and Hibbs, 2012[24]).

Землетрус у Чилі 2010

Подія та її наслідки: Землетрус 2010 року, що стався 27 лютого біля узбережжя центрального Чилі, призвів до загальних збитків на суму 30 мільярдів доларів США (18% ВВП), з яких 20,9 мільярда доларів США (12,7% ВВП) було завдано через пошкодження інфраструктури. Землетрус зачепив регіон, на який припадає 30-40% національного виробничого потенціалу. Майже вся комерційна діяльність у цьому регіоні була призупинена на кілька днів, і хоча більшість галузей промисловості змогли відновити виробництво, деякі основні галузі, зокрема, пов'язані з виробництвом целюлозно-паперової продукції, виноробством та нафтопереробкою, не здійснювали комерційної діяльності або значно скоротили її протягом декількох місяців. Загальний спад національної економічної активності в березні 2010 року оцінювався на рівні 5%. Економічні негаразди продовжувалися протягом наступних трьох місяців, і нарешті повернулися до рівня, що передував землетрусу, у липні
2010 року (Muir-Wood, 2011[26]). Наслідки землетрусу могли б бути набагато гіршими, якби не цілеспрямоване планування в енергетиці та суворі будівельні норми, розроблені з урахуванням сейсмічного ризику (Fermandois, 2011[27]).

Винесені уроки: Аналізуючи наслідки землетрусу 2010 року, уряд Чилі вжив заходів для усунення виявлених вразливостей. На оперативному рівні уряд Чилі взяв на себе зобов'язання вирішити проблеми з перебоями зв'язку і моніторингу, що сталися в 2010 році, інвестувавши кошти в процеси моніторингу в режимі реального часу і надійні телекомунікаційні системи з резервними копіями (Fermandois, 2011[27]).

Ісландська хмара попелу, 2010

Подія та її наслідки: У квітні 2010 року ісландський вулкан Ейяф'ятлайокудль вивергнув величезну хмару попелу, яка поступово рухалася небом Європи. Як наслідок, європейські органи управління повітряним рухом оголосили зони заборони польотів для 20 країн у повітряному просторі Європи через потенційно небезпечні умови потрапляння дрібних частинок попелу в двигуни літаків, що може призвести до виходу з ладу обладнання (Mazzocchi, Hansstein та Ragona, 2010[28]). Британський уряд взяв на себе ініціативу закриття аеропортів, спираючись на інформацію лондонської філії Міжнародної служби спостереження за вулканами авіакомпанії "Міжнародні авіалінії" (International Airways Volcano Watch), яка підтримувала зв'язок з Національною службою управління повітряним рухом (NATS) Великобританії (Alexander, 2013).

Інші країни Північної та Центральної Європи наслідували цей процес. Рішення про закриття ґрунтувалися на приблизних даних про розсіювання попелу, але не було надано ні даних, ні карт, що вказували б на точний рівень концентрації попелу в небі всієї Європи. Закриття європейських аеропортів і повітряного простору тривало понад сім днів, було скасовано до 100 000 рейсів, що вплинуло на 10 мільйонів пасажирських подорожей (Eurocontrol, 2010[29]). Авіаційна галузь зіткнулася з високими витратами до 400 мільйонів доларів США на день (IATA, 2010[30]). Пасажири, що опинилися у скрутному становищі, шукали інші види транспорту, зокрема, поїзди, транскордонну мережу Eurostar та пороми, які не були ні обладнані, ні гнучкіші для такого попиту. Якби криза тривала довше, відсутність інтеграції між різними видами транспорту в рамках Європейської транспортної системи зазнала б серйозних проблем з переміщенням застряглих людей і товарів, а також зазнала б величезних економічних втрат (Alexander, 2013[31]).

Винесені уроки: Транспортний сектор, який включає авіацію та аеропорти, вважається критично важливою інфраструктурою в більшості країн. Криза, пов'язана з хмарою попелу в Ісландії, виявила необхідність посилення координації між науковими спільнотами та каналами обміну інформацією з органами влади для прийняття більш обґрунтованих рішень, що особливо важливо під час криз (Alexander, 2013[31]). Фізичні порогові значення щільності повітряного попелу для безпечного польоту були визначені дещо довільно і не враховували, що хмара не є однорідною небезпекою для авіації. Однак наявна інформація стала основою для прийняття ризикованих рішень щодо обмеження повного доступу до повітряного простору і призвела до збільшення кількості перебоїв у роботі європейських транспортних систем. Крім того, відсутність заздалегідь розроблених процедур і планування для управління такого роду кризами призвела до імпровізованого реагування на динамічні і мінливі метеорологічні умови (Alexander, 2013). Для забезпечення безпечних, прагматичних і скоординованих рішень необхідний тісніший зв'язок між оперативними, регуляторними і політичними органами (Eurocontrol, 2010[29]). Цей випадок показує, що управління кризами вимагає посилення регіональної та міжнародної координації для реагування на перебої в роботі транспорту, а також необхідності розробки планів безперервності бізнесу і планів на випадок надзвичайних ситуацій для вирішення проблем пасажирів, які опинилися в скрутному становищі, та економічних витрат (Mazzocchi, Hansstein and Ragona, 2010[28]).

Відключення електроенергії на північному сході США та в Канаді, 2003

Подія та її наслідки: 14 серпня 2003 року несправність високовольтної лінії електропередач на півночі Огайо, яка зачепилася за зарослі дерев, призвела до відключення системи (Minkel, 2008[32]). Зазвичай така подія мала б викликати тривогу, але система сигналізації не спрацювала. Поки оператори намагалися виявити проблему, додаткові лінії зачепили дерева і вимкнулися, що призвело до перевантаження ліній, які залишалися в робочому стані. Через дві години після виникнення проблеми перевантажені лінії вимкнулися, що призвело до каскадних збоїв у південно-східній Канаді та восьми штатах на північному сході США. Відключення вплинуло на низку інших критично важливих секторів інфраструктури, включаючи енергетику, зв'язок, фінанси, охорону здоров'я, харчову промисловість, водопостачання, транспорт, безпеку, уряд і виробництво. Зрештою, відключення електроенергії вплинуло на 50 мільйонів людей як у США, так і в Канаді, а його вартість оцінюється в 6 мільярдів доларів США (Minkel, 2008[32]).

Вивчені уроки: Відключення електроенергії у 2003 році слугує прикладом проблем, пов'язаних з різним рівнем фрагментарного контролю, підзвітності та повноважень щодо критичної інфраструктури (U.S.-Canada Power System Outage Task Force, 2004[33]). В офіційному двосторонньому урядовому звіті, присвяченому дослідженню відключення Північно-Східної енергосистеми у 2003 році, описані прямі причини та фактори, що сприяли цьому інциденту, в тому числі "нездатність підтримувати адекватну підтримку реактивної потужності; нездатність забезпечити роботу в безпечних межах; неадекватне управління рослинністю; неадекватна підготовка операторів; нездатність ідентифікувати аварійні ситуації;

і повідомляти про це сусіднім системам; і неналежна видимість в регіональному масштабі над великою енергосистемою". Останнє призвело до ситуацій, коли, наприклад, в Оттаві мости, які перетинали Квебек, були наполовину освітлені, тому що в Гатіно, Квебек, електроенергія все ще подавалася, але, схоже, не було можливості передати її на сторону провінції Онтаріо. Ці висновки перетворилися на кілька важливих уроків, викладених у формі рекомендацій. Наприклад, Цільова група стверджує, що регуляторні органи, електроенергетичний сектор та інші зацікавлені сторони повинні дотримуватися високих стандартів надійності, використовуючи ринкові механізми, коли і де це можливо, але завжди віддаючи перевагу високій надійності перед комерційними цілями, якщо виникають конфлікти між ними. У звіті також підкреслюється, що і регулятори, і споживачі повинні визнати, що надійність вимагає інвестиційних та операційних витрат, які бізнес не захоче брати на себе, якщо ці витрати не супроводжуватимуться гарантіями з боку регуляторів щодо можливості їх відшкодування. Під впливом аналізу інциденту з відключенням електроенергії Конгрес США прийняв Закон про енергетичну політику 2005 року, який дозволив Федеральній комісії з регулювання енергетики (FERC) запровадити нові стандарти Північноамериканської корпорації з надійності електропостачання; через п'ять років після інциденту FERC затвердила 96 нових стандартів надійності (Minkel, 2008[32]).

2. Виклики управління для стійкості критичної інфраструктури

У цьому розділі розглядається мінливий контекст політики щодо критичної інфраструктури та представлено низку управлінських викликів, пов'язаних з розробкою та впровадженням політики у цій сфері. Вирішення проблеми зростаючої взаємозалежності та складності критичної інфраструктури вимагає переходу від захисту окремих активів до системного підходу до забезпечення стійкості. У цьому розділі пропонується низка складових для впровадження такого системного підходу, а також обговорюється роль урядів та зацікавлених сторін у забезпеченні стійкості критичної інфраструктури. Наприкінці висвітлюються виклики в управлінні, які необхідно подолати політикам, щоб пристосувати політику щодо критичної інфраструктури до динамічного ландшафту ризиків нашого часу

Від захисту критичної інфраструктури до стійкості

Зростання невизначеності вимагає більш адаптивної політики щодо критичної інфраструктури

Протягом десятиліть уряди приділяли особливу увагу важливості критичної інфраструктури та пов'язаним з нею вразливостям. До середини 2000-х років більшість політик і заходів у сфері критичної інфраструктури були зосереджені на захисті активів. Новий підхід виявився необхідним з огляду на зростання вартості катастроф, масштабних терористичних атак, таких як теракти 11 вересня 2001 року в США, вибухи в Лондоні 2005 року, а також дедалі частіших кібератак, спрямованих на об'єкти критичної інфраструктури. Уряди почали зміщувати акцент із захисту критичної інфраструктури на стійкість критичної інфраструктури, щоб пристосувати свою політику до мінливого ландшафту ризиків (Critical Five, 2014[34]).

Зосередження на стійкості не виключає захисту або міркувань безпеки. Він радше розширює об'єктив рамок критичної інфраструктури, інтегруючи такі поняття, як адаптивність, гнучкість і надійність (Flynn, 2008[35]) (Barami, 2013[36]). В рамках парадигми захисту критичної інфраструктури зацікавлені сторони розглядають управління ризиками критичної інфраструктури переважно з точки зору активів з акцентом на безпеку і фізичні заходи для запобігання порушенням критичної інфраструктури в цілому.

Перехід до перспективи, що базується на стійкості, зумовлений значним ступенем невизначеності щодо інтенсивності та складності майбутніх катастроф та їхнього потенційного впливу на інфраструктуру. Наприклад, невизначеність, пов'язану зі зміною клімату, необхідно враховувати при плануванні довгострокових інвестицій в інфраструктуру і при розробці заходів, пов'язаних із забезпеченням безперервності надання послуг. Характер невизначеності, пов'язаної зкатастрофами, вимагає поетапних підходів, які готують активи і системи до швидкого відновлення і реабілітації.

Визначення стійкості критичної інфраструктури

Стійкість можна визначити як здатність критичної інфраструктури поглинати збурення, відновлюватися після збоїв і адаптуватися до мінливих умов, зберігаючи при цьому по суті ті ж самі функції, що й до руйнівної події (OECD, 2014[20]); (Chang et al., 2014[37]). Це визначення включає незамінну здатність протистояти інцидентам без втрати функціональності, обмежуючи тривалість перерви в наданні послуг, а також мінімізуючи час відновлення.

Таким чином, коли відбувається інйидент, цілі стійкості критично важливої інфраструктури можуть бути виміряні у двох вимірах: обмеження масштабу пошкоджень та обмеження тривалості перерви у наданні послуг, спричиненої пошкодженнями. Важливо зазначити, що відновлення не обов'язково означає повернення до попереднього стану, який існував до інциденту, але може передбачати зміну, адаптацію до нових умов та покращення функціональності систем з плином часу.

У цьому контексті забезпечення стійкості критичної інфраструктури здійснюється шляхом забезпечення поєднання декількох ключових якостей (OECD, 2011[9]):

- *Надійність* описує здатність продовжувати роботу або залишатися стійкими перед обличчям катастрофи. Це передбачає проектування структур або систем, які є достатньо міцними, щоб витримати передбачувані потрясіння. Це також передбачає інвестування в елементи критично важливої інфраструктури та їх підтримку, щоб вони могли витримати події з низькою ймовірністю, але з високими наслідками.

- *Резервування* описує здатність продовжувати роботу завдяки заміні або резервним системам, які можуть бути задіяні, якщо щось важливе вийде з ладу або перестане працювати.

- *Винахідливість* описує здатність вміло керувати подією в міру її розгортання. Це включає в себе визначення варіантів, пріоритетів, що потрібно зробити, щоб контролювати збитки і почати їх пом'якшувати, а також донесення рішень до людей, які будуть їх виконувати. Винахідливість залежить насамперед від людей, а не від технологій. Швидке відновлення - це здатність повернутися до нормального життя якнайшвидше після катастрофи. Плани на випадок непередбачуваних ситуацій та безперервності бізнесу, ефективні аварійні служби та засоби доставки потрібних людей і ресурсів у потрібне місце мають вирішальне значення.

- *Адаптивність* описує засоби для засвоєння нових уроків, які можна винести з катастрофи. Вона передбачає перегляд планів, модифікацію процедур і впровадження нових інструментів і технологій, необхідних для підвищення надійності, винахідливості та здатності до відновлення до наступної кризи.

Міжнародні фреймворки підтримки стійкості критичної інфраструктури

Виходячи з цього визначення, державна політика, спрямована на підвищення стійкості критичної інфраструктури, повинна поєднувати заходи, спрямовані на стимулювання резервування, надійності систем, резервних потужностей, швидкого відновлення та адаптації до нових ризиків або мінливих факторів ризику.Рекомендація OECP з управління критичними ризиками визнає важливість досягнення стійкості критичної інфраструктури для посилення управління ризиками на національному рівні та зменшення взаємного та каскадного впливу надзвичайних ситуацій (OECD, 2014[1]). Для досягнення цієї мети Рекомендаціязакликає уряди до дій:

- Визначити, де перебої в роботі критично важливої інфраструктури та ланцюгів постачання можуть призвести до перехресного впливу на інші галузі та географічні кордони, а також спричинити каскадні ефекти.

- Розробити фіскальні та регуляторні варіанти, які сприятимуть створенню резервних потужностей, диверсифікації або резервних систем для зменшення ризику збоїв і тривалих періодів перебоїв у роботі систем критичної інфраструктури.

- Координувати проектування мереж критичної інфраструктури (наприклад,енергетичних, транспортних, телекомунікаційних та інформаційних систем) з політикою містобудування та управління територіями.

- Використовувати можливості приватного сектору для розбудови стійкої інфраструктури.

- Заохочувати бізнес вживати заходів для забезпечення безперервності бізнесу, приділяючи особливу увагу операторам критичної інфраструктури, шляхом розробки стандартів та інструментарію, призначених для управління ризиками, що загрожують операціям або наданню основних послуг.

- Забезпечити функціонування критично важливої інфраструктури, інформаційних систем та мереж після інциденту.

- Забезпечити наявність та застосування планів реагування на випадок надзвичайних ситуацій на випадок інциденту, який порушує функціонування мереж критично важливої інфраструктури.

Після прийняття Рекомендації OECP з управління критичними ризиками у 2014році на кількох міжнародних форумах було визнано важливість стійкості інфраструктури. Ісе-Сімські принципи G7 щодо сприяння якісним інвестиціям в інфраструктуру (G7, 2016[38]) підкреслюють стійкість до стихійних лих, тероризму та ризиків кібератак

для забезпечення надійної експлуатації та економічної ефективності з огляду на важливість життєвого циклу. Аналогічним чином, Сендайська рамкова програма ООН зі зниження ризиків стихійних лих (Управління ООН для зменшення ризиків катастроф, 2015[39]) закликає країни "суттєво зменшити шкоду, завдану катастрофами критично важливим об'єктам інфраструктури та порушення надання базових послуг", а Ціль сталого розвитку ООН №9 - розбудовувати стійку до тероризму інфраструктуру. Що стосується конкретно тероризму, Резолюція Ради Безпеки ООН 2341 визнає "зростаючу важливість забезпечення надійності та стійкості критично важливої інфраструктури та її захисту від терористичних атак для національної безпеки, громадської безпеки та економіки відповідних держав, а також добробуту і благополуччя їхнього населення" (Рада Безпеки Організації Об'єднаних Націй, 2017[40]). Всеохоплююча Рамкова програма ОЕСР з управління інфраструктурою (OECD, 2017[11]) також виділяє стійкість інфраструктури як один з
10 ключових викликів в управлінні.

Прийняття системного підходу до стійкості критичної інфраструктури

Перехід від захисту критичної інфраструктури до забезпечення її стійкості має на меті врахувати ключові зміни в ландшафті ризиків, що характеризуються зростанням невизначеності. Для того, щоб краще інтегрувати складність, взаємозалежність і взаємопов'язаність критичної інфраструктури, прийняття системного підходу до стійкості критичної інфраструктури забезпечує додаткові перспективи.

Барамі (2013) підкреслює складний і багатогранний характер стійкості критичної інфраструктури. Барамі застосовує багаторівневий підхід, що ґрунтується на оцінці ризиків і враховує взаємозалежності складних інфраструктур, розглядаючи при цьому потенційні рішення, які можна застосувати протягом життєвого циклу інфраструктурної системи (тобто, проектування, будівництво та експлуатація). Таким чином, стійкість визначається не як єдиний результат або виключно здатність до відновлення після катастрофи, а скоріше як динамічний процес, який застосовує метод, заснований на ризиках і життєвому циклі, для усунення вразливостей систем критичної інфраструктури, роблячи системи більш відмовостійкими, ефективними, розумнішими і здатними краще адаптуватися до несподіваних викликів (Barami, 2013[36]).

Семінар Форуму ОЕСР з питань ризиків високого рівня "Системне мислення для забезпечення стійкості критичної інфраструктури" (OECD and EU JRC, 2018[41]) розширив це поняття системного підходу, застосованого до стійкості критичної інфраструктури, і запропонував низку ключових ознак що має враховувати державна політика у цій сфері:

- *Комплексні небезпеки та загрози*: Політики протидії окремим загрозам недостатньо для розбудови стійкості інфраструктури. Наслідки урагану Сенді для критичної інфраструктури в Нью-Йорку, де після 11 вересня були проведенізначні захисні заходи, продемонстрували, що одних лише захисних заходів недостатньо для подолання низки потенційних порушень у роботі критичної інфраструктури та пов'язаних з ними каскадних ризиків. Прийняття підходу до забезпечення стійкості критичної інфраструктури, що враховує всі небезпеки і загрози, дозволяє політикам і операторам краще підготуватися до несподіванок.

  Системний рівень: Спочатку політика захисту критичної інфраструктури зосереджувалася насамперед на впровадженні заходів захисту на рівні об'єктів. Однак інфраструктурні активи, як правило, є лише компонентами більш широкої складної системи, яка повинна розглядатися в повному обсязі в рамках комплексної стратегії стійкості. Деякі активи системи є більш важливими, ніж інші, наприклад, через залежність або (не)існуючу надмірність. Системний підхід дозволяє визначити пріоритетність найбільш важливих компонентів за допомогою моделювання залежностей та оцінки критичності, а також усунути слабкі місця, які в іншому випадку створюють критичні вразливості для всієї системи.

- *Багатогалузевий*: подолання взаємозалежностей вимагає від політиків та операторів вийти за рамки системного підходу і спрямувати зусилля на всі сектори критичної інфраструктури в рамках комплексної політики забезпечення стійкості. Хоча оператори інфраструктури, як правило, добре усвідомлюють власну залежність від критично важливих секторів (наприклад, електроенергетика, платіжні системи), вони можуть не усвідомлювати залежність інших секторів від їхніх власних послуг. Від картографування взаємозалежностей до розробки спільних цілей безперервності бізнесу, багатосекторальний підхід є важливим для всеосяжної політики забезпечення стійкості критичної інфраструктури.

- *Транскордонний вимір*: Аналогічно, взаємозалежність і взаємопов'язаність не можна повністю зрозуміти, не враховуючи їх міжнародний вимір. Небезпеки і загрози не зупиняються на національних кордонах. У деяких випадках системи критичної інфраструктури перетинають кордони, надаючи послуги в декількох країнах. Оператори інфраструктури також можуть управляти критичною інфраструктурою в декількох країнах. Це робить інтеграцію міжнародного співробітництва в політику забезпечення стійкості критичної інфраструктури ще більш актуальною. Обмін передовим досвідом, прийняття спільних підходів, розробка спільних стандартів у сфері стійкості критичної інфраструктури - це ті варіанти політики, які можуть сприяти міжнародному співробітництву в цій сфері.

- *Підхід на основі життєвого циклу*: На різних етапах життєвого циклу інфраструктури можуть застосовуватися різні заходи стійкості та безпеки: інтеграція надійності та резервування вимагає інвестицій на етапі проектування, тоді як розробка планування безперервності бізнесу більше стосується етапу експлуатації, а адаптивність може ґрунтуватися на модернізації інфраструктури. Таким чином, важливо розробити комплексну політику, яка забезпечить стійкість протягом усього життєвого циклу критично важливої інфраструктури, починаючи з етапу проектування і закінчуючи її експлуатацією,обслуговуванням і модернізацією.

- *Повний цикл управління ризиками*: Комплексна політика стійкості повинна включати заходи протягом усього циклу управління ризиками, від оцінки ризиків, запобігання ризикам, готовності до надзвичайних ситуацій і реагування на них до відновлення і реконструкції (Moteff, 2012[42]). Стійкість критичної інфраструктури має свої особливості на кожному з цих етапів. Оцінка ризиків повинна включати оцінку залежностей і критичності. Запобігання ризикам включає заходи з підвищення надійності на етапі проектування, а також спеціальні діалоги з підвищення обізнаності з операторами інфраструктури. Готовність до надзвичайних ситуацій та реагування на них вимагають спеціальних систем оповіщення, заходів з безперервності бізнесу та резервного копіювання, а також спеціальних аварійних команд та можливостей. Етап відновлення та реконструкції повинен включати в себе деградований режим, плани швидкого відновлення, а також спеціальні схеми фінансування, в тому числі для відновлення кращого стану об'єктів.

- *Ризик-орієнтований та багаторівневий підхід*: Враховуючи значний ступінь невизначеності щодо інтенсивності та складності майбутніх катастроф, різноманітні виміри вразливості інфраструктурних систем та всі взаємозв'язки між цими системами, визначення пріоритетності заходів з підвищення стійкості має важливе значення. Лише багаторівневий підхід, що базується на оцінці ризиків, може врахувати складні взаємозалежності інфраструктури, одночасно розглядаючи потенційні рішення, які можуть бути застосовані в інфраструктурних системах протягом усього життєвого циклу (Barami, 2013[36]).

Виклики в управлінні для забезпечення стійкості критичної інфраструктуриполітики

Численні зацікавлені сторони для забезпечення стійкості інфраструктури

Проектування інфраструктури, інвестиції, будівництво, власність, експлуатація або регулювання залучають багато зацікавлених сторін, які відіграють певну роль у розбудові стійкості.

Як зазначено в Рамковій програмі ОЕСР щодо кращого управління інфраструктурою (OECD, 2017[11]), існує багато способів надання інфраструктурних послуг. Роль державного сектору може бути різною, і існують гібридні форми. Оскільки в останні десятиліття власність на інфраструктуру переходить від державного забезпечення через державні підприємства до приватизації, контроль держави над інфраструктурними активами зменшується. Аналогічно, традиційні державні закупівлі або державно-приватне партнерство - впливатиме на те, як стійкість може бути інтегрована в проєктування та експлуатацію інфраструктури. У цьому контексті управління ризиками та стійкість стають нерозривно пов'язаними з ширшим питанням управління інфраструктурою та формуванням політики. З огляду на сучасні тенденції до збільшення глобальних інвестицій в інфраструктуру, забезпечення належного масштабування інвестицій у стійкість вимагає, щоб моделі управління інфраструктурою включали стійкість як один з критеріїв прийняття рішень. Власники та оператори об'єктів критичної інфраструктури несуть основну відповідальність за захист своїх активів і підтримання безперервності послуг, які вони надають. Незалежно від того, чи є вони державними, приватними або гібридними, власники, як правило, хочуть захистити свої капітальні активи від пошкодження або знищення внаслідок катастрофи або іншого інциденту. Аналогічно, оператори зацікавлені у підтримці безперервності надання послуг та уникненні перебоїв не лише через збитки, яких вони можуть потенційно зазнати у разі припинення надання послуг, але й через занепокоєння своєю репутацією та іміджем перед клієнтами або користувачами. Тим не менш, власники та оператори не можуть самостійно усунути всі вразливі місця і можуть не мати стимулів для оцінки повного огляду всього обсягу своїх взаємозалежностей. Взаємозалежність між секторами критичної інфраструктури та потенційні каскадні ефекти, які можуть виникнути в разі катастрофи, вимагають міжсекторальної співпраці.

Яка роль урядів?

Уряди відіграють ключову роль у забезпеченні стійкості критичної інфраструктури,оскільки вони відповідають за забезпечення безпеки громадян, а також є розробниками інфраструктурної політики та регуляторами, власниками або операторами в деяких випадках, а також основними користувачами або клієнтами. Посадові особи, відповідальні за управління ризиками, повиннікоординувати роботу між урядjv і забезпечувати, щоб всі відповідні політичні цілі могли бути досягнуті одночасно, збалансовуючи відповідні компроміси. Цей перелік висвітлює різноманітні аспекти,які уряди повинні враховувати при розробці національної політики безпеки та стійкості критичної інфраструктури.

По-перше, як зазначено в Рекомендаціях ОЕСР з управління критичними ризиками, уряди несуть відповідальність за встановлення рівнів готовності на національному рівні в рамках національної стратегії управління критичними ризиками. У новому ландшафті критичних ризиків, з якими стикаються уряди, встановлення національних цілей у сфері безпеки та стійкості критичної інфраструктури має фундаментальне значення для сприяння загальній стійкості націй. Більшість країн ОЕСР вже розробили стратегії та програми з безпеки та стійкості критичної інфраструктури (див. Розділ 3). З огляду на взаємозалежність між різними секторами інфраструктури, уряд також має відігравати важливу роль у забезпеченні належного розкриття та вирішення цієї взаємозалежності, а також уникнення пов'язаних з нею прогалин у політиці.

По-друге, уряди відіграють ключову роль у формуванні інфраструктурної політики та нагляді за нею. Забезпечення того, щоб інфраструктура якнайкраще сприяла підвищенню продуктивності та забезпечувала рівні можливості і рівний доступ до послуг для громадян, є ключовими цілями політики у сфері надання інфраструктурних послуг (ОЕСР, 2017[11]). Функція нагляду та регулювання уряду

можуть бути делеговані секторальному регулятору, який матиме повноваження встановлювати ключові цілі та регулювати діяльність у секторі. У цьому відношенні, занепокоєння щодо стійкості та необхідності забезпечення достатніх резервних потужностей, можливо, доведеться збалансувати з необхідністю підтримувати рівні правила гри та стимулювати конкуренцію, щоб знизити ціни та покращити споживчий надлишок, не ставлячи при цьому під загрозу прийнятний рівень ризиків.

По-третє, уряд може бути власником та оператором інфраструктури або через пряме надання послуг, або через державні підприємства, або через інші способи надання інфраструктурних послуг. Застосовуючи стандарти стійкості та безпеки до інфраструктурних систем, за які він відповідає, уряд може стати прикладом для наслідування. Це також може бути показовим для уряду щодо витрат, понесених на інвестиції в стійкість, що потенційно може краще інформувати процес прийняття рішень і пов'язаний з цим аналіз витрат і вигод для інвестицій в стійкість критичної інфраструктури.

Нарешті, уряди також є користувачами або клієнтами інфраструктури, а отже, залежать від різних об'єктів критичної інфраструктури для підтримки власної безперервності. Таким чином, уряди мають особливі очікування щодо безперервності критичної інфраструктури, яка забезпечує виконання ключових функцій уряду. Деякі країни, наприклад, визначили уряд як один із секторів критичної інфраструктури. Питання, яке постає перед урядами при розробці політики щодо критичної інфраструктури, полягає в тому, чи вимагатиме її безперервність певних рівнів стійкості та/або стандартів стійкості критичної інфраструктури порівняно з іншими секторами.

Партнерство задля забезпечення стійкості критичної інфраструктурита вирішення пов'язаних з цим проблем управління

Хоча уряди продовжують володіти, інвестувати, експлуатувати та регулювати критично важливу інфраструктуру в деяких секторах, все більша частка критично важливої інфраструктури перебуває у приватній власності або під управліннямприватного сектору. У деяких країнах приватний сектор управляє більшістю цих інфраструктурних систем. Тому стійкість цих систем залежить від партнерства урядів з операторами інфраструктури з державного і приватного секторів у зусиллях із забезпечення стійкості шляхом створення відповідних механізмів управління.

Оператори критичної інфраструктури та уряди часто погоджуються з необхідністю захисту ключових активів і підтримки їхніх послуг, але погляди на необхідний рівень стійкості безпеки, засоби його досягнення та вимоги, які повинні застосовуватися, можуть відрізнятися. Серед політичних питань, які потребують вирішення, - критичність конкретних об'єктів для більш широкої мережі, забезпечення рівних умов для операторів, прийнятна тривалість "простою", розподіл витрат між різними зацікавленими сторонами на забезпечення стійкості та уникнення потенційних ситуацій "фрірайдингу".

Політичні підходи, які обмежуються обов'язковими заходами, що вимагають від операторів критичної інфраструктури вжиття заходів з підвищення стійкості, не завжди є найбільш прийнятними, оскільки це може, серед іншого, стати проблемою конкуренції, а також готовності та платоспроможності постачальників послуг. Додаткові підходи до управління, які сприяють регулярному обміну інформацією, взаємній довірі та потенційно збалансованій державній фінансовій підтримці інвестицій у підвищення стійкості критичної інфраструктури, можуть призвести до кращих результатів, якщо вони будуть ретельно розроблені. Ефективна співпраця між урядом та постачальниками з метою розробки та впровадження політики повинна дозволити державним службам більш ефективно виконувати свої завдання (такі як моніторинг, раннє попередження, превентивні інвестиції або реагування на надзвичайні ситуації), але таким чином, щоб не ставити під загрозу інтереси приватного сектору, в тому числі конфіденційність.

Встановлення партнерських відносин між урядами та операторами (державними та приватними) для заохочення діалогу з цих питань є корисним підходом до спільного формування політики стійкості та безпеки критичної інфраструктури, а також її імплементації. У будь-якому випадку, такий діалог має забезпечити рішення для подолання наведених нижче викликів в управлінні безпекою та стійкістю критичної інфраструктури:

- *Встановлення довіри*: оператори критичної інфраструктури не завжди готові ділитися інформацією про вразливість до небезпек і загроз з урядом, а також з іншими операторами, які залежать від них, або *навпаки.*
- *Безпека обміну інформацією*: забезпечення конфіденційності інформації про вразливість, а також про інвестиції в стійкість з боку операторів інфраструктури є ключовим аспектом, особливо в конкурентних секторах.
- *Механізми розподілу витрат*: ще одним важливим аспектом з економічної точки зору є розуміння того, якою "ціною" можна досягти стійкості, і хто буде платити за інвестиції в стійкість.
- *Міжнародне співробітництво*: з огляду на транскордонний вимір систем критичної інфраструктури, механізми управління повинні включати міжнародний вимір.
- *Швидкі зміни та розвиток технологій*: зважаючи на швидкі темпи інновацій у багатьох секторах інфраструктури, посилення їхньої стійкості вимагає адаптованих рішень, оскільки класичні регуляторні норми можуть не встигати за нововведеннями.

Посилання

Барамі, Б. (2013), *Стійкість інфраструктури: Ризик-орієнтована система*, Міністерство транспорту США, https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20Risk-Based%20Framework.pdf (дата перегляду: 25 лютого 2019 р.). [36]

Чанг, С. та ін. (2014), "На шляху до міст, стійких до катастроф: Характеризуючи стійкість інфраструктурних систем за допомогою експертних оцінок", *Аналіз ризиків*, т. 34/3, с. 416-434, http://dx.doi.org/10.1111/risa.12133. [37]

Critical Five (2014), *Формування спільного розуміння наративу щодо критичної інфраструктури*, https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative- critical-infrastructure-2014-508.pdf (дата перегляду: 25 лютого 2019 р.). [34]

Флінн, С. (2008), "Америка стійка, кидає виклик тероризму і пом'якшує наслідки стихійних лих", *Foreign Affairs*, https://www.foreignaffairs.com/articles/2008-03-02/america-resilient (дата звернення: 25 лютого 2019 р.). [35]

G7 (2016), *Декларація лідерів G7 Ісе-Сіма*, https://www.mofa.go.jp/files/000160266.pdf (дата перегляду: 25 лютого 2019 року). [38]

Мотефф, Дж. (2012), *Звіт CRS щодо стійкості критичної інфраструктури Конгресу: Еволюція політики і програм та питання для Конгресу*, Дослідницька служба Конгресу, https://fas.org/sgp/crs/homesec/R42683.pdf (дата перегляду: 25 лютого 2019 р.). [42]

ОЕСР (2017), *Правильне управління інфраструктурою: Рамки для кращого управління*, OECD Publishing, Париж, https://dx.doi.org/10.1787/9789264272453-en. [11]

ОЕСР (2014), *Підвищення стійкості через інноваційне управління ризиками*, Огляди ОЕСР щодо політики управління ризиками, Публікація ОЕСР, Париж, https://dx.doi.org/10.1787/9789264209114- en. [20]

ОЕСР (2014), *Рекомендація Ради з управління критичними ризиками*, http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf (дата перегляду: 25 лютого 2019 року). [1]

ОЕСР (2011), *Майбутні глобальні інциденти: Покращення управління ризиками*, Огляди ОЕСРщодо політики управління ризиками, ОЕСР Publishing, Париж, https://dx.doi.org/10.1787/9789264114586- en. [9]

ОЕСР та EU JRC (2018), *Системне мислення для забезпечення стійкості та безпеки критичної інфраструктури - семінар ОЕСР/ JRC - ОЕСР*, http://www.oecd.org/gov/risk/workshop-oecd-jrc-system- thinking-for-critical-infrastructure-resilience-and-security.htm (дата звернення 25 лютого 2019 року). [41]

Управління ООН зі зниження ризиків катастроф (2015), *Сендайська рамкова програма зі зниження ризиків катастроф на 2015 - 2030 роки*, https://www.unisdr.org/files/43291_sendaiframeworkfordrren.pdf (дата перегляду: 25 лютого 2019 року). [39]

Рада Безпеки ООН (2017), *Резолюція Ради Безпеки 2341 - Загрози міжнародному миру та безпеці, спричинені терористичними актами*, http://unscr.com/en/resolutions/2341 (дата перегляду: 25 лютого 2019 року). [40]

3. Актуальний стан управління стійкістю критичної інфраструктури

У цьому розділі наведено огляд політики стійкості критичної інфраструктури в країнах ОЕСР. Базуючись на міжкраїновому опитуванні, у цьому розділі розглядаються різні підходи, використані країнами для визначення критичної інфраструктури, цільових секторів інфраструктури та оцінки їх критичності. У розділі також обговорюються різні форми партнерства між урядом та операторами та розглядаються політичні інструменти, які використовуються урядами для сприяння стійкості критичної інфраструктури.

Державна політика критичної інфраструктури в країнах ОЕСР

Стратегії та програми критичної інфраструктури

У середині 2000-х років почали з'являтися комплексні багатогалузеві державні політики для підтримки стійкості або захисту критичної інфраструктури. З 34 країн ОЕСР, які відповіли на опитування щодо управління критичними ризиками, 90% зазначили, що вони визнали певні сектори інфраструктури критичними (OECD, 2018).[2]). Багато країн ОЕСР визначили сектори критичної інфраструктури, створили інвентаризацію активів за допомогою процесу оцінки критичності та ризиків, а також створили національні програми для посилення їх стійкості до потрясінь. Такі програми, як правило, побудовані на механізмі управління, який дозволяє обмінюватися інформацією між урядом та операторами критичної інфраструктури та включає в себе комбінацію політичних інструментів, починаючи від регулювання та закінчуючи механізмами стимулювання для підтримки реалізації цілей стійкості критичної інфраструктури. Перелік цих національних стратегій або програм наведено в Додатку 1.

У цьому розділі звіту докладніше розповідається про те, як ці національні політики розробляються та впроваджуються з метою надання інформації про поточний стан у країнах ОЕСР. Відповіді країни на опитування ОЕСР щодо критичної інфраструктури, проведене в 2017-2018 роках, допомогли інформувати цей розділ (загальні результати представлені в Додатках 3.A-3.D). В опитуванні взяли участь 25 країн ОЕСР: Австрія, Бельгія, Канада, Чехія, Естонія, Фінляндія, Франція, Німеччина, Ірландія, Ізраїль, Корея, Латвія, Люксембург, Нідерланди, Нова Зеландія, Норвегія, Польща, Португалія, Словаччина Республіки, Іспанії, Швеції, Швейцарії, Туреччини, Великобританії та США.

Визначення критичної інфраструктури відрізняються в різних країнах

Визначення критичної інфраструктури є необхідним першим кроком у створенні політики безпеки та стійкості критичної інфраструктури. Як показано в Додатку 3.A, офіційні визначення критичної інфраструктури відрізняються в різних країнах. Деякі визначення відносяться до критичної інфраструктури як інфраструктури, функціонування якої є життєво важливим або необхідним для економічного та соціального добробуту, тоді як інші підкреслюють її важливість для функціонування держави або національної безпеки.

У половині з 28 визначень, зібраних під час опитування та кабінетного дослідження, критична інфраструктура описується як поєднання життєво важливих процесів для добробуту суспільства та безпеки держави. Інша половина залишається зосередженою лише на суспільному добробуті та безпеці.

Ще одне спостереження показує зростаючу стурбованість взаємозв'язком і взаємозалежністю критичної інфраструктури та необхідність прийняття системного підходу. Це можна знайти в багатьох визначеннях, які детально визначають критичну інфраструктуру як поєднання мереж, систем, засобів і технологій, які сприяють наданню основних послуг або підтримують життєво важливі функції. Інші визначення також включають інституційні чи організаційні структури, що підтримують надання послуг.

Хоча визначення різняться, можна погодитися, що загальне поняття критичної інфраструктури означає, що збій матиме серйозні наслідки для соціально-економічного добробуту та громадської безпеки, включаючи національну безпеку. Австралія, Канада, Нова Зеландія, Сполучене Королівство та Сполучені Штати розробили спільний наратив і визначення критичної інфраструктури, також відомої як національно значуща інфраструктура:

«системи, активи, засоби та мережі, які надають основні послуги та необхідні для національна безпека, економічна безпека, процвітання, а також здоров'я та безпека їхніх відповідних націй (Critical Five, 2014[34]).

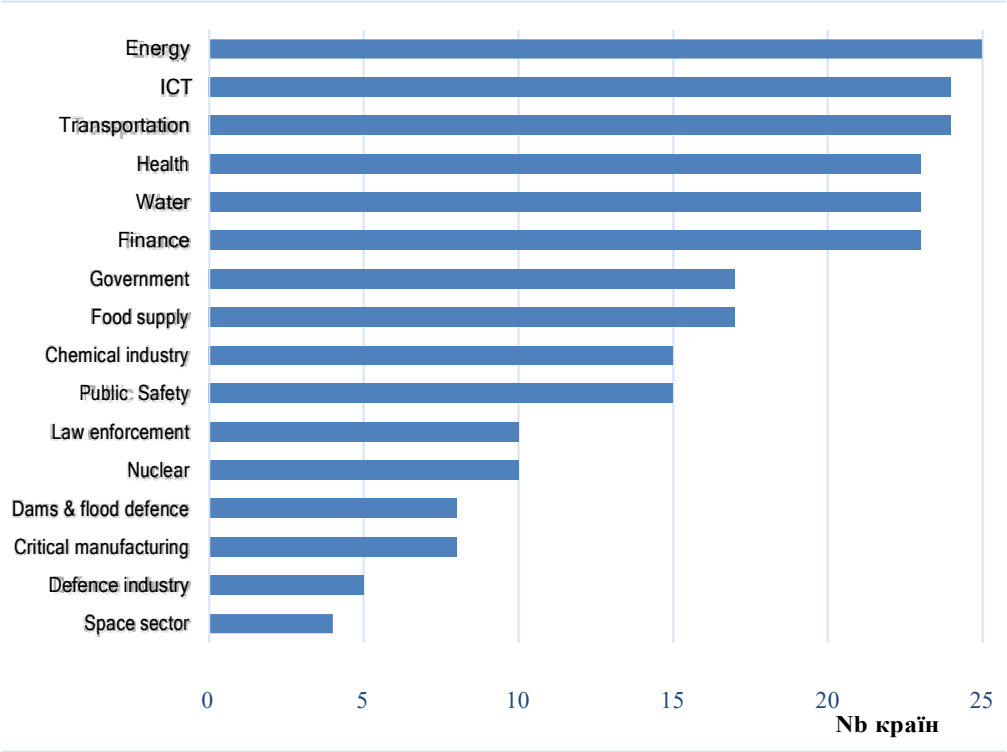
Важливим аспектом є те, що визначення критичної інфраструктури не повинно бути статичним, а оновлення та перегляд цього визначення може бути відповіддю на динамічний національний та міжнародний ландшафт ризиків. Наприклад, Швейцарія наразі переглядає та спрощує своє визначення до «Критичні інфраструктури — це процеси, системи та засоби, які мають важливе значення для функціонування економіки та добробуту населення відповідно». Це спрощення дозволить адаптувати масштаб програми критичної інфраструктури до мінливих умов легше, ніж раніше, коли визначення було більш директивним. Подібним чином у Сполученому Королівстві визначення еволюціонувало, щоб включити вплив на національну безпеку, національну оборону або функціонування держави серед критеріїв для визначення критичної національної інфраструктури.

Які сектори критичної інфраструктури?

Метою визначення критичної інфраструктури є націлювання на сектори, які мають найбільше значення для соціальної та економічної безпеки та стабільності. Окрім визначень, списки секторів також відрізняються в різних країнах. Порівняльна таблиця, у якій відображено сектори, які вважаються критично важливою інфраструктурою, дає змогу оглянути загальні тенденції та сектори, які є більш специфічними для країни. У таблиці в Додатку 3.C представлено порівняння між країнами щодо того, як країни відрізняються щодо категоризації секторів критичної інфраструктури, тоді як на рисунку 3.1 представлено синтез найбільш поширених типів секторів критичної інфраструктури в країнах ОЕСР за результатами опитування ОЕСР.

Деякі країни мають велику кількість секторів критичної інфраструктури, наприклад Сполучені Штати з 16 різними секторами (White House, 2013).[43]). Інші країни можуть обмежити свою політику критичної інфраструктури лише двома секторами, наприклад Португалія, лише з електроенергією та транспорт, який вважається сектором критичної інфраструктури відповідно до положень Директиви Європейської Ради від 2008 року щодо ідентифікації та позначення європейської критичної інфраструктури та оцінки необхідності покращення їх захисту (Європейська Рада, 2008[44]).

Малюнок 3.1. Сектори визначеної критичної інфраструктури в країнах ОЕСР



примітка: Відповіді отримані з 25 країн ОЕСР.
Джерело: Дослідження ОЕСР щодо стійкості та безпеки критичної інфраструктури (2018)

Загалом шість секторів широко класифікуються як критичні в країнах ОЕСР: інформаційні та комунікаційні технології, енергетика, фінанси, охорона здоров'я, транспорт і вода. Друга група секторів, включаючи уряд, постачання продуктів харчування, хімічну промисловість або громадську безпеку, згадується як критична принаймні в половині країн, які відповіли. Інші сектори здаються більш специфічними для країни. Сюди входять правоохоронні органи, ядерна оборона, греблі та продовольчий захист, критично важливе виробництво, оборонна промисловість у космічному секторі, які не вважаються критично важливими для функціонування суспільства для політики переважної більшості країн щодо критичної інфраструктури.

Подібно до загального визначення критичної інфраструктури, список критичних секторів може змінюватися з часом, щоб усунути нові вразливості та нові ризики. Деякі країни також вирішили визначити загальні сектори, а також підсектори критичної інфраструктури, що призводить до відмінностей у категоризації між країнами. Наприклад, Швейцарія не передбачає окремої категорії для ядерного сектору, як це було б у Сполучених Штатах, натомість це підкатегорія в секторі постачання та розподілу енергії. Хоча ці відмінності відображають національні переваги, може бути важливо краще узгодити підходи між країнами, особливо для сприяння транскордонному та міжнародному співробітництву з цього питання політики.

Виявлення критично важливих активів і оцінка їх вразливості

Наступним кроком у комплексній політиці критичної інфраструктури є визначення системного аналітичного підходу для визначення пріоритетів заходів стійкості критичної інфраструктури. Процес встановлення пріоритетів включає кілька етапів оцінки та може інформувати про цільове планування та інвестиційні рішення. По-перше, не всі інфраструктурні активи мають однаковий рівень критичності. Слід провести оцінку критичності, щоб визначити активи, системи та мережі, які є справді критичними (DHS, 2013).[45]); (Теохаріду та Джанопулос, 2015[46]).

Визначення критичних активів з оцінкою критичності

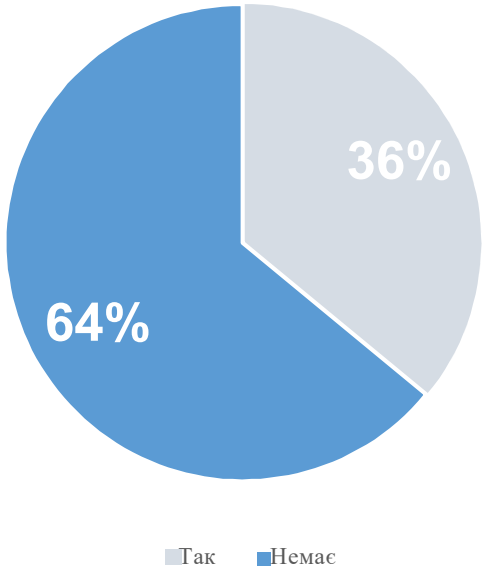
Аналіз критичності повинен включати оцінку наслідків порушення роботи критичної інфраструктури за низкою попередньо встановлених критеріїв. У країнах ОЕСР використовується кілька підходів. Наприклад, у Швейцарії вперше проведено диференціацію між різними секторами та підсекторами за трьома категоріями критичності (дуже висока критичність, висока критичність, нормальна критичність). У Нідерландах економічні, фізичні та соціальні критерії дають змогу визначити різні процеси критичної інфраструктури, але потім розрізняють категорію A, де збої можуть мати значні наслідки та каскадні наслідки, і категорію B, де вплив може бути меншим, щоб відобразити розмаїття критичної інфраструктури та встановлення пріоритетів. З точки зору критеріїв,[44]).

Важливим моментом оцінки критичності є включення оцінки взаємозалежності, щоб визначити критичні точки системи або між різними секторами, які є важливими для продовження роботи під час кризи, щоб уникнути каскадних збоїв. Залежності та взаємозалежності критичної інфраструктури можуть бути фізичними, коли стан один

Інфраструктура залежить від матеріального результату іншої, але також можуть бути цифрові, географічні або логічні залежності, які слід враховувати при такій оцінці (Rinaldi, Peerenboom and Kelly, 2001).[47]); (Маколей, 2009[48]). На цьому фоні важливо розробити моделі для оцінки втрат послуг, для чого необхідно визначити функціональні зв'язки між системами інфраструктури.

Хоча аналіз взаємозалежності є сферою, де дослідження досягають значного прогресу, методології ще не широко використовуються в країнах ОЕСР: лише 36% респондентів Опитування ОЕСР вказали, що вони виявили залежності (рис. 3.2). Аргонська національна лабораторія в Сполучених Штатах надає корисний огляд різних методів, які уряди та оператори можуть використовувати для такої оцінки взаємозалежності критичної інфраструктури (Petit et al., 2015).[49]).

Малюнок 3.2. Картографування взаємозалежностей критичної інфраструктури в країнах ОЕСР



Примітка: Відповідь на запитання «Чи ваш центральний уряд відобразив взаємозалежності між різними секторами критичної інфраструктури?» серед 25 респондентів опитування ОЕСР

Джерело: Дослідження ОЕСР щодо стійкості та безпеки критичної інфраструктури (2018)

Оцінка критичності зазвичай призводить до розробки інвентаризації критичних активів, реєстрів або карт з різними рівнями класифікації відповідно до їх критичності. Більшість країн, які розробили програми та стратегії критичної інфраструктури, створили такі інвентаризації. Наприклад, у Франції Генеральний секретаріат з питань оборони та національної безпеки точно визначає та визначає критичну інфраструктуру, а намагання зосередитися на найбільш критичних призвело до скорочення їх кількості з понад 7000 до приблизно 1500. Є також приклади транскордонного картографування критичної інфраструктури, наприклад, на рівні Європейського Союзу, в контексті Директиви ЄС 2008/114/ЕС щодо ідентифікації та позначення європейських критичних інфраструктур та оцінки потреби у покращенні їх захисту.

Проведення аналізу вразливостей для виявлення слабких місць

Після визначення та ієрархічної класифікації критичних активів оцінка вразливості дозволяє виявити слабкі місця, де ймовірно можуть статися потенційні збої. Ретельна оцінка вразливості критичної інфраструктури дає розуміння найважливіших ризиків, загроз, вразливостей і ступеня стійкості цієї інфраструктури. Для цього важливо провести стрес-тест на вразливість критичної інфраструктури до ряду сценаріїв ризику різної ймовірності, величини або їх комбінації в діапазоні потенційних небезпек і загроз. Ці оцінки розглядають найбільш імовірні сценарії, на додаток до тих, які є менш імовірними, але все ж можуть матеріалізуватися.

Цілісний підхід, що включає всі небезпеки, може допомогти виявити складні вразливі місця. Національна стратегія Канади щодо критичної інфраструктури так само наголошує на необхідності аналізу ризиків усіх небезпек, який враховує випадкові, навмисні та природні небезпеки ((Громадська безпека Канади, 2014 р.).[50])). Важливо також інтегрувати в аналіз вразливі місця систем управління критичною інфраструктурою, оскільки збої в управлінні під час криз є надто поширеними. Спільний дослідницький центр Європейської комісії, наприклад, розробив інструмент стрес-тестування, який зосереджується на цих складних аспектах управління із застосуванням у ядерному та банківському секторах. (Galbusera, Giannopoulos and Ward, 2014[51]).

Оцінку вразливості критичної інфраструктури можна виконувати за допомогою різних методологій. У вставці 3.1 наведено приклади таких методологій із ряду країн ОЕСР. Ці методології варіюються від детерміністських підходів до імовірнісних методів. Детерміновані підходи аналізують та інтерпретують історичні події катастроф і доступні ретроспективні дані у світлі нових подій. Сценарії катастроф і симуляції розширюють ретроспективний аналіз.

Оцінка ризику як основа для інвестицій у стійкість

Виявлення слабких місць дозволяє визначити пріоритети, де зосередити зусилля щодо стійкості в існуючих системах інфраструктури: на точках збою, які матимуть найсерйозніші наслідки. Така пріоритезація може інформувати про цільове планування та інвестиційні рішення, наприклад, яка інфраструктура повинна бути зміцнена або переміщена в першу чергу, або яка інфраструктура повинна отримати пріоритетне відновлення після катастрофи, щоб забезпечити швидке відновлення (Verner, Petit and Kihaek, 2017).[52]).

Оцінку ризику можна доповнити, щоб оцінити переваги інвестицій у стійкість або безпеку для зменшення ризиків як для існуючої інфраструктури, так і для нових проектів. Порівнюючи переваги різних заходів стійкості щодо зниження ризику збоїв, аналіз витрат і вигод з урахуванням ризиків може сприяти прийняттю рішень і інвестиційним рішенням щодо стійкості.

Вставка 3.1. Методології оцінки ризиків критичної інфраструктури в ОЕСР країни

Методологія оцінки ризиків і стійкості критичних інфраструктур і систем(CRISRRAM).

***CRISRRAM** – це методологія, розроблена Європейською Комісією. Він використовує всі небезпеки та системний підхід, розглядаючи ризики та вразливі місця критичної інфраструктури на рівні активів, системному рівні та рівні суспільства. Щоб подолати складність оцінки ризиків, CRISRRAM використовує підхід, заснований на сценаріях, і рекомендує оцінку всіх відповідних сценаріїв з однією та кількома небезпеками. Щоб вибрати відповідні сценарії, слід виконати оцінку ймовірності загрози.*

RAMCAP-Plus

Методологія RAMCAP-Plus була розроблена Американським товариством інженерів-будівельників як підхід до оцінки всіх ризиків і стійкості. Він охоплює всі інфраструктури, що враховують подвійні цілі захисту та стійкості. Сім кроків методології: характеристика активів; характеристика загрози; аналіз наслідків; аналіз вразливості; оцінка загрози; оцінка ризику та стійкості; управління ризиками та стійкістю. Інструмент розроблено для використання як операторами критичної інфраструктури, так і особами, які приймають рішення.

Регіональна програма оцінки стійкості DHS (RRAP)

Програма регіональної оцінки стійкості (RRAP) — це спільна оцінка конкретної критичної інфраструктури в межах визначеної географічної області та регіонального аналізу навколишньої інфраструктури для вирішення низки проблем стійкості інфраструктури, які можуть мати значні наслідки на регіональному та національному рівні. Ці добровільні нерегулятивні проекти RRAP здійснюються під керівництвом Міністерства внутрішньої безпеки США та щороку відбираються Департаментом за допомогою та під керівництвом федеральних, штатних і місцевих партнерів. Цей підхід відтворюється в Канаді.

***Джерело*: (Джаннопулос, Філіппіні та Шіммер, 2012[53]); (Теохаріду таДжанопулос, 2015[46])**

Обмін інформацією про ризики та вразливі місця

Більшість країн ОЕСР створили платформи для обміну інформацією

Механізми управління для посилення критичної стійкості підкреслюють необхідність партнерства та платформ для сприяння обміну інформацією та знаннями. Зобов’язання урядів та операторів брати участь у діалозі щодо цих питань через інституціоналізовані регулярні зустрічі виявилося корисним для побудови взаємної довіри на основі спільних інтересів, а також для стимулювання регулярного обміну інформацією, спільних навчань, обізнаності про ситуацію, координації дій, взаємних допомога, обмінзобладнання та аварійні запаси.

Кілька країн розробили програми та підходи довихованецьзасновані на довірі зв'язки між урядом і приватними власниками та операторами. Технічні рішення, такі як обмін інформацією та веб-портали для співпраці, можуть служити безпечним середовищем, де зацікавлені сторони приватного та державного секторів можуть легко та регулярно обмінюватися даними, інформацією та передовими практиками, що стосуються стійкості критичної інфраструктури (Bach et al., 2013).[25]); (Льюїс, 2006[54])).

Опитування OECD показує, що 80% респондентів створили такі механізми або платформи обміну інформацією, найчастіше на добровільній основі. Вставка 3.2 надає приклади успішного залучення зацікавлених сторін у критичній інфраструктурі та безпечних підходів до обміну інформацією.

Проблеми для ефективного обміну інформацією

Хоча обмін інформацією дає багато переваг для кращого розуміння та обміну досвідом для підвищення стійкості критичної інфраструктури, залишається кілька поширених проблем.

Забезпечення безпеки інформації, якою обмінюються власники та оператори критичної інфраструктури, є важливим компонентом для побудови взаємної довіри, оскільки частина цієї інформації може бути важливою для конкурентоспроможності на ринку або їх іміджу. Оскільки оператори не завжди можуть ділитися конфіденційною інформацією про свої вразливості та/або критичні залежності за межами безпечних кіл, забезпечення взаємної довіри та безпеки спільної інформації є важливим аспектом для сприяння діалогу та обміну.

Не менш важливо зосередитися на якості, а не на кількості інформації, яка передається через ці механізми. Чим чіткішою та точнішою є інформація, яка надається, тим більшу додану цінність вона може запропонувати для підвищення стійкості критичної інфраструктури. Усі сторони в уряді та приватному секторі повинні побачити переваги цієї практики обміну інформацією зі своїх відповідних сторін. Фільтрування великої кількості інформації є менш ефективним, ніж обмін найважливішими елементами безпеки критичної інфраструктури.

Якісна інформація може створити стимули для підвищення стійкості.

Оператори можуть не захотіти брати участь у такому партнерстві, якщо вони побоюються, що це призведе до додаткових витрат, які їм доведеться фінансувати, коли стане відомо про їхні вразливі місця. Подібним чином, ризик того, що конкуренти не будуть залучені до процесу та користуватимуться підвищеним рівнем стійкості, який це призведе, може спричинити труднощі для залучення операторів. Мінімальні стандарти безпеки можуть допомогти гарантувати відсутність «найслабших ланок», які можуть поставити під загрозу загальну безпеку системи, а також подолати недостатні інвестиції в стійкість і відсутність бажання брати участь.

Вставка 3.2. Залучення зацікавлених сторін у критичній інфраструктурі та обмін інформацією

Прагнучи сприяти ефективним і результативним відносинам між групами зацікавлених сторін із спільною відповідальністю за стійкість критичної інфраструктури, кілька країн розробили програми та підходи для розвитку довірчих зв'язків між урядом і приватними власниками та операторами.

• ***Австралійська довірена мережа обміну інформацією (TISN) для стійкості критичної інфраструктури***

TISN *забезпечує безпечне, неконкурентне середовище, в якому всі зацікавлені сторони критичної інфраструктури можуть співпрацювати та брати участь в ініціативах з підвищення стійкості. Мережа дозволяє власникам і операторам різних секторних груп регулярно обмінюватися інформацією та співпрацювати всередині та між секторами для вирішення проблем безпеки та безперервності бізнесу.*

• ***Канадський шлюз критичної інфраструктури***

Шлюз відповідає одній із цілей канадської національної стратегії та плану дій щодо критичної інфраструктури – це своєчасне просування обміну інформацією та захисту між партнерами з критичної інфраструктури. Це некласифікований веб-простір для спільної роботи, який включає членів спільноти критичної інфраструктури.

• ***Інформаційна мережа попереджень про критичну інфраструктуру Європейського Союзу (CIWIN)***

CIWIN *— це система обміну інформацією, розроблена як допоміжний компонент Європейської програми захисту критичної інфраструктури. CIWIN сприяє обміну інформацією про спільні загрози, уразливості та відповідні заходи та стратегії для зменшення ризику для критичної інфраструктури між членами Європейського Союзу та Європейською Комісією. На додаток до функції обміну інформацією, CIWIN служить системою швидкого оповіщення для раннього попередження про гострі ризики та загрози.*

• ***Центри обміну та аналізу інформації США (ISAC)***

Спеціальні секторальні ***ISAC*** *можуть бути розширенням уряду на національному рівні, як у випадку з телекомунікаційним ISAC США, яким керує Національна система зв'язку в рамках Міністерства внутрішньої безпеки США, або повністю управлятися галуззю, як США. Water ISAC, некомерційне розширення професійного товариства водного сектора. ISAC розглядаються як джерело найкращих практик, пов'язаних із безпекою, а також індикацій небезпеки та загроз, попереджень та оцінок.*

• ***Програма консультанта з безпеки Міністерства внутрішньої безпеки США (PSA).***

Програма передбачає активну взаємодію між державними партнерами та власниками та операторами приватного сектору, відповідальними за критичну інфраструктуру. PSA планує, координує та проводить дослідження безпеки та стійкості та оцінки критичної інфраструктури національного значення. Програма також проводить інформаційну діяльність і надає власникам, операторам та іншим зацікавленим сторонам доступ до ресурсів безпеки та стійкості критичної інфраструктури, навчання та інформації. Під час і після інциденту консультанти служать зв'язком між державними службовцями та власниками та операторами критичної інфраструктури в приватному секторі.

Джерела:Уряд Австралії, надійна мережа обміну інформацією,http://www.tisn.gov.au ; Канадський інформаційний шлюз критичної інфраструктури,https://cigateways.ps.gc.ca ; ЄС критично Інформаційна мережа попередження про інфраструктуру,http://ec.europa.eu/dgs/home-affairs/what-wedo/networks/critical_infrastructure_warning_information_network/index_en.htm;

НАСДепартамент внутрішньої безпеки, Партнерство для забезпечення безпеки та стійкості критичної інфраструктури, https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-andresilience ; DHS США, радники з питань безпеки,https://www.dhs.gov/protective-security-advisors

Пріоритезація заходів стійкості та інструментів політики

Існує велика різноманітність інструментів політики для сприяння інвестиціям операторів у стійкість

Підвищення стійкості до критичної інфраструктури є спільними зусиллями кількох зацікавлених сторін, які потребують поєднання інструментів для збору інформації, визначення пріоритетів для інвестицій у стійкість і збільшення загальних стимулів.

Уряди можуть вибирати з різноманітних політичних інструментів і механізмів для посилення стійкості критичної інфраструктури. Інструменти варіюються від директивних регуляторних інструментів, механізмів компенсації до добровільних рамок, заснованих на партнерстві між урядом та операторами. Двадцять два інструменти політики були визначені в Огляді ОЕСР щодо стійкості критичної інфраструктури (табл. 3.1). Ці інструменти політики докладніше описані в Додатку 3.D. Цей вичерпний перелік має на меті представити різні варіанти політики, які уряд може використовувати після створення програми стійкості критичної інфраструктури, визначення її найбільш критичної інфраструктури та її вразливості та встановлення механізму обміну інформацією з операторами критичної інфраструктури.

Таблиця 3.1. Інструменти політики для підвищення стійкості критичної інфраструктури

1. Надання інформації про небезпеки та загрози
2. Добровільні механізми або платформи обміну інформацією
3. Обов’язкові механізми або платформи обміну інформацією
4. Заходи з підвищення обізнаності та тренінги
5. Рекомендації щодо стійкості для операторів критичної інфраструктури
6. Сприяння розвитку/використанню професійних стандартів
7. Механізм стимулювання для оцінки ризиків і вразливостей
8. Механізми стимулювання інвестування в стійкість
9. Галузеві нормативні акти, присвячені ЗІВ
10. Правила забезпечення безперервності діяльності, що базуються на ефективності
11. Обов'язкові плани забезпечення безперервності діяльності
12. Перевірки та оцінка ефективності
13. Штрафи за недотримання вимог стійкості
14. Інші види стягнень за невиконання
15. Ранжування за результатами перевірки/виконання
16. Звіт про стійкість операторів
17. Обмін передовим досвідом
18. Державні інвестиції в стійкість інфраструктури
19. Рекомендації для субнаціональних рівнів управління
20. Обов'язкове страхування критичної інфраструктури
21. Рецензування, моніторинг та оцінка
22. Галузеві угоди про взаємодопомогу

Примітка: *Цей список інструментів політики був підготовлений Секретаріатом ОЕСР на основі підходів, представлених на Форумі високого рівня ризиків ОЕСР, і кабінетних досліджень*
Джерело: Секретаріат ОЕСР

Визначення плюсів і мінусів цих різних інструментів у різних політичних контекстах може стати великою підтримкою для розробки політики захисту критичної інфраструктури та стійкості. Форум високого рівня ризиків OECP шляхом свого опитування та тематичних досліджень ініціював аналіз цих інструментів політики. Наступні міркування можуть сприяти вибору, який уряди можуть зробити серед цих різних варіантів.

Регулювання є важливим методом, який забезпечує обов'язкові вимоги та механізми забезпечення стійкості критичної інфраструктури. Регуляторний підхід має сильні сторони в тому, що він передбачає обов'язкові вимоги, але він також може виявитися дорогим і створити часові затримки між технологічними розробками в багатьох секторах, які потребують регулярного оновлення.

Можуть бути застосовані різні нормативні підходи: від директивних галузевих нормативних актів до тих, що базуються на ефективності, що дозволяє операторам самим визначати шляхи досягнення цілей стійкості.

Фінансові стимули забезпечують ще один спосіб збільшення інвестицій і планів безперервності для захисту критичної інфраструктури та стійкості. Розробка механізмів компенсації для клієнтів у разі збою в обслуговуванні або інших типів штрафів може бути використана для інтерналізації переваг стійкості. Це надає операторам вибір шляхів підвищення їх стійкості. У Фінляндії Закон про енергетичний ринок 2013 року передбачає таку структуру стимулів для операторів розподілу електроенергії, щоб вони інвестували в стійкість своєї мережі, з поєднанням цінових стимулів для покращення стійкості з важливими комісіями у випадку, якщо цільові показники стійкості не досягнуті (розділ 4).

Державне фінансування, яке використовується для стійкості критичної інфраструктури, може встановити стандарти та продемонструвати цінність початкових інвестицій у стійкість. Інтеграція стійкості до великих державних інвестиційних проектів є прикладом цінності та переваг цих інвестицій і може створити стимули для інших власників і операторів критичної інфраструктури наслідувати їхній приклад (OECD, 2018).[12]). У державних закупівлях дедалі більше враховується стійкість до зміни клімату, що може слугувати підходом до поширення інших ризиків. Наприклад, інвестиції в громадський транспорт у розмірі 30 мільярдів євро у Великий Париж були розроблені з урахуванням особливих вимог щодо стійкості до повеней, що виходять за рамки існуючих норм (OECP, 2014 р.).[7]).

Тиск з боку колег — це ще один варіант політики, який працює серед власників і операторів критичної інфраструктури, ґрунтуючись на підтримці їхнього іміджу та рейтингу перед громадськістю. Створення публічного доступу до оцінок критичної інфраструктури створює занепокоєння для компаній та їх іміджу. Рейтинги є важливими показниками стійкості та механізмом створення стимулів. Корея включила механізм тиску з боку колег у свою систему для управління несправністю інфраструктури. Щороку періодична загальнонаціональна діагностика безпеки проводить вибіркову діагностику для 21 типу інфраструктури. Ці оцінки оприлюднюються та забезпечують рейтинг інфраструктури, створюючи важливі стимули для компаній підтримувати свій суспільний імідж. Інший приклад можна знайти в Національному агентстві з надзвичайних ситуацій (NESA) у Фінляндії. Річні оцінки планів забезпечення безперервності діяльності операторів в енергетичному секторі представлені групі операторів, щоб вони могли порівнювати свою ефективність і вчитися один у одного (Див. розділ 4). Хоча в цьому випадку результати не оприлюднюються, тиск з боку колег у секторі створює стимули для покращення продуктивності.

Дедалі більше публічне оприлюднення кліматичних ризиків також може надати елементи роздумів щодо стійкості критичної інфраструктури до численних небезпек (OECD, 2018).[12])

Пошук правильного поєднання між обов'язковими та добровільними рамками

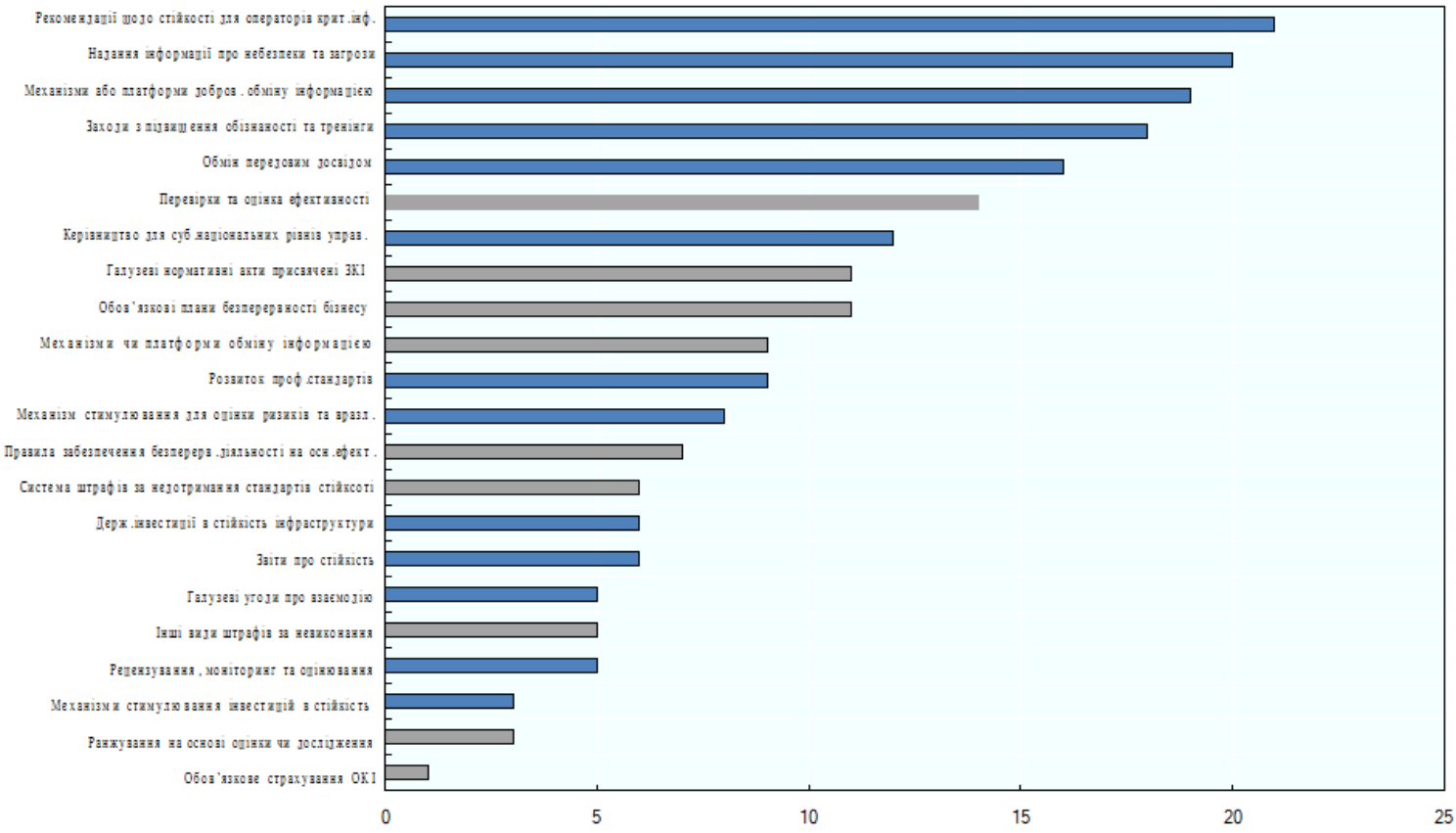
Урядам важливо знайти правильну комбінацію між обов'язковими та добровільними рамками, щоб посилити залучення зацікавлених сторін до стійкості. Як показано на рисунку 3.3, результати опитування ОЕСР вказують на перевагу добровільним структурам для посилення стійкості критичної інфраструктури.

Такі інструменти, як інструкції для субнаціональних рівнів уряду, інформаційно-просвітницькі заходи та тренінги, надання інформації про небезпеки та загрози, інструкції щодо стійкості для операторів критичної інфраструктури та механізм добровільного обміну інформацією є інструменти політики, які найчастіше використовуються урядами ОЕСР. Навпаки, більш суворі інструменти, такі як інспекції та оцінка ефективності, галузеві приписи або обов'язкові плани безперервності бізнесу, менше використовуються країнами ОЕСР для сприяння стійкості критичної інфраструктури.

Така перевага добровільним структурам демонструє, що в цілому політика стійкості критичної інфраструктури все ще знаходиться на ранньому етапі розвитку в багатьох країнах ОЕСР. У цьому контексті участь операторів у широких партнерських відносинах із багатьма зацікавленими сторонами та урядами залишається ключовим пріоритетом, що дозволяє зміцнювати довіру між громадськістю та приватним сектором. Прийняття добровільних рамок видається більш ефективним для досягнення цієї мети.

Тим не менш, цей підхід не обов'язково гарантує достатньо сильну структуру стимулів для забезпечення того, щоб достатні інвестиції були ефективно здійснені для досягнення очікуваних цілей стійкості. З роками, коли цінність цих партнерств буде широко визнана, можна очікувати, що обов'язкові підходи будуть легше прийняті та більш широко розроблені, щоб гарантувати, що оператори забезпечать певні форми мінімальних загальних стандартів стійкості. Набір політичних інструментів ОЕСР щодо управління стійкістю критичної інфраструктури, запропонований у Розділі 5, пропонує шлях вперед для урядів, які прагнуть поступово зміцнити стійкість критичної інфраструктури у своїх країнах за допомогою поетапного підходу, заснованого на партнерстві.

Малюнок 3.3. Інструменти політики для стійкості критичної інфраструктури в країнах ОЕСР



Примітка: 22 країни ОЕСР відповіли на опитування станом на 10 вересня 2018 року – обов'язкові інструменти позначено сірим кольором, добровільні – синім.

Джерело: Дослідження ОЕСР щодо стійкості критичної інфраструктури (2018)

Угоди про розподіл витрат для стійких інвестицій

Оператори дуже зацікавлені в збереженні безперервності своїх послуг і своєї репутації шляхом інвестування в стійкість. Однак інвестиції в стійкість часто передбачають авансові витрати, навіть якщо вони повинні бути компенсовані з точки зору більшої надійності обслуговування та стійкості до потрясінь.

Питання в тому, як знайти правильний баланс. Надмірні вимоги, встановлені урядами для посилення стійкості, можуть призвести до додаткових витрат на обслуговування клієнтів, громадян і підприємств. Вибираючи інструменти політики, які найкраще підходять для підвищення стійкості критичної інфраструктури в їх національному контексті, уряди повинні оцінити, як ці різні варіанти можуть забезпечити ефективні стимули для операторів інвестувати в стійкість, одночасно керуючи наслідками для вартості послуг. Розв'язання цього економічного рівняння є наріжним каменем для ефективної політики, але простого рішення немає. Як показано в прикладі Фінляндії в Розділі 4, участь у надійних партнерствах і регулярний діалог між урядами, регуляторними органами та операторами повинні дозволити обговорити механізми розподілу витрат для досягнення цілей стійкості.

Список літератури:

Bach, C. та ін. (2013), «Додавання цінності дослідженням критичної інфраструктури та ризику катастроф управління: концепція стійкості»,*http://journals.openedition.org/sapiens*6.1, *https://journals.openedition.org/sapiens/1626* (дата доступу: 25 лютого 2019 р.).

Барамі, Б. (2013),*Відмовостійкість інфраструктури: структура на основі ризиків*, Департамент США Транспорт, *https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20 Risk- Based%20Framework.pdf* (дата доступу: 25 лютого 2019 р.).

Chang, S. та ін. (2014), «До міст, стійких до стихійних лих: характеристика стійкості Інфраструктурні системи з експертними оцінками»,*Аналіз ризиків*, Вип. 34/3, стор. 416-434,*http://dx.doi.org/10.1111/risa.12133* .

Критична п'ятірка (2014),*Формування спільного розуміння для спільної критичної інфраструктуриРозповідь*,*https://www.dhs.gov/sites/default/files/publications/critical-five-shared- narrativecritical-infrastructure-2014-508.pdf* (дата доступу: 25 лютого 2019 р.).

DHS (2013),*NIPP 2013: Партнерство для безпеки та стійкості критичної інфраструктури |Вітчизняна безпека*, *https://www.dhs.gov/publication/nipp-2013-partnering-criticalinfrastructure-security-and-resilience* (дата доступу: 25 лютого 2019 р.).

Європейська рада (2008),*ДИРЕКТИВА РАДИ 2008/114/ЄС від 8 грудня 2008 року про ідентифікація та позначення європейських критичних інфраструктур та оцінка необхідностіпокращення їх захисту*,*https://eurlex.europa.eu/LexUriServ/LexUriServ.do?_uri=OJ:L:2008:345:0075:0082:EN:PDF* (дата доступу: 26 лютого 2019 р.).

Флінн, С. (2015),*Підвищення стійкості критичної інфраструктури після супербурі Сенді: урокидля Нью-Йорка та нації*Північно-східний університет, Бостон, Массачусетс, *http://dx.doi.org/10.17760/D20241717* Флінн, С. (2008), «Стійка Америка, яка кидає виклик тероризму та пом'якшує стихійні лиха»,*Зовнішня політика*, *https://www.foreignaffairs.com/articles/2008-03-02/america-resilient* (дата доступу: 25 лютого 2019 р.).

Galbusera, L., G. Giannopoulos and D. Ward (2014),*Розробка стрес-тестів для покращеннястійкість критичної інфраструктури: аналіз здійсненності*, Спільний дослідницький центр Європейської Комісії,*http://dx.doi.org/10.2788/954065* .

Giannopoulos, G., R. Filippini і M. Schimmer (2012),*Методології оцінки ризиків дляЗахист критичної інфраструктури. Частина I: Сучасний стан*, Спільний дослідницький центр Європейської Комісії,*http://dx.doi.org/10.2788/22260* .

Льюїс, Т. (2006),*Захист критичної інфраструктури у внутрішній безпеці: захист мережінація*, Wiley-Interscience.

Маколей, Т. (2009),Критична інфраструктура: розуміння її складових частин, вразливості,операційні ризики та взаємозалежності, CRC Press, *https://www.crcpress.com/Critical-Infrastructure-Understanding-Its-Component-Parts- Vulnerabilities/Macaulay/p/book/9781420068351* (дата доступу: 26 лютого 2019 р.)

Мотефф, Дж. (2012),*Звіт CRS для Конгресу Стійкість критичної інфраструктури: еволюціяПолітика, програми та питання для Конгресу*, Дослідницька служба Конгресу, *https://fas.org/sgp/crs/homesec/R42683.pdf* (дата доступу: 25 лютого 2019 р.).

ОЕСР (2018),*Оцінка глобального прогресу в управлінні критичними ризиками*, Огляди ОЕСРполітики управління ризиками, OECD Publishing, Париж, *https://dx.doi.org/10.1787/9789264309272-en* .

OECD (2018), «Стійка до клімату інфраструктура», *Політичний документ ОЕСР з навколишнього середовища*, № 14, ОЕСР, Париж, *http://www.oecd.org/environment/cc/policy-perspectives-climate-resilientinfrastructure.pdf* (дата доступу: 25 лютого 2019 р.).

ОЕСР (2014),*Басейн Сени, Іль-де-Франс, 2014: стійкість до великих повеней*, OECD Reviews of Політика управління ризиками, OECD Publishing, Париж, *https://dx.doi.org/10.1787/9789264208728-en* .

ОЕСР (2011),*Майбутні глобальні шоки: покращення управління ризиками*, OECD Reviews of Risk

Політика управління, видавництво ОЕСР, Париж,*https://dx.doi.org/10.1787/9789264114586- en* .

ОЕСР та ЄС JRC (2018),*Системне мислення для стійкості та безпеки критичної інфраструктури - Семінар OECD/ JRC - OECD*,*http://www.oecd.org/gov/risk/workshop-oecd-jrc-systemthinking- for-critical-infrastructure-resilience-and-security.htm* (дата доступу: 25 лютого 2019 р.).Petit, F. та ін. (2015), *Аналіз залежностей і взаємозалежностей критичної інфраструктури*, Аргонська національна лабораторія, *https://publications.anl.gov/anlpubs/2015/06/111906.pdf* (датадоступу: 26 лютого 2019 р.).

Громадська безпека Канади (2014), План дій щодо критичної інфраструктури на 2014-2017 рр, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl- nfrstrctr-2014-17-eng.pdf (дата доступу: 26 лютог 2019 р.).

Rinaldi, S., J. Peerenboom і T. Kelly (2001), *Ідентифікація, розуміння та аналіз Взаємозалежності критичної інфраструктури*, *https://pdfs.semanticscholar.org/b1b7/ d1e0bb39badc3592373427840a4039d9717d.pdf* (дата доступу: 26 лютого 2019 р.).

Theocharidou, M. and G. Giannopoulos (2015), «Методології оцінки ризиків для критичнихзахист інфраструктури. Частина II: Новий підхід», *http://dx.doi.org/10.2788/621843* .

Вернер, Д., Ф. Петі та К. Кіхаек (2017), «Включення пріоритезації в критичну інфраструктуру Програми безпеки та стійкості - HOMELAND SECURITY AFFAIRS",*Справи внутрішньої безпеки*,Вип. 13, *https://www.hsaj.org/articles/14091* (дата доступу: 26 лютого 2019 р.).

Білий дім (2013), *Президентська політична директива – Безпека критичної інфраструктури та Стійкість | whitehouse.gov*, *https://obamawhitehouse.archives.gov/the-pressoffice/ 2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil* (дата доступу: 25 лютого 2019 р.).

Додаток 3.А. Стратегія або програма критичної інфраструктури та керівник відповідальна установа

Країна	Так/ Ні*	Стратегія або програма критичної інфраструктури	Керівник чи відповідальна установа
Австралія	Так	Стратегія стійкості критичної інфрваструктури(2015) https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF	Департамент Ген.прокурора / Центр Критичної Інфраструктури
Австрія	Так	Австрійська програма захисту критичної інфраструктури – Мастерплан 2014 http://archiv.bundeskanzleramt.at/DocView.axd?CobId=58907	Федеральна канцелярія Федеральне міністерство внутрішніх справ
Бельгія	Так	Стратегія захисту критичної інфраструктури Бельгії https://crisiscentrum.be/nl/inhoud/kritieke-infrastructuur-0	Федеральна державна служба внутрішніх справ, Національний кризовий центр (дирекція CIPRA)
Канада	Так	Національна стратегія щодо критичної інфраструктури www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx	Публічна Безпека Канади
Чілі	Ні		
Чехія	Так	Національна програма захисту критичної інфраструктури (2010), Комплексна стратегія Чехії щодо критичної інфраструктури (2010)	МВС Чехії
Данія	Ні		
Естонія	Так	План розвитку внутрішньої безпеки 2015 – 2020 https://valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf	МВС
Фінляндія	Так	Постанова уряду про безпеку надання послуг (2013) https://www.nesa.fi/security-of-supply/objectives/	Національне агенство з надзвичайних ситуацій http://www.nesa.fi/
Франція	Так	Загальна міжвідомча інструкція з безпеки провадження життєво важливої діяльності http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf Закон про захист критичної інфраструктури (defence code – articles L. 1332-1 to L. 1332-7, R. 1332-1 to R. 1332-42	Генеральний секретаріат оборони та національної безпеки (SGDSN) www.sgdsn.fr
Німеччина	Так	Національна стратегія з захисту критичної інфраструктури (2009) https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1	Федеральне МВС
Греція	Так		
Венгрія	Ні		
Ісландія	Так		
Ірландія	Так		
Ізраіль	Так		Національне управління з питань надзвичайних ситуацій при Міністерстві оборони
Італія	Ні		
Японія	Ні		
Півд. Корея	Так	План захисту національної інфраструктури https://opengov.seoul.go.kr/sanction/10812531	Міністерство внутрішніх справ та безпеки (MOIS)
Латвія	Ні	Процедури ідентифікації критичної інфраструктури Кабінету Міністрів Латвії No. 496, adopted on 1 June 2010 http://likumi.lv/doc.php?id=212031 ; Процедура імплементації та застосування безпекових заходів для критичної інфраструктури Постанова No. 100 (2017) http://likumi.lv/doc.php?id=225776 Постанова про плани цивільного захисту Кабінету Міністрів No. 658, доповнено 7 Листопада 2017 https://likumi.lv/ta/id/294938-noteikumi-par-civilas-aizsardzibas-planu-strukturu-un-tajos-ieklaujamo-informaciju	Міжвідомча комісія з національної безпеки Секретаріат МВС

Люксембург	Так	Постанова Великого князівства від 21 лютого 2018 року, яка встановлює ідентифікацію та позначення критичної інфраструктури http://data.legilux.public.lu/eli/etat/leg/rgd/2018/02/21/a152/jo Постанова Великого князівства від 21 лютого 2018 року, що визначає структуру планів безпеки та безперервності діяльності критичної інфраструктури http://data.legilux.public.lu/eli/etat/leg/rgd/2018/02/21/a151/jo	Верховна комісія з національного захисту https://hcpn.gouvernement.lu/en/service/attributions.html
Мексика	Ні		
Голандія	Так	Захист Критичної Інфраструктури, Січень 2018 https://english.nctv.nl/binaries/Factsheet%20Vitaal%20ENG%202016%20(web)_tcm32-240750.pdf	Національний координатор з безпеки та контртероризму (NCTV)https://english.nctv.nl/
Нова Зеландія	Так	Зобов'язання постачальників інфраструктури вимагаються Законом про управління в надзвичайних ситуаціях цивільної оборони 2002 року та вторинним законодавством, включаючи наказ про Національний план управління на випадок надзвичайних ситуацій цивільної оборони 2015 року та Керівництво, зокрема «Lifeline Utilities and CDEM – Керівництво для директорів Lifeline Utilities and Civil Defence Management Groups» [DGL 16/14]. Тридцятирічний план розвитку інфраструктури Нової Зеландії на 2015 рік визначає довгострокове бачення центрального уряду, щоб інфраструктура була стійкою, скоординованою та сприяла міцній економіці та високим стандартам життя.	Міністерство з питань цивільної оборони та з питань надзвичайних ситуацій (MCDEM)
Норвегія	Так	Життєвоважливі функції для суспільства https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf	Directorate for Civil Protection (DSB) https://www.dsb.no/menyartikler/english/
Польща	Так	Національна програма з захисту критичної інфраструктури http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf	Урядовий центр охорони (RCB)
Португалія	Ні	Немає конкретної національної програми чи стратегії, але є національне положення про ЗКІ (Закон-декрет 62/2011 від 9 травня) http://www.prociv.pt/bk/RISCOSPREV/INFRAESTRUTURASCRITICAS/Documents/DL_62_2011_identificacao_e_protecao_de_infraestruturas_essenciais.pdf	Національне управління цивільного захисту (ANPC) Система внутрішньої безпеки (SSI)
Словакія	Ні	Акт про критичну інфраструктуру No 45/2011	MBC
Словенія	Ні		
Іспанія	Так	Закон 8/2011 від 28 квітня «Встановлення заходів для захисту критичної інфраструктури» та Королівський указ 704/2011 від 20 травня http://www.cnpic.es/ Національний план захисту критичної інфраструктури (оновлений у лютому 2016 р. – секретна інформація) Іспанська система планування захисту критичної інфраструктури (секретно) http://www.cnpic.es/en/Preguntas_Frecuentes/que_es_el_sistema_de_planificacion_PIC/index.html	Національний центр захисту критичної інфраструктури та кібербезпеки (CNPIC)
Швеція	Так	План заходів з захисту життєво-важливих функцій та послуг та критичної інфраструктури https://www.msb.se/RibData/Filer/pdf/27412.pdf	Swedish Civil Contingencies Agency (MSB)
Швейцарія	Так	Нова стратегія ЗКІ зі змінами від Федеральних Зборів від 8 грудня, 2017 www.infraprotection.ch	Фелеральний офіс з цивільного захисту (FOCP)
Туреччина	Так	2014-2023 Дорожня карта протидії техногенних надзвичайних ситуацій 2018-2022 AFAD Стратегічний план	Президентство з ліквідації наслідків стихійних лих і надзвичайних ситуацій
Великобританія	Так	2015 Стратегія національної безпеки та Стратегічний огляд оборони та безпеки http://www.cpni.gov.uk/about/cni/	Центр з захисту критичної інфраструктури (CPNI) Національний центр кібербезпеки (NCSC)
США	Так	NIPP 2013: Партнерство для забезпечення безпеки та стійкості критичної інфраструктури та плани для окремих секторів на 2015 рік https://www.dhs.gov/2015-sector-specific-plans	Департамент внутрішньої безпеки (DHS)

* : Так або Ні відповідь на запитання «Чи прийняв ваш національний уряд стратегію абопрограму критичної інфраструктури?»

Додаток 3.В. Визначення критичної інфраструктури в країнах ОЕСР

Країна	Офіційне визначення критичної інфраструктури
Австралія	Ті фізичні об'єкти, ланцюги поставок, інформаційні технології та комунікаційні мережі, які, якщо їх знищити, погіршити або зробити недоступними протягом тривалого періоду, можуть суттєво вплинути на соціальний чи економічний добробут нації або вплинуть на здатність Австралії проводити національну оборону та забезпечувати національну безпеку Джерело: Стратегія стійкості критичної інфраструктури (2010) і Стратегія стійкості критичної інфраструктури: план (2015)
Австрія	Критичні інфраструктури – це ті інфраструктури (системи, об'єкти, процеси, мережі або їх частини), які є важливими для підтримки важливих соціальних функцій і чиє порушення або знищення серйозно впливає на здоров'я, безпеку чи економічний і соціальний добробут великих частин чи ефективне функціонування державних установ Джерело:http://archiv.bundeskanzleramt.at/DocView.axd?CobId=58907
Бельгія	У бельгійському законодавстві критична інфраструктура визначається як «актив, система або її частина федерального значення, яка має важливе значення для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, безпеки, економічного чи соціального добробуту людей, а також порушення або знищення яких мало б значний вплив внаслідок нездатності підтримувати ці функції» Джерело:https://crisiscentrum.be/sites/default/files/loi_du_1er_juillet_2011_sur_les_ic.pdf
Канада	Критична інфраструктура стосується процесів, систем, об'єктів, технологій, мереж, активів і послуг, необхідних для здоров'я, безпеки, економічного добробуту канадців і ефективного функціонування уряду. Джерело: Національна стратегія розвитку критичної інфраструктури (2009) та План дій щодо критичної інфраструктури на 2014-2017 рр.
Європейський Союз	Критична інфраструктура «означає актив, систему або її частину, розташовану в державах-членах, яка є важливою для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, безпеки, економічного чи соціального добробуту людей, і порушення або знищення якої призведе до значний вплив у державі-члені в результаті нездатності підтримувати ці функції. Європейська критична інфраструктура» або «ECI» означає критичну інфраструктуру, розташовану в державах-членах, порушення або знищення якої матиме значний вплив принаймні на дві держави-члени. Джерело: Директива Ради 2008/114/ЕС
Чехія	Критична інфраструктура - елемент критичної інфраструктури або система елементів критичної інфраструктури, порушення роботи яких мало б суттєвий вплив на безпеку держави, забезпечення основних життєвих потреб населення, здоров'я людей та економіку держави - (АКТ ПРО КРИЗОВИЙ МЕНЕДЖМЕНТ N. 240/2000 Зб).
Об'єднані Нації	Фізичні споруди, засоби, мережі та інші активи, які надають послуги, необхідні для соціального та економічного функціонування спільноти чи суспільства. Джерело: UNISDR Terminology on Disaster Risk Reduction https://www.unisdr.org/we/inform/terminology
Естонія	Прийняте таке ж визначення, як і в Директиві Європейської Ради 2008. Крім того, Естонія ввела термін «життєво важливі послуги» у національне законодавство. Життєво необхідна послуга – це послуга, яка має величезний вплив на функціонування суспільства і переривання якої становить безпосередню загрозу життю чи здоров'ю людей або функціонуванню іншої життєво важливої служби чи служби загального інтересу. Життєво важливі служби розглядаються в цілому разом із будівлею, обладнанням, персоналом, резервами та іншими подібними об'єктами, необхідними для функціонування життєво важливих послуг. Джерело: Управління інформаційної системи Естонської Республіки https://www.ria.ee/en/ciip.html
Люксембург	Критична інфраструктура означає будь-яку точку, систему або її частину, яка необхідна для захисту життєво важливих інтересів або суттєвих потреб усієї чи частини країни чи населення, або яка, ймовірно, буде піддана певній загрозі Джерело: Loi 23 juillet, 2016http://legilux.public.lu/eli/etat/leg/memorial/2016/137
Франція	Інституції, структури чи об'єкти, які надають основні товари та послуги, що утворюють основу французького суспільства та його способу життя. Джерело: Генеральний секретаріат оборони та національної безпеки (SGDSN), січень 2017 р http://cache.media.education.gouv.fr/file/2017/54/5/SGDSN-PLAQUETTE_SAIV_ANG_12012017_763545.pdf
Німеччина	Критичні інфраструктури (KI) — це організаційні та фізичні структури та об'єкти, які мають таке життєво важливе значення для суспільства та економіки країни, що їх несправність або деградація призведе до тривалого дефіциту поставок, значного порушення громадської безпеки та безпеки або інших драматичних наслідків. Джерело: Національна стратегія захисту критичної інфраструктури (2009)
Ізраіль	Комплекс будівель та інфраструктури, технологічних систем, матеріально-технічного обладнання, обчислювальних і комунікаційних систем, які інституційно активовані та контрольовані, що надає життєво важливі послуги населенню та економіці. Джерело: Анкета критичної інфраструктури Форуму високого рівня ризиків ОЕСР 2017 р.
Півд. Корея	Національна інфраструктура передбачає, що об'єкти вважаються необхідними для постійного управління для захисту національної інфраструктури відповідно до наступних стандартів, 1.Хвильовий вплив на іншу інфраструктуру, системи тощо; 2.Необхідність принаймні двох центральних адміністративних органів для спільного реагування на катастрофи; 3.Масштаби та масштаби шкоди, завданої будь-якою катастрофою національній безпеці, економіці та суспільству; Можливість того, що може статися катастрофа, і легкість відновлення після такої катастрофи. Джерело: Рамковий закон про управління надзвичайними ситуаціями та забезпечення безпеки
Мексика	Стратегічна інфраструктура визначається як інфраструктура, необхідна для надання суспільних благ і послуг, знищення або порушення якої становить загрозу національній безпеці.

Голандія	Певні процеси дуже критичні для голландського суспільства. Невдача або зрив таких процесів призведе до серйозних соціальних розладів і створить загрозу національній безпеці. Ці процеси разом утворюють критичну інфраструктуру Нідерландів. Джерело: Національний координатор з питань безпеки та боротьби з тероризмом, січень 2018 р. https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf
Нова Зеландія	Критична інфраструктура, яку також називають інфраструктурою національного значення, може бути широко визначена як системи, активи, засоби та мережі, які надають основні послуги та необхідні для національної безпеки, економічної безпеки, процвітання, здоров'я та безпеки відповідних націй. Джерело: Critical 5 – Forging a Common Understanding for Critical Infrastructure, спільна розповідь, березень 2014 р., Казначейство Нової Зеландії.
Норвегія	Критична інфраструктура – це об'єкти та системи, які є абсолютно необхідними для підтримки критичних функцій громади, що, знову ж таки, покриває базові потреби суспільства та почуття безпеки населення. Джерело: Опитування ОЕСР щодо критичної інфраструктури (2017)
Польща	Закон від 26 квітня 2007 року про антикризовий менеджмент (Dz. U. [Закон. вісник] від 2013 р., п. 1166 та 2015 р., п. 1485 надалі іменований як: «Закон про управління в кризових ситуаціях») визначає критичну інфраструктуру як системи та функціональні об'єкти, що входять до їхньої частини, які взаємопов'язані, такі як будівельні майданчики, об'єкти, установки, ключові служби для безпеки держави та її громадян і служить для забезпечення ефективної діяльності органів державного управління, а також установ і підприємців Джерело: Національна програма захисту критичної інфраструктури Польщі, 2015 р
Португалія	Критична інфраструктура – це компонент, система або її частина, яка є важливою для підтримки життєво важливих функцій суспільства, здоров'я, безпеки та економічного чи соціального добробуту, і порушення чи знищення якої матиме значний вплив, враховуючи обставини, що інфраструктура не зможе продовжувати виконувати ці функції. Джерело: Опитування ОЕСР щодо критичної інфраструктури (2017)
Словакія	a) Елемент критичної інфраструктури (надалі іменований як «елемент») означає головним чином інженерну споруду, державну службу та інформаційну систему в секторі критичної інфраструктури, порушення або знищення якої повинно, згідно з галузевими критеріями та наскрізними критеріями, мати негативні наслідки вплив на виконання економічних і соціальних функцій держави, а відтак і на якість життя мешканців щодо захисту їхнього життя, здоров'я, безпеки, власності, а також навколишнього середовища; b) Сектор критичної інфраструктури (далі – «сектор») означає частину критичної інфраструктури, яка включає елементи; сектор може включати один або більше підгалузей критичної інфраструктури (далі- «підсектор»); c) Критична інфраструктура означає систему, яка поділена на сектори та елементи Джерело: Закон Словаччини № 45/2011
Іспанія	Критичні інфраструктури – це ті стратегічні інфраструктури (об'єкти, мережі, системи та фізичне обладнання, на яких базується функціонування основних послуг), які є незамінними та де альтернативне рішення неможливе, так що їх порушення або знищення може серйозно вплинути на основні послуги. Джерело: CNPIC (2017)http://www.cnpic.es/en/Legislacion_Aplicable/Generico/index.html
Швеція	Ті активи, системи або їх частини, розташовані в державах-членах ЄС, які мають важливе значення для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, безпеки, економічного чи соціального добробуту людей, і порушення або знищення яких матиме значну шкоду. вплив на державу-члена в результаті нездатності підтримувати ці функції. Термін «Критична інфраструктура» (KI) стосується діяльності, засобів, вузлів, інфраструктури та послуг, які підтримують життєво важливі функції суспільства (VSF). Життєво важливі соціальні функції (VSF) — це термін для діяльності, яка підтримує задану функціональність. Кожна така функція включена в один або декілька суспільних секторів Джерело: Шведське агентство цивільних непередбачених ситуацій, 2016 р.; План дій щодо захисту життєво важливих функцій суспільства та критичної інфраструктури (2014)
Швейцарія	Критичні інфраструктури – це процеси, системи та об'єкти, які мають важливе значення для функціонування економіки та добробуту населення відповідно Джерело: Опитування ОЕСР щодо критичної інфраструктури (2017)
Туреччина	Сукупність мереж, активів, систем і структур, які могли б спричинити серйозний вплив на безпеку, економіку, здоров'я громадян в результаті негативного впливу на поведінку навколишнього середовища, соціальний порядок і державну службу, якщо вони не виконують свої функції частково або повністю. Джерело: Опитування ОЕСР щодо критичної інфраструктури (2017)
Великобританія	Ті критичні елементи інфраструктури (а саме активи, об'єкти, системи, мережі або процеси та основні працівники, які їх обслуговують і сприяють), втрата або компрометація яких може призвести до: а) Серйозний шкідливий вплив на доступність, цілісність або надання основних послуг – у тому числі тих послуг, цілісність яких у разі порушення може призвести до значних людських жертв або жертв – беручи до уваги значні економічні чи соціальні наслідки; та/або б) Значний вплив на національну безпеку, національну оборону або функціонування держави. Джерело: Опитування ОЕСР щодо критичної інфраструктури (2017)
США	Критична інфраструктура — це системи й активи, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що непрацездатність або знищення таких систем і активів матиме виснажливий вплив на безпеку, національну економічну безпеку, охорону здоров'я чи безпеку країни або будь-яку комбінацію ці питання. Джерело: Національний план захисту інфраструктури 2013 р. Партнерство для безпеки та стійкості критичної інфраструктури.

Додаток 3.C. Список критичних секторів для країн ОЕСР

	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA
Енергетика	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ядерка				●			●		●			●	●				●		●				●	●								●
Зв'язок	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Транспорт	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Вода	●	●	●	●	●		●	●	●	●	●	●	●				●		●	●	●		●	●	●	●		●				●
Дамби та греблі	●					●	●					●			●	●		●	●	●		●	●	●					●		●	●
Вироб. та постач їжі	●	●		●	●		●	●	●		●	●	●				●				●			●		●				●	●	●
Здоров'я	●	●	●	●	●	●	●	●	●	●	●	●	●				●		●	●	●			●		●		●		●	●	●
Фінанси та банки	●	●	●	●	●		●	●	●	●	●	●	●				●		●	●	●		●	●		●		●		●	●	●
Урядування		●		●	●		●	●	●			●	●				●		●	●	●			●		●				●		●
Цивіль.захист	●	●		●	●		●	●	●				●				●			●	●		●	●						●		●
Правосуддя		●				●		●				●	●				●			●	●		●	●								
Хімічна промис.	●	●			●				●		●	●	●				●			●	●		●	●		●		●				●
Космічний сект.			●						●			●	●																			
Оборон. Індустр.	●										●	●	●				●			●												●
Критичне виробництво				●							●	●					●							●							●	●
Інше.		●	●					●	●	●	●	●	●				●		●	●	●		●	●	●	●				●	●	●

Додаток 3.D. Перелік і опис інструментів політики для підвищення стійкості критичної інфраструктури

Інструмент політики	Опис
Надання інформації пронебезпеки та загрози	Уряди надають власникам і операторам критичної інфраструктури результати оцінки небезпек і загроз на національному рівні або в інфраструктурі.
Механізми або платформи добровільного обміну інформацією	Уряди заохочують власників і операторів критичної інфраструктури обмінюватися інформацією, що стосується безпеки та стійкості активів і систем, між собою та з урядом на добровільній основі.
Обов'язкові механізми або платформи обміну інформацією	Закони та нормативні акти вимагають від операторів критичної інфраструктури ділитися з урядом інформацією, яка стосується безпеки та стійкості активів і систем.
Заходи з підвищення обізнаності та тренінги	Заходи з підвищення обізнаності та тренінги сприяють розвитку культури ризику в критичній інфраструктурі. Тренінги та навчання перевіряють системи управління критичною інфраструктурою в надзвичайних ситуаціях та формують ознайомлення з відповідними обов'язками під час криз.
Рекомендації щодо стійкості для операторів критичної інфраструктури	Рекомендації щодо стійкості окреслюють кроки та методи, які оператори критичної інфраструктури повинні виконувати для підвищення стійкості своїх активів і систем загалом. Такі керівні принципи можуть бути вузькими за обсягом, надаючи, наприклад, лише керівництво для оцінки небезпеки на рівні оператора, або широкими за обсягом, перераховуючи численні інструменти та заходи.
Сприяння розвитку/використанню професійного стандарт	Галузеві нормативні акти, присвячені CIP
Механізм стимулювання для оцінки ризиків і вразливостей	Правила забезпечення безперервності діяльності на основі ефективності які заохочують операторів критичної інфраструктури проводити оцінку небезпеки, ризику та вразливості. Стимулами можуть бути надання технічної підтримки та керівних документів або механізми винагороди, такі як оприлюднені огляди досягнення цілей стійкості або сертифікації.
Механізми стимулювання інвестування в стійкість	Уряди надають стимули, які заохочують операторів критичної інфраструктури інвестувати в стійкість критичної інфраструктури, зокрема: субсидії, аналіз витрат і вигод або участь уряду в схемах страхування.
Розробка професійних стандартів стійкості критичної інфраструктури, таких як коди та контрольні показники можливостей і стандартів операцій	Уряди розробляють нормативні акти, які визначають операторів критичної інфраструктури для виконання певних. Цей інструмент встановлює обов'язкові зобов'язання для критичної інфраструктури, яких необхідно виконати, щоб забезпечити захист і стійкість на основі галузевих особливостей. Норми, які заохочують операторів критичної інфраструктури досягати цільового рівня продуктивності для підтримки послуг під час збоїв.
Обов'язкові плани безперервності бізнесу	Уряди вимагають від операторів критичної інфраструктури розробки планів безперервності бізнесу. Такі плани включають заходи запобігання та готовності (включаючи плани на випадок надзвичайних ситуацій), на які оператори можуть покладатися під час небезпечних подій, щоб забезпечити продовження бізнес-операцій.
Перевірки та оцінка ефективності	Уповноважені інспектори перевіряють, чи оператори критичної інфраструктури запровадили необхідні заходи стійкості.
Штрафи за недотримання вимог стійкості	У випадках, коли перевірки виявляють, що оператори критичної
Інші види штрафів за невиконання	Інші види покарань за невідповідність можуть включати: анулювання ліцензії на експлуатацію або тимчасове усунення з експлуатації до виконання вимог.
Ранжування на основі результатів перевірки/виконання	Уряд рейтингує та оголошує результати еревірки/виконання. Оператори зацікавлені в тому, щоб добре потрапити в подібні рейтинги, оскільки збереження іміджу та репутації є важливим фактором успіху бізнесу
Звітність по стійкості по операторам	Самооцінка стійкості операторів критичної інфраструктури та надання результатів уряду та/або широкій громадськості.
Обмін передовим досвідом	Державні інвестиції в стійкість застосовуються до нової громадської інфраструктури на додаток до забезпечення того, щоб прогалини в стійкості були задоволені там, де є потреби. Державне фінансування для створення стійких систем критичної інфраструктури може встановити стандарти для промисловості та продемонструвати цінність цих початкових інвестицій у стійкість.
Державні інвестиції в стійкість інфраструктури	Державні інвестиції в стійкість застосовуються до нової громадської інфраструктури на додаток до забезпечення того, щоб прогалини в стійкості були задоволені там, де є потреби. Державне фінансування для створення стійких систем критичної інфраструктури може встановити стандарти для промисловості та продемонструвати цінність цих початкових інвестицій у стійкість.
Керівництво для субнаціональних рівнів управління	Керівні принципи для субнаціональних рівнів управління щодо обізнаності про критичну інфраструктуру у відповідних юрисдикціях і поблизу, яка може становити транскордонні ризики, і як посилити стійкість цих систем
Обов'язкове страхування критичної інфраструктури	Зобов'язання, встановлені для власників і операторів критичної інфраструктури, купувати страхування заздалегідь на випадок шоку або зриву послуг.
Рецензування, моніторинг та оцінка	Експерти переглядають і оцінюють прогрес на основі узгоджених критеріїв оцінки відповідно до вказівок щодо стійкості до окремих секторів... Результати можуть виявити потенційні прогалини та надати пропозиції щодо напрямків покращення.

Додаток 3.E. Практика країн щодо стійкості критичної інфраструктури визначено в Інструментарії OECP з управління ризиками (TRIG)

Надійна мережа обміну інформацією для критичної інфраструктури в Австралії

Довірена мережа обміну інформацією (TISN) для стійкості критичної інфраструктури була створена урядом Австралії в 2003 році з метою надання допомоги організаціям критичної інфраструктури для кращого запобігання, підготовки, реагування та відновлення після збоїв і несприятливих подій. TISN забезпечує форуми національного рівня для власників і операторів критичної інфраструктури для обговорення вразливостей критичної інфраструктури з відповідними урядовими установами та спільної роботи над розробкою стратегій і рішень для зменшення ризиків. На чолі з Департаментом генерального прокурора та за підтримки ряду австралійських урядових установ TISN тепер охоплює сотні членів, включаючи представників багатьох найбільших і найвідоміших компаній Австралії, а також урядів штатів і територій. TISN працює на основі всіх небезпек. Він складається з семи секторальних груп критичної інфраструктури (енергетика, вода, зв'язок, банки та фінанси, охорона здоров'я, транспорт, продовольство) та дві консультативні групи експертів. Члени TISN регулярно зустрічаються у своїх галузевих групах у безпечному, неконкурентному середовищі, щоб обмінюватися важливою інформацією про ризики та стратегії пом'якшення, а також розробляти колективні рішення для спільних проблем. Крім того, проводяться регулярні зустрічі та навчання між групами та з урядами.

Обґрунтування

Критична інфраструктура надає основні послуги, такі як харчування, вода, охорона здоров'я, електроенергія, зв'язок, транспорт і банківська справа. Без цих послуг соціальна єдність Австралії, економічне процвітання та громадська безпека знаходяться під загрозою. Trusted Information Sharing Network реагує на це, забезпечуючи форум для державних і приватних зацікавлених сторін для співпраці для підвищення стійкості критичної інфраструктури.

Цілі

- ✓ *Встановлюйте ефективне партнерство між бізнесом та державою з власниками та операторами критичної інфраструктури;*
- ✓ *Обмін інформацією та методами, необхідними для оцінки та зменшення ризиків для критичної інфраструктури;*
- ✓ *Розвиток потенціалу стійкості в організаціях.*

Результати

- *З моменту свого створення TISN вплинув на національне обговорення питань критичної інфраструктури, співпрацюючи з ключовими зацікавленими сторонами, щоб уможливити зміни;*
- *TISN сприяв узгодженому підходу до усунення спільних загроз і вразливостей і підвищення стійкості в критичних секторах інфраструктури;*

- *Ініціативи TISN включають розробку спільних структур, посібників і планових документів, підготовку широкомасштабних навчань і організацію семінарів. Ці ініціативи сприяли підвищенню стійкості систем критичної інфраструктури в Австралії.*

Вивчені уроки

- *Створення платформ для обміну інформацією між політиками, власниками таоператорами критичної інфраструктури має великі переваги.*
- *Партнерство між бізнесом і урядом має ключове значення для заохочення приватного сектора довзаємних інтересів, таких як безперервність і стійкість бізнесу.*
- *Створення платформ для обміну інформацією між політиками, власниками та операторами критичної інфраструктури має великі переваги.*
- *Партнерство між бізнесом і урядом має ключове значення для заохочення приватного сектора довзаємних інтересів, таких як безперервність і стійкість бізнесу.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/ trustedinformationsharingnetworkforcriticalinfrastructureinaustralia.htm

Інтегрований підхід до захисту критичної інфраструктури в Нідерландах

Новий інтегрований підхід до захисту критичної інфраструктури був створений у травні 2015 року в рамках Стратегії національної безпеки та безпеки, розробленої міністерством безпеки та юстиції Нідерландів. Підхід містить три кроки. По-перше, підхід визначає, що таке критична інфраструктура, на основі економічних, фізичних і соціальних критеріїв впливу. Критерії розроблено на основі національного процесу оцінки ризиків. Ступінь критичності залежить від наслідків збою виявлених критичних секторів. Розрізняють категорію A, де збої можуть мати значні наслідки та каскадні наслідки, і категорію B, де наслідки можуть бути меншими, щоб відобразити різноманіття критичної інфраструктури та встановити пріоритети. По-друге, оцінка вразливості дає розуміння найважливіших ризиків, загрози, вразливості та ступінь стійкості цієї інфраструктури. Третім кроком підходу є укладення угод щодо підтримки або, за необхідності, підвищення стійкості життєво важливої інфраструктури. Це дозволяє використовувати індивідуальний підхід для підвищення стійкості на основі ризиків, загроз і вразливостей. Крім того, критична інфраструктура буде включена до національних структур управління кризою.

Обґрунтування

Гарантування безперервності критичної інфраструктури становить спільний інтерес як для операторів інфраструктури (як правило, приватних), так і для суспільства в Нідерландах. Критична інфраструктура включає продукти, послуги та основні процеси, які, якщо вони вийдуть з ладу, можуть спричинити масштабні соціальні зриви. Ось чому уряд і важливі організації в Нідерландах співпрацюють у захисті цієї інфраструктури.

Необхідний комплексний підхід через кількість сторін, мереж і рівнів, які беруть участь. Це динамічна та складна сфера через технологічний розвиток і взаємозв'язок критичних процесів. Суспільство стало більш залежним від критичної інфраструктури, тоді як невдача такої інфраструктури стала менш сприйнятою суспільством. Інфраструктура стала більш залежною та вразливішою до (навмисних) кіберінцидентів. Крім того, взаємозв'язок критичних процесів ускладнює прогнозування ефектів каскаду. Каскадні ефекти, викликані збоями процесів, призводять до більшого впливу на суспільство.

Цілі

- *Надійна критична інфраструктура*
- *Виявлення критичної інфраструктури на основі*
- *впливу Розуміння ризиків, загроз і вразливостей*
- *Розробка індивідуальних угод*

Результати

- *Методологія ідентифікації на основі впливу Від галузевого підходу до*
- *процесного підходу Визначення критичної інфраструктури на*
- *національному рівні пріоритетний перелік критичної*
- *інфраструктури на національному рівні Індивідуальні угоди для*
- *кожного критичного процесу*
- *Методика моніторингу та оцінки*

Вивчені уроки

- *Сприяння підходу, що враховує всі небезпеки, є хорошим способом взаємодії з приватними операторами, оскільки вони можуть бути особливо зацікавлені в одній конкретній загрозі, не маючи повного уявлення про ризики*

- *Наявність чітких і прозорих критеріїв для ідентифікації критичної інфраструктури сприяє залученню різних зацікавлених сторін.*
- *Потрібне політичне рішення, які критерії впливу вважаються руйнівними. Існує ризик того, щозміни в суспільних уподобаннях можуть призвести до змін у порогових значеннях, що вимагатиме переоцінки критичної інфраструктури.*
- *Розвиток партнерства з приватними операторами вимагає розвитку довіри між державним і приватним секторами та загального розуміння* проблем, *які виникають удовгостроковій перспективі.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/integratedapproachforcriticalinfrastructureprotectioninthenetherlands.htm

Національна стратегія захисту критичної інфраструктури в Німеччині

Німецька національна стратегія захисту критичної інфраструктури підсумовує цілі та завдання Федеральної адміністрації та її політико-стратегічний підхід до активного вирішення питань захисту критичної інфраструктури (CIP). Стратегія ґрунтується на принципі спільних дій держави, суспільства, бізнесу та промисловості. Держава співпрацює з іншими державними та приватними суб'єктами у розробці аналізу та концепцій захисту. Стратегія спочатку визначає критичну інфраструктуру як організаційні та фізичні структури та об'єкти, які мають таке життєво важливе значення для суспільства та економіки країни, що їх несправність або деградація призведе до стійкого дефіциту постачання, значного порушення громадської безпеки та безпеки або інших драматичних наслідків. Він також визначає основні загрози, ризики та вразливі місця систем критичної інфраструктури в Німеччині. Його керівний принцип полягає в тому, що відповідальність за безпеку, надійність і доступність такої інфраструктури є спільною відповідальністю. У Стратегії аналізуються існуючі заходи та пропонується подальший шлях структурування різних ініціатив і подальшого вдосконалення захисту систем критичної інфраструктури. Він розробляє вказівки щодо запобігання,

реагування та сталого розвитку, засновані на трьох стовпах: (1) Запобігання та зменшення втрати послуг і пропонує подальший шлях структурування різних ініціатив і подальшого вдосконалення захисту систем критичної інфраструктури. Він розробляє вказівки щодо запобігання, реагування та сталого розвитку, засновані на трьох стовпах: (1) Запобігання та зменшення втрати послуг і пропонує подальший шлях структурування різних ініціатив і подальшого вдосконалення захисту систем критичної інфраструктури. Він розробляє вказівки щодо запобігання, реагування та сталого розвитку, засновані на трьох стовпах: (1) Запобігання та зменшення втрати послуг

(2) Сприяння резервним системам (резервування) і надзвичайним можливостям (3) Посилення можливостей самозахисту. Зараз тривають розробки щодо захисту критичної інфраструктури в Німеччині

Обґрунтування

Інфраструктура загалом і критична інфраструктура зокрема життєво важливі для функціонування та добробуту сучасних і ефективних суспільств. Німеччина є однією з провідних індустріальних і технологічно орієнтованих націй. Німеччина також є важливим місцем для ділової діяльності та промисловості. Забезпечення конкурентоспроможності країни в глобалізованих економічних і технологічних умовах значною мірою залежить від наявності високоефективної та добре функціонуючої інфраструктури. Таким чином, забезпечення захисту цієї інфраструктури є ключовою функцією заходів готовності, пов'язаних з безпекою, які вживаються промисловістю та урядовими установами, і є центральним питанням політики безпеки країни.

Цілі

- *Керівництво федеральним урядом, а також землями, муніципалітетами та підприємствами в їхніхзусиллях із захисту критичної інфраструктури.*
- *Скоординовано сприяйте стійкості критичної інфраструктури.*
- *Зміцнюйте громадську безпеку*
- *Сприяти спільним діям уряду, компаній і/або операцій і громадянського суспільства для захисту критичної інфраструктури*

Результати

- *Впровадження робочих пакетів у Федерації, землях та місцевих органах влади, які включають (1) визначення загальних цілей захисту, (2) аналіз загроз, вразливостей і можливостей управління, (3) оцінку загроз, (4) специфікацію цілі захисту з урахуванням існуючих захисних заходів; аналіз існуючих нормативних актів і, де це можливо, визначення додаткових заходів, що сприяють досягненню мети; і, якщо потрібно, законодавство.*
- *Розробка програм і планів (таких як Національний план захисту інформаційної інфраструктури), конкретних рекомендацій щодо дій (таких як Національна базова концепція захисту, Керівництво з управління ризиками та кризовими ситуаціями для операцій критичної інфраструктури, а також стандартів, норм і правил (таких як Стандарти інформаційної безпеки BSI, або правила Німецької асоціації газопостачання таводопостачання щодо управління ризиками у сфері питного водопостачання).*

Вивчені уроки

- *Збереження захисту критичної інфраструктури набуває все більшого значення, особливов контексті все більш взаємозалежних економік.*
- *Співпраця та партнерство у сфері критичної інфраструктури як з органами влади, так і, зокрема, з приватними постачальниками послуг є життєво важливими для забезпечення успішної роботи.*

- *Метою стратегії критичної інфраструктури має бути не абсолютний захист, авпровадження заходів, які сприяють стійкості.*
- *Міжгалузева співпраця та координація є ключовими для досягнення стійкості критичноїінфраструктури.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/ nationalstrategyforcriticalinfrastructureprotectioningermany.htm

Швейцарська базова стратегія захисту критичної інфраструктури

Швейцарська національна стратегія захисту критичної інфраструктури була створена в 2012 році на основі «Базової стратегії захисту критичної інфраструктури» (2009). Головною метою Стратегії є підвищення стійкості критичної інфраструктури Швейцарії. Стратегія окреслює стратегічні цілі, а також ключові принципи та описує заходи, які необхідно вжити у сфері критичної інфраструктури. Ці заходи включають покращення загальної відмовостійкості критичної інфраструктури та покращення загальної основи для міжгалузевої співпраці. Стратегія охоплює визначення комплексних підходів до захисту, ідентифікацію та компіляцію елементів і об'єктів критичної інфраструктури в секретному реєстрі, створення міжгалузевих державно-приватних платформ, та обмін інформацією про ризики, зокрема оцінку ризиків і системи попередження, між зацікавленими сторонами. У Стратегії також розглядається федеральна підтримка для усунення збоїв у критичній інфраструктурі, якщо ресурси операторів і піддержавних суб'єктів перевантажені. Він встановлює постійний процес підвищення стійкості систем критичної інфраструктури шляхом сприяння скоординованому підходу між відповідними операторами CI, а також спеціалізованими та регуляторними органами. Десять секторів вважаються критичними на національному рівні, включаючи енергетику, транспорт, інформаційні та комунікаційні технології, фінансові послуги, державне управління, охорону здоров'я, громадську безпеку та транспорт. Вони поділяються на 28 підсекторів, як-от постачання природного газу, постачання нафти та енергопостачання в секторі енергопостачання. зокрема системи оцінки ризиків і попередження серед зацікавлених сторін. У Стратегії також розглядається федеральна підтримка для усунення збоїв у критичній інфраструктурі, якщо ресурси операторів і піддержавних суб'єктів перевантажені. Він встановлює постійний процес підвищення стійкості систем критичної інфраструктури шляхом сприяння скоординованому підходу між відповідними операторами CI, а також спеціалізованими та регуляторними органами. Десять секторів вважаються критичними на національному рівні, включаючи енергетику, транспорт, інформаційні та комунікаційні технології, фінансові послуги, державне управління, охорону здоров'я, громадську безпеку та транспорт. Вони поділяються на 28 підсекторів, як-от постачання природного газу, постачання нафти та енергопостачання в секторі енергопостачання. зокрема системи оцінки ризиків і попередження серед зацікавлених сторін. У Стратегії також розглядається федеральна підтримка для усунення збоїв у критичній інфраструктурі, якщо ресурси операторів і піддержавних суб'єктів перевантажені. Він встановлює постійний процес підвищення стійкості систем критичної інфраструктури шляхом сприяння скоординованому підходу між відповідними операторами CI, а також спеціалізованими та регуляторними органами. Десять секторів вважаються критичними на національному рівні, включаючи енергетику, транспорт, інформаційні та

комунікаційні технології, фінансові послуги, державне управління, охорону здоров'я, громадську безпеку та транспорт. Вони поділяються на 28 підсекторів, як-от постачання природного газу, постачання нафти та енергопостачання

Обґрунтування

Швейцарія дуже залежить від безперервної роботи критичної інфраструктури,

яка забезпечує постачання життєво важливих товарів і послуг. Збої можуть мати швидкі наслідки для населення та основи його існування, а також можуть вплинути на іншу критичну інфраструктуру через каскадні ефекти. У різних критичних секторах заходи захисту вже впроваджуються на індивідуальній основі. Однак відсутність міжгалузевої координації між зацікавленими сторонами критичної інфраструктури та необхідність просування консолідованого підходу на національному рівні створили потребу в інтегрованій національній стратегії.

Цілі

- *Сприяння підтримці працездатності систем критичної інфраструктури, визначення*
- *систем критичної інфраструктури, які необхідно захистити,*
- *Полегшення процедур аналізу ризиків,*
- *Започаткування міжгалузевої співпраці шляхом створення платформ координації таобміну інформацією.*

Результати

- *Класифікована інвентаризація критичної інфраструктури*
- *Створено рекомендації щодо критичної інфраструктури*
- *Проведені підгалузеві оцінки ризиків і вразливості Встановлені*
- *допоміжні інструменти (наприклад, методологія, сценарії тощо)*

Вивчені уроки

- *Захист критичної інфраструктури сьогодні стає все більш важливим, зокрема у великих містах і малих взаємозалежних країнах, таких як Швейцарія.*
- *Метою стратегії критичної інфраструктури має бути не абсолютний захист, авпровадження заходів для підвищення стійкості.*
- *Міжгалузева співпраця та координація є ключовими.*
- *Слід заохочувати співробітництво між країнами у світі, що все більше глобалізується.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/swissbasicstrategyforcriticalinfrastructureprotection.htm

Державно-приватне партнерство для стійкості критичної інфраструктури у Фінляндії

Національне агентство з надзвичайних ситуацій (NESA), створене в 1993 році, займається плануванням, розробкою та підтримкою безпеки постачання у Фінляндії. Незважаючи на те, що його історична роль у підтримці резервних запасів для захисту засобів до існування населення, а також функціонування економіки залишається частиною його стратегічних завдань, NESA все активніше впроваджує безперервність і стійкість бізнесу в різних секторах економіки через громадські -приватне партнерство. NESA створила мережу тематичних кластерів, де ключові зацікавлені сторони критичних секторів, таких як: постачання продуктів харчування, енергетика, транспорт, охорона здоров'я чи промисловість, розвивають партнерства з метою оцінки вразливості та ефективності та планування стійкості. NESA також пропонує спеціальні інструменти, такі як інформаційні системи, засоби зберігання та транспортування для підтримки безперервності роботи в цих доменах. NESA також фінансує конкретні заходи, пов'язані з безперервністю бізнесу та захистом критичної інфраструктури. Агентство готує щорічні звіти, в яких оцінюється діяльність компаній у

критичних секторах, включаючи рейтинги та конкретні рекомендації

Обґрунтування

Фінляндія стикається з особливою вразливістю щодо порушення ланцюгів постачання та критичної інфраструктури, що становить серйозну проблему. Суворі зимові умови, висока залежність від морського транспорту та міжнародних ринків, взаємозалежності та складність критично важливих мереж є одними з ключових викликів для безпеки поставок у Фінляндії.

Отже, Фінляндія доклала значних зусиль для забезпечення постачання та підтримки безперервності послуг. Це є першочерговою проблемою Стратегії безпеки суспільства, згідно з якою функціонування економіки та інфраструктури є однією із семи життєво важливих функцій фінського суспільства.

Цілі

- *Забезпечення поставок для забезпечення безперервності економічної діяльності тафункціонування критичної інфраструктури у випадках серйозних порушень та надзвичайних обставин;*
- *Створення приватно-державного партнерства як основного методу забезпечення постачання тарозвитку безперервності бізнесу;*
- *Впровадження технічних і фінансових заходів для підтримки розвитку безперервності бізнесу в суспільстві, виробництві товарів і послуг, необхідних увиняткових умовах.*

Результати

- *Розширення державно-приватного партнерства з компаніями в критичних секторах (зараз понад 1000), які всі дали план безперервності бізнесу, специфічний для їх діяльності та сектора;*
- *Створено 7 тематичних кластерів і спеціалізованих груп для обговорення та впровадження галузевихполітик безпеки постачання та безперервності бізнесу;*
- *Розроблено інструменти управління безперервністю, призначені для підтримки організацій у їхніх зусиллях зуправління безперервністю.*

Вивчені уроки

- *Державні органи в країнах не повинні брати на себе повну відповідальність за підтримку безперервності послуг, але також приватний сектор повинен інвестувати певні зусилля в готовність, щоб досягти загальносуспільного підходу до запобігання ризикам*
- *Стимулювання зусиль приватного сектору щодо забезпечення безперервності бізнесу має важливе значення для сприяння його участі в цих зусиллях. Оцінка діяльності окремих компаній є додатковимі ефективним способом стимулювання прогресу.*
- *Оскільки безпека поставок і безперервність критичної інфраструктури залежить від ринку, особлива увага до питань, пов'язаних із чесною конкуренцією, недискримінацією та рівнимставленням, є фундаментальною при розробці політики*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/ publicprivatepartnershipsforcriticalinfrastructuresresilienceinfinland.htm

Національна програма захисту критичної інфраструктури в Польщі

Польська національна програма захисту критичної інфраструктури (NCIPP) була прийнята в березні 2013 року Радою міністрів Польщі, головною метою якої є забезпечення захисту систем критичної інфраструктури. NCIPP визначає бачення та цілі процесів захисту критичної інфраструктури та охоплює всі фази циклу управління ризиками: він спрямований не лише на забезпечення захисту критичної інфраструктури від загроз (запобігання), але й на сприяння зменшенню впливу та тривалості потенційні збитки (готовність і реагування). NCIPP охоплює наступні системи інфраструктури: енергетика, зв'язок, ІКТ, фінансова система, продовольче постачання, водопостачання, охорона здоров'я, транспорт, рятування, державне управління та виробництво, зберігання та використання хімічних і радіоактивних речовин. NCIPP описує співпрацю, яка має бути встановлена між окремими особами, і встановлює ролі та відповідальність для кожної зацікавленої сторони. NCIPP приділяє особливу увагу розбудові партнерства між зацікавленими сторонами. Обмін інформацією та знаннями між усіма рівнями управління, а також між державним і приватним секторами є ключовим фактором захисту систем інфраструктури. NCIPP також визначає низку передових практик і рекомендацій для забезпечення безперебійного функціонування критичної інфраструктури в кількох сферах, таких як технічний захист, захист IT/OT, правовий захист, плани безперервності/відновлення бізнесу. Передовий досвід і рекомендації були розширені, особливо в області захисту IT/OT. У листопаді 2015 року NCIPP оновлено. Тепер він містить нові пріоритети та завдання на 2015-2017 роки

Обґрунтування

Критична інфраструктура є ключовою для безперебійного функціонування державного та приватного секторів. Таким чином, захист критичної інфраструктури в Польщі має важливе значення для безперебійного функціонування економічної системи; Стійкість критичної інфраструктури також є пріоритетом, оскільки вона може негативно вплинути на життя громадян Польщі.

Цілі

- *Підвищення стійкості систем критичної інфраструктури в Польщі;*
- *Підвищення обізнаності про важливість критичної інфраструктури та вдосконаленнясистем оцінки ризиків;*
- *Дозволити скоординоване та засноване на ризиках партнерство для захисту критичноїінфраструктури*

Результати

- *Було організовано три зустрічі Національного форуму із захисту інфраструктури, на якому зібралися представники приватного сектору та адміністрації для обміну інформацією щодо стійкості критичної інфраструктури в Польщі.*
- *Розроблено чотири підручники: з перевірки автентичності документів, з вибухових загроз для критичної інфраструктури, із застосування біометрії до критичної інфраструктури та з технічного захисту систем критичної інфраструктури.*
- *Понад 800 осіб пройшли підготовку за напрямками, які охоплюють ці підручники.*

Вивчені уроки

- *Люди є найціннішим ресурсом для захисту критичної інфраструктури. Їх знання,досвід і відданість є ключовими для досягнення поставлених цілей.*
- *Стратегія, пов'язана з управлінням ризиками, повинна охоплювати чіткі цілі та плани дій, атакож точно визначати ролі кожної зацікавленої сторони.*

- *Широке партнерство та обмін інформацією є важливими для сприяння захисту критичної інфраструктури.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/ nationalcriticalinfrastructureprotectionprogrammeinpoland.htm

Національна стратегія Канади щодо критичної інфраструктури

Національна стратегія критичної інфраструктури визначає напрямок підвищення стійкості критичної інфраструктури Канади до поточних і нових небезпек. Стратегія представляє спільний підхід до посилення стійкості критичної інфраструктури, забезпечуючи доповнення федеральної, провінційної та територіальної діяльності щодо критичної інфраструктури та дотримання законів кожної юрисдикції. Він окреслює механізми покращеного обміну інформацією та захисту інформації, а також визначає важливість підходу до управління ризиками для посилення стійкості критичної інфраструктури в Канаді. Підвищення стійкості критичної інфраструктури може бути досягнуто шляхом відповідної комбінації заходів безпеки для вирішення навмисних і випадкових інцидентів, практики забезпечення безперервності бізнесу для усунення збоїв і забезпечення безперервного надання основних послуг. У ньому також розглядається важливість планування управління надзвичайними ситуаціями для забезпечення наявності відповідних процедур реагування непередбачені збої та стихійні лиха. На національному рівні Стратегія класифікує критичну інфраструктуру за 10 такими секторами: енергетика та комунальні послуги, фінанси, продовольство, транспорт, уряд, інформаційні та комунікаційні технології, охорона здоров'я, безпека, вода, виробництво

Обґрунтування

Оскільки ризики для критичної інфраструктури поширюються на різні юрисдикції та сектори, Стратегія передбачає комплексний і спільний федеральний, провінційний і територіальний підхід до підвищення стійкості критичної інфраструктури. Цей загальний підхід дозволяє партнерам колективно реагувати на ризики та спрямовувати ресурси на найбільш уразливі ділянки критичної інфраструктури.

Цілі

- *Розбудова партнерства на всіх рівнях влади та з приватним сектором; Впровадження*
- *підходу до управління ризиками, що включає всі небезпеки;*
- *Сприяння своєчасному обміну інформацією між партнерами*

Результати

Національна стратегія супроводжувалася Планом дій щодо критичної інфраструктури (2010 р.), у якому визначено пункти дій для кожної з трьох стратегічних цілей. Підсумок прогресу, досягнутого в рамках оригінального Плану дій, міститься в оновленому Плані дій щодо критичної інфраструктури (2014-2017). Наступний етап Плану дій включає вжиття додаткових кроків для кожної з трьох стратегічних цілей, викладених у Національній стратегії, спираючись на те, що вже було досягнуто в рамках початкового Плану дій (2010), з наголосом на відчутні заходи з управління ризиками

Вивчені уроки

- *Захист критичної інфраструктури сьогодні стає все більш важливим,зокрема в контексті все більш взаємозалежних економік.*
- *Метою стратегії критичної інфраструктури має бути не абсолютний захист, авпровадження заходів, які сприяють стійкості.*
- *Міжгалузева співпраця та координація є ключовими.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/canadasnationalstrategyforcriticalinfrastructure.htm

Набір інструментів для захисту критичної інфраструктури та стійкості США

Міністерство внутрішньої безпеки США створило інструментарій захисту критичної інфраструктури та стійкості для власників і операторів критичної інфраструктури на місцевому та регіональному рівнях, щоб покращити їхню здатність готуватися до повного спектру аварії 21-го століття, захищатися від неї, реагувати на неї та відновлюватися після неї. небезпеки та загрози століття. Набір інструментів розроблений, щоб допомогти власникам і операторам критичної інфраструктури включити ключові концепції Національного плану захисту інфраструктури США (NIPP) у свою повсякденну діяльність. Набір інструментів включає: Коротке відео, яке висвітлює роль місцевих і регіональних громад і приватного сектору в зусиллях із захисту національної інфраструктури. Ресурс для планування навчань, який надає прості інструменти, які допоможуть власникам і операторам спланувати «настільні» тренування на основі обговорення для оцінки захисту та стійкості інфраструктури. Питання що часто задаються про роль власників і операторів у захисті та стійкості критичної інфраструктури. Посилання на додаткові онлайн-довідкові матеріали та навчальні ресурси, пов'язані із захистом і стійкістю інфраструктури. Інформація про партнерство із захисту критичної інфраструктури та обмін інформацією.

Обґрунтування

Будучи системою критичної інфраструктури, основні медичні послуги повинні залишатися доступними для громад і окремих людей під час екстремальних погодних явищ і відразу після них, навіть під час тривалих відключень комунальних послуг і збоїв у транспортній інфраструктурі. Стійкі організації охорони здоров'я повинні передбачати ризики екстремальних погодних умов і виходити за рамки обмежень регіональної державної політики, вразливості місцевого розвитку та проблеми інфраструктури громади, коли вони розміщують, будують і модернізують заклади охорони здоров'я. Збої та збитки, яких зазнав сектор охорони здоров'я США після нещодавніх екстремальних погодних явищ, демонструють потребу в конкретних вказівках щодо способів управління новими та розвиваючимися небезпеками, пов'язаними зі зміною клімату. Наприклад, під час суперторму «Сенді» в Нью-Йорку кілька лікарень довелося евакуювати через те, що їхні резервні генератори електроенергії були розташовані в підвалі та були затоплені, або через те, що не було плану заправляти їх протягом довшого періоду, ніж 24 години. ч. Крім того, деякі з найдорожчого обладнання, наприклад рентгенівські апарати, також знаходилися в підвалі лікарні, що призвело до великих втрат у секторі. Ці події також надали можливість винести уроки з минулих катастроф, щоб медичні заклади та громади, які вони обслуговують, могли бути більш стійкими в майбутньому. З цих причин Міністерство охорони здоров'я та соціальних служб розробило Інструментарій для стійких і кліматично стійких медичних закладів для підтримки стійкості в секторі охорони здоров'я.

Цілі

- *Діліться найкращими практиками для постачальників медичних послуг, професіоналів з дизайну, політиків та інших, щоб сприяти безперервності догляду до, під час і після екстремальних погодних явищ.*
- *Оцініть поточний стан інфраструктури охорони здоров'я щодо екстремальних погодних ризиків і варіанти політики, які можна прийняти для підвищення готовності до кліматичних змін.*

- *Допомога організаціям, які займаються кліматичною стійкістю закладів охорони здоров'я, покращити їхню стійкість до екстремальних погодних явищ.*

Результати

- *Набір інструментів містить набір контрольних списків для кожного з п'яти елементів кліматичної стійкості. Ці контрольні списки можуть допомогти організаціям охорони здоров'я в оцінці пов'язаної зкліматом інфраструктури та вразливості надання медичної допомоги як на рівні системи, так і на рівніустанови, а також оцінити результати їхньої політики стійкості.*
- *Набір інструментів стійкості до зміни клімату також містить інструменти та процеси для перетворення результатів контрольного списку в практичний план для покращення стійкості та полегшить визначення стратегій для реалізації на основі оцінки, наданої контрольним списком.*

Вивчені уроки

- *Галузеві плани, які містять вказівки щодо готовності до ризиків і стійкості до ризиків, єкорисними для забезпечення актуальності та відповідності варіантів політики.*

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/uscriticalinfrastructureprotectionandresiliencetoolkit.htm

Британський центр захисту національної інфраструктури (CPNI)

Центр захисту національної інфраструктури (CPNI) захищає національну безпеку, надаючи консультації організаціям національної інфраструктури Великобританії з фізичної, кадрової та кібербезпеки. Щоб досягти захисної безпеки в секторах національної інфраструктури, CPNI підтримує зусилля зі зменшення вразливості до тероризму та інших загроз, зберігаючи основні послуги Великобританії (надаються зв'язком, екстреними службами, енергетикою, фінансами, продовольством, урядом, охороною здоров'я, транспортом і водопостачанням) безпечніше. Без цих послуг Сполучене Королівство може зазнати серйозних наслідків, включаючи серйозні економічні збитки, серйозні соціальні зриви або навіть великі людські втрати. Консультації CPNI націлені насамперед на організації критичної національної інфраструктури, які мають вирішальне значення для безперервного надання основних послуг у Великобританії. CPNI працює як з партнерами з приватного, так і з державного сектору. Серед ключових партнерів – Національний технічний орган із забезпечення інформації (CESG) і поліція – Національне управління безпеки з питань боротьби з тероризмом (NaCTSO) і мережа Радника з питань безпеки з питань боротьби з тероризмом (CTSA), а також підприємства та організації, що займаються критичною національною інфраструктурою. CPNI було створено 1 лютого 2007 року в результаті злиття Національного координаційного центру безпеки інфраструктури (NISCC) і Консультаційного центру національної безпеки (NSAC). Раніше NISCC надавав поради компаніям, які працюють у критичній національній інфраструктурі, тоді як NSAC був підрозділом MI5, який надавав поради щодо безпеки іншим частинам уряду Великобританії. Серед ключових партнерів – Національний технічний орган із забезпечення інформації (CESG) і поліція – Національне управління безпеки з питань боротьби з тероризмом (NaCTSO) і мережа Радника з питань безпеки з питань боротьби з тероризмом (CTSA), а також підприємства та організації, що займаються критичною національною інфраструктурою. CPNI було створено 1 лютого 2007 року в результаті злиття Національного координаційного центру безпеки інфраструктури (NISCC) і Консультаційного центру національної безпеки (NSAC). Раніше NISCC надавав поради компаніям, які працюють у критичній національній інфраструктурі, тоді як NSAC був підрозділом MI5, який надавав поради щодо безпеки іншим частинам уряду Великобританії.

Серед ключових партнерів – Національний технічний орган із забезпечення інформації (CESG) і поліція – Національне управління безпеки з питань боротьби з тероризмом (NaCTSO) і мережа Радника з питань безпеки з питань боротьби з тероризмом (CTSA), а також підприємства та організації, що займаються критичною національною інфраструктурою. CPNI було створено 1 лютого 2007 року в результаті злиття

Національного координаційного центру безпеки інфраструктури (NISCC) і Консультаційного центру національної безпеки (NSAC). Раніше NISCC надавав поради компаніям, які працюють у критичній національній інфраструктурі.

Обґрунтування

Національна критична інфраструктура визнається як «ці критичні елементи інфраструктури» (а саме активи, об'єкти, системи, мережі або процеси та основні працівники, які їх обслуговують і сприяють), втрата або компрометація яких може призвести до: a) значної шкоди вплив на доступність, цілісність або надання основних послуг – у тому числі тих послуг, цілісність яких, у разі порушення, може призвести до значних втрат чи жертв – беручи до уваги значні економічні чи соціальні наслідки; та/або b) значний вплив на національну безпеку, національну оборону або функціонування держави. Досягнення захисної безпеки, тобто «запровадження або вбудовування в проект заходів або протоколів безпеки, щоб загрози можна було стримувати, виявляти або мінімізувати наслідки атаки», у критичній інфраструктурі має вирішальне значення для запобігання серйозних економічних збитків, соціальних порушення або масштабна втрата життів.

Цілі

- *Підтримувати зусилля зі зменшення вразливості до тероризму та інших загроз у критичній інфраструктуріВеликобританії*
- *Вирішувати основні загрози, визначені в Стратегії національної безпеки Великобританії, тобто шпигунство,тероризм, кіберзагрози та інші загрози*
- *Надавати операторам критичної інфраструктури поради щодо безпеки та послуги з плануваннябезпеки*
- *Захистити національну безпеку*

Результати

В останні роки CPNI періодично попереджає про зростання рівня кіберзлочинності. Захист цифрових систем, у тому числі відкритих бездротових точок доступу, впровадження надійних брандмауерів і шифрування зв'язку є важливими пріоритетами, аналогічними безпеці фізичної власності та об'єктів.

Вивчені уроки

Надання централізованих консультацій критично важливим національним інфраструктурним організаціям щодо вразливості та аспектів безпеки є важливим компонентом підвищення обізнаності з цього питання. Таким чином керівництво допомагає інфраструктурі приймати більш обґрунтовані рішення та реагувати на ранні попереджувальні знаки.

Джерело:https://www.oecd.org/governance/toolkit-on-riskgovernance/goodpractices/page/centrefortheprotectionofnationalinfrastructurecpni.htm

4. Практичний приклад стійкості критичної інфраструктури: передача електроенергії та поширення у Фінляндії

Дослідження системи передачі та розподілу електроенергії Фінляндії в цьому розділі ілюструє, як уряди можуть створити ефективну модель управління, яка сприяє інвестиціям у стійкість інфраструктури. Фінляндія розвиває рамки співпраці для посилення стійкості критичної інфраструктури, яка наголошує на співробітництві між державним і приватним секторами, обміні інформацією та досягненні консенсусу щодо розробки політики та встановлення цілей. Завдяки амбітним цілям стійкості ця модель управління показала чудові результати в перші роки впровадження. Тим не менш, виникли нові виклики, включаючи те, як вирішити наслідки з точки зору витрат для клієнтів, різницю між більшими та меншими потужностями операторів, а також наслідки цифровізації та зміни клімату.

вступ

Мережа передачі та розподілу електроенергії визначена як критична інфраструктурна служба у Фінляндії, а збої в енергопостачаннях вважаються одними з найбільш критичних національних ризиків. Постачання електроенергії є життєво важливим для функціонування суспільства та економіки, особливо враховуючи високий ступінь залежності багатьох інших критичних секторів від енергопостачання (наприклад, телекомунікації, водопостачання, транспорт). У Фінляндії суворі кліматичні умови, розсіяне населення та старіння інфраструктури наражають електромережу на низку ризиків. Окрім небезпек, пов'язаних із погодними умовами, технічні аварії, гібридні загрози та кібератаки вимагають більшої уваги через потенційну вразливість, пов'язану з технологічними розробками в секторі, що характеризується підвищеною автоматизацією, цифровізацією,

Фінляндія поставила собі за мету бути найбезпечнішим суспільством у Європі. Досягнення національних цілей стійкості потребує зміцнення стійкості національної критичної інфраструктури та, зокрема, електричної мережі. Досвід екстремальної погоди у Фінляндії ілюструє масштабні наслідки перебоїв з електроенергією. У грудні 2011 року сильний шторм Тапані залишив понад 500 000 людей без електрики від кількох годин до 3 тижнів, що вплинуло на життєдіяльність громад, телекомунікаційні та водопровідні системи, закриття підприємств тощо. Вартість ремонту електромережі оцінювалася в 102,5 млн євро, а оператори виплатили споживачам 71 млн євро компенсації. Після події, громадське невдоволення значними перебоями призвело до політичних дискусій щодо термінової необхідності оновлення заходів готовності в електромережі. У 2013 році положення Закону про ринок електроенергії було оновлено та встановлено нові цілі стійкості, які потрібно досягти до 31.12.2028. Було внесено додаткові зміни щодо обмеження часу відключення, із схемами компенсації та штрафами для операторів розподілу.

У цьому прикладі обговорюються питання управління, пов'язані зі зміцненням стійкості мережі передачі та розподілу електроенергії у Фінляндії. Поряд із цілями стійкості до 2028 року Фінляндія розвиває рамки співпраці для посилення стійкості критичної інфраструктури, яка наголошує на державно-приватній співпраці, обміні інформацією та досягненні консенсусу щодо розробки політики та встановлення цілей. Підхід до управління ґрунтується на галузевих політиках безпеки постачання та комплексній національній стратегії, яка передбачає участь та координацію багатьох зацікавлених сторін. Цей підхід передбачає поєднання політичних інструментів для стимулювання інвестицій у стійкість, як нормативних, так і добровільних. Приклад ілюструє ці передові практики у Фінляндії,

Мережа передачі та розподілу електроенергії як критична інфраструктура у Фінляндії

Електропостачання є пріоритетом у Фінляндії

Мережі виробництва, передачі та розподілу енергії вважаються критично важливими інфраструктурними послугами у Фінляндії, а стійкість до збоїв вважається одним із найвищих пріоритетів.Рішення уряду від 2013 року щодо цілей безпеки постачання перераховує збої в електромережі як першу серйозну загрозу спроможності фінського суспільства функціонувати належним чином (Міністерство зайнятості та економіки, 2013). Національна оцінка ризиків 2015 року додатково підкреслює критичність енергопостачання для функціонування суспільства та економіки, а також надає перелік сценаріїв серйозних збоїв та їхніх потенційних наслідків (Міністерство внутрішніх справ, 2016). Національна оцінка ризиків

інформує Стратегію безпеки суспільства (2017), яка представляє надійне електропостачання як основну вимогу для всіх життєво важливих сфер суспільства: його переривання може поставити під загрозу інші критичні функції та вплинути на добробут населення.

Фінська система передачі та розподілу електроенергії

Концентрація виробництва електроенергії, залежність від імпорту електроенергії в пікові періоди, а також величезна територія Фінляндії та розпорошене сільське населення формують фінську мережу передачі та розподілу електроенергії. Потужність виробництва електроенергії у Фінляндії на даний момент становить 12 000 МВт, яку виробляють 150 компаній на 400 виробничих підприємствах. У той час як виробництво електроенергії з біомаси, торфу та гідроенергії поширене по всій території Фінляндії, ядерний і природний газ зосереджені в південній частині.

Очікується, що концентрація виробництва енергії зросте на півдні, коли новий ядерний реактор Олкілуото 3 почне працювати, доповнюючи чотири існуючі в Ловіісі та Олкілуото. З орієнтовним піковим попитом, що перевищує 15 000 МВт протягом зими,

Велика мережа передачі та розподілу електроенергії управляється різними операторами з різними рівнями операційних і фінансових можливостей. Відповідно до директив Європейського Союзу, мережа складається з однієї загальнонаціональної електромережі та ряду місцевих монополій з розподілу. Контрольований державою оператор системи передачі (TSO) Fingrid управляє основною мережею, яка складається з приблизно 14 400 км повітряних ліній високої напруги та 113 підстанцій. Він забезпечує баланс між попитом і пропозицією електроенергії, а також керує транскордонними з'єднаннями зі Швецією (2 підводні та 2 повітряні лінії), країнами Балтії та Росією. Регіональні та розподільні мережі середньої та низької напруги охоплюють відповідно 140 000 км (80% – повітряні лінії) та 240 000 км (60% – повітряні кабелі). За них відповідають 77 операторів систем розподілу (ОРС). Декілька з них керують більшою частиною ринку, а їхня власність – це шматок між державним і приватним. Наприклад, Helsinki DSO Helen Sähköverkko на 100% належить місту Гельсінкі, найбільший DSO Caruna належить приватним інвесторам і пенсійним фондам, а багато малих DSO у сільській місцевості належать місцевим муніципалітетам. Це робить DSO дуже різноманітними за їхніми можливостями інвестувати та підтримувати розподільні мережі та послуги. і багато малих DSO у сільській місцевості належать місцевим муніципалітетам. Це робить DSO дуже різноманітними за їхніми можливостями інвестувати та підтримувати розподільні мережі та послуги. і багато малих DSO у сільській місцевості належать місцевим муніципалітетам. Це робить DSO дуже різноманітними за їхніми можливостями інвестувати та підтримувати розподільні мережі та послуги.

Як і в багатьох країнах ОЕСР, ринок електроенергії Фінляндії зазнає серйозних змін, спричинених інноваціями та політикою щодо зміни клімату. Такі мегатренди, як поступова відмова від використання вугілля до 2029 року, зростання частки відновлюваних джерел енергії з періодичним виробництвом, розгортання інтелектуальних мереж і автоматизованих систем управління призводять до збільшення гнучкості між попитом і пропозицією, а також до залежності від інформаційних систем. Ці зміни викликають питання про те, як ці зміни вплинуть на безпеку постачання електроенергії та як системним операторам та операторам систем передачі електроенергії доведеться адаптуватися.

Основні ризики та вразливі місця фінської системи передачі та розподілу електроенергії

До 2010 року фінська система передачі та розподілу мала надзвичайно високі показники надійності, але сильні шторми поставили під сумнів її стійкість до кліматичних

ризиків, особливо щодо розподільних мереж.Суворі кліматичні умови та великі відстані електричної мережі до розосередженого населення по всій Фінляндії роблять відключення електроенергії критичним ризиком із серйозними потенційними наслідками (Forssen, 2016). У Національному ризику 2015 року.

За оцінкою, сценарій масштабного зимового шторму вважається найбільш вірогідною серйозною регіональною подією з найбільшим впливом, зокрема через збої з електроенергією, які він може створити. Сильні шторми в 2010 і 2011 роках повалили дерева на повітряні лінії, які проходять через великі лісові території країни і є важкодоступними для швидкого ремонту (Kufeoglu and Lehtonen, 2014). Ці події призвели до серйозних соціально-економічних наслідків у багатьох секторах по всій країні (вставка 4.1). Відомо також, що регулярні снігові бурі накопичують сніг на повітряних лініях або на деревах, які можуть згинати та розривати електромережі або пошкоджувати захисне обладнання.

Слід також ретельно розглянути вплив зміни клімату на моделі небезпеки та їхні потенційні наслідки для ризиків для мереж передачі та розподілу електроенергії.. Масштабні пожежі влітку 2018 року, які вразили сусідню Швецію, викликали занепокоєння, що підвищення температури може призвести до більш частих лісових пожеж у Скандинавії з потенційними наслідками для електричних мереж. Підвищення рівня моря та прибережні повені є ще одним ризиком для Фінляндії, особливо вздовж південно-західного узбережжя та більшої частини Гельсінкі, де щільність населення є найвищою, і затоплені підстанції можуть порушити розподіл. Незважаючи на те, що Фінська національна оцінка ризиків не пов’язана зі зміною клімату, вона також згадує специфічний ризик 100-річної повторюваної сонячної бурі та її наслідки для систем електроенергії.

Вставка 4.1. Шторм Тапані в 2011 році

Циклон Дагмар у грудні 2011 року, місцево відомий як шторм Тапані, продемонстрував, наскільки руйнівною та руйнівною може бути така екстремальна погода для електромережі. У той час як попередній шторм влітку 2010 року, який залишив 400 000 людей без електрики, був значним попередженням, наслідки Тапані були набагато серйознішими, оскільки це сталося взимку. Дві послідовні хвилі сильних поривів вітру вразили більшу частину західного узбережжя Фінляндії 26тисі 27тисУ грудні шторм Тапані спричинив найбільший занепокоєння у суспільстві за останні роки. 570 000 людей постраждали від перебоїв з електропостачанням, що становить одне з шести домогосподарств у країні, деякі з них тривали більше 15 днів, через труднощі з відновленням послуг. Сильний вітер і падіння дерев спричинили понад 60 000 збоїв у електромережі, а перебої з електропостачанням мали серйозні каскадні наслідки, в тому числі на високовольтну мережу Fingrid. Серйозно постраждали системи опалення, лікарні, водорозподільні та очисні споруди, а перерва в телекомунікаційних службах, які не живляться, спричинила подальші наслідки: з’єднання віддаленого доступу до електричних підстанцій було втрачено, комунікаційна мережа фінської влади зламалася, а відновлення електропостачання тривало довше. Хоча оцінки всіх цих непрямих збитків недоступні, шторм спричинив витрати на ремонт до 102,5 мільйона євро для операторів електроенергетики, 120 мільйонів євро внаслідок пошкодження лісів і оператори виплатили компенсацію своїм клієнтам у розмірі 71 мільйона євро. Ця екстремальна погодна катастрофа стала поворотним моментом для Фінляндії, щоб переглянути політику безпеки постачання в секторі електроенергії.

Джерело:(Куфеоглу та Лехтонен, 2014)

На додаток до природних небезпек, технічних збоїв або аварій, взаємозалежності та кіберзагрози чи інші ризики безпеці є ключовими питаннями для підходу, що враховує всі небезпеки та загрози, до стійкості фінських систем передачі та розподілу електроенергії. 18 липня 2018 року під час пожежі в трансформаторі струму на підстанції Olkiluoto згоріли захисні кабелі (Fingrid, 2018). У результаті дві атомні електростанції були закриті та виведені з мережі, що спричинило серйозний шок у постачанні, що вимагало активації резервів енергії. Це підкреслило потенційний ефект доміно цих типів аварій і необхідність планування готовності. Подібна ситуація під час зимового піку споживання могла мати набагато гірші наслідки для

основної мережі. Залежність Фінляндії від імпорту з сусідніх країн, які можуть постраждати від подібних небезпек від холодного морозу до зимового шторму, створює ще один серйозний ризик у разі кількох несправностей, що стосуються скандинавських країн одночасно. Нарешті, взаємозалежність з іншими критично важливими секторами, зокрема з мережами ІКТ, є ключовим питанням, над яким слід поміркувати, оскільки операції з електромережами рухаються до підвищення рівня автоматизації та цифровізації (Pantelli and Mancarella, 2017). Це може створити нові місця вразливості до кібератак, до яких як влада, так і оператори повинні серйозно поставитися,

Управління стійкістю передачі та розподілу електроенергії

Фінляндія має добре налагоджену політику критичної інфраструктури

У цьому динамічному середовищі ризиків, де взаємозалежність і взаємозв'язок систем створюють потенціал для згубних наслідків збоїв, Фінляндія протягом десятиліття була піонером стійкості критичної інфраструктури у своїй політиці управління ризиками.З амбітною метою стати найбезпечнішою країною в Європі стратегічна структура Фінляндії щодо управління ризиками добре узгоджується з Рекомендаціями ОЕСР щодо управління критичними ризиками (OECD, 2014). Національна оцінка ризиків підтримує загальнодержавну стратегію безпеки суспільства, яка з 2010 року ставить життєво важливі функції для суспільства в основу. З акцентом на стійкість потоку послуг, життєво важливих для функціонування суспільства та уряду, ця стратегія ввійшла в основу Постанова Уряду 2013 року «Про забезпечення цілей безпеки». Цей політичний документ, вперше прийнятий у 1988 році та переглядаючийся приблизно кожні 5-7 років з того часу, визначає наступні цілі стійкості: безперервність економічної діяльності та функціонування критичної інфраструктури у разі серйозних збоїв і надзвичайних ситуацій.

Стратегічний підхід Фінляндії покладає лідерство на галузеві міністерства щодо стійкості критичної інфраструктури та наголошує на структурі співпраці, що використовує державно-приватну співпрацю.Стратегія безпеки постачання гармонізує національні принципи готовності між адміністративними гілками, окреслюючи чіткі ролі та обов'язки в усьому уряді, у тому числі на місцевому рівні (Міністерство зайнятості та економіки, 2013). Висвітлюючи принципи співпраці з приватним сектором і координації з міжнародними партнерами, ця комплексна стратегія підкреслює важливість партнерства та добре функціонуючих ринків і правил для стійкості критичної інфраструктури.

Для підтримки впровадження політики стійкості критичної інфраструктури Національна організація аварійного постачання (NESO) є наріжним каменем для державного та приватного співробітництва, що дозволяє побудувати спільне бачення критичних ризиків і стійкості.NESO об'єднує галузь і уряд у галузевих групах, щоб виробити спільне розуміння критичних ризиків і вразливості інфраструктури та обговорити практичні заходи готовності та планування безперервності бізнесу. Національне агентство з надзвичайних ситуацій (NESA) при Міністерстві економіки та зайнятості має завдання проводити аналіз ризиків, координувати обмін інформацією, сприяти співробітництву між державним та приватним секторами та впроваджувати політику безпеки постачання в критичних секторах. З більш ніж тисячею компаній, задіяних у системі пулінгу (рис. 4.1), NESO вважається добре функціонуючий механізм управління стійкістю критичної інфраструктури зацікавленими сторонами.

Малюнок 4.1. Система об'єднання NESA: державно-приватна модель співпраці

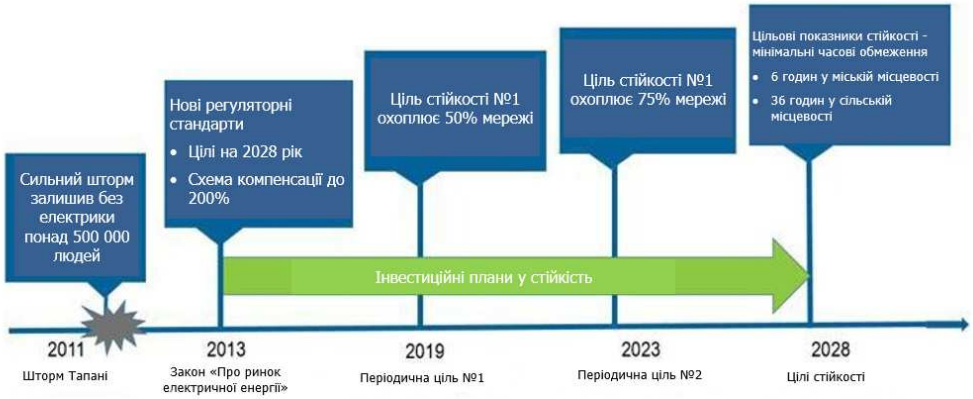
Регулювання ринку електроенергії також є ключовим інструментом, який використовується у Фінляндії для підвищення стійкості

Регулювання ринку електроенергії у Фінляндії протягом тривалого часу приділяло пильну увагу стійкості мереж передачі та розподілу.Як і в більшості країн, енергетичний сектор у Фінляндії має довгу історію регулювання для забезпечення якості та надійності послуг, що містить стандарти безпеки та заходи для підтримки прийнятних цін для клієнтів. Закон про ринок електроенергії 2003 року встановив нормативну базу для енергетичного сектору та встановив ліміти часу відключень із змінними штрафами у вигляді компенсацій споживачам відповідно до попередньо встановленого часу відключень понад 12 годин збою (Міністерство економіки та зайнятості, 2013). . Цей масштабований підхід був досить інноваційним на той час і добре доповнював інші цінові стимули для дистриб'юторських компаній для підвищення стійкості своїх мереж на основі рівня надійності та якості.

Цього складного підходу виявилося недостатньо, щоб уникнути масштабних перебоїв з електропостачанням під час штормів 2010 та 2011 років, що змусило Міністерство економіки та зайнятості переглянути правила та посилити стимули для інвестицій у стійкість. Редакція Закону про ринок електроенергії 2013 року відкоригувала вищезазначену схему, встановивши вищі компенсації, які оператори розподілу виплачують своїм споживачам у разі тривалого відключення. Ці компенсації тепер можуть сягати до 200% річної середньої плати за електроенергію - максимум до 2000 євро - якщо збій перевищує 12 днів, порівняно з попередньою 100% компенсацією понад 5 днів відключення. Хоча це положення стосується всіх збоїв, переглянутий Закон також встановлює обов'язкові показники стійкості до небезпечних погодних умов, яких оператори повинні виконати до кінця 2028 року. Він визначає, що найдовший прийнятний час перерви становитиме 6 годин у міських районах і 36 годин у сільській місцевості. Як галузевий регулюючий орган, Управління енергетики оцінює відповідність DSO проміжним цілям, передбаченим у затверджених інвестиційних планах, які вони повинні подавати кожні два роки (Рисунок 4.2). Регулювання ґрунтується на механізмі стимулювання, включаючи стимулювання якості та безпеки постачання. Перший заохочує DSO досягати вищого за мінімальний рівень надійності постачання за рахунок витрат на відключення, а другий – відповідати нормативним критеріям із застосуванням економічно ефективних заходів, і Він уточнює, що найдовший допустимий час перерви становитиме 6 годин у містах і 36 годин у сільській місцевості. Як галузевий регулюючий орган, Управління енергетики оцінює відповідність DSO проміжним цілям, передбаченим у затверджених інвестиційних планах, які вони повинні подавати кожні два роки (Рисунок 4.2). Регулювання ґрунтується на механізмі стимулювання, включаючи стимулювання якості та безпеки постачання. Перший заохочує DSO досягати вищого за мінімальний рівень надійності постачання за рахунок витрат на відключення,

а другий – відповідати нормативним критеріям із застосуванням економічно ефективних заходів, і Він уточнює, що найдовший допустимий час перерви становитиме 6 годин у містах і 36 годин у сільській місцевості. Як галузевий регулюючий орган, Управління енергетики оцінює відповідність DSO проміжним цілям, передбаченим у затверджених інвестиційних планах, які вони повинні подавати кожні два роки (Рисунок 4.2). Регулювання ґрунтується на механізмі стимулювання, включаючи стимулювання якості та безпеки постачання. Перший заохочує DSO досягати вищого за мінімальний рівень надійності постачання за рахунок витрат на відключення, а другий – відповідати нормативним критеріям із застосуванням економічно ефективних заходів, і Регулювання ґрунтується на механізмі стимулювання, включаючи стимулювання якості та безпеки постачання. Перший заохочує DSO продовжувати регулярні інвестиції в технічне обслуговування та на випадок непередбачених обставин. Крім того, Закон 2013 року робить плани забезпечення безперервності діяльності обов'язковими для операторів. Ухвалення нового законодавства вимагало, щоб усі DSO повторно подали заявку на отримання ліцензії на діяльність у 2013 році, і тепер ці комунальні підприємства мають чіткий план дій для збільшення інвестицій у стійкість та посилення своїх зусиль щодо готовності.

Малюнок 4.2. Проміжні цілі щодо досягнення цілей стійкості до 2018 року



Система галузевих об'єднань та асоціацій, координована NESA, була ключовою для зміцнення довіри між зацікавленими сторонами в електроенергетиці та досягнення консенсусу щодо цих цілей стійкості

Управлінський підхід до посилення стійкості енергетичної мережі у Фінляндії наголошує на добровільній основі та співпраці між промисловістю та галузевими державними органами.Пул електропостачання та централізованого теплопостачання має спеціальну підгрупу з передачі та розподілу електроенергії, яка об'єднує всіх учасників галузі, органи влади та регулятора на добровільній основі для обміну інформацією, підвищення готовності та участі в розробці політики. На чолі з галуззю – TSO Fingrid є його головою – пул є незалежним у визначенні своїх членів, а його завдання визначені в контракті, підписаному з NESA. Існують сильні стимули для операторів брати участь у системі об'єднання завдяки широкому спектру переваг від інформаційних ресурсів, обміну передовим досвідом та участі в тренінгах. NESA забезпечує необхідну інфраструктуру для обміну інформацією та підтримує діяльність пулу.

Регулярні зустрічі та інституціоналізований діалог в рамках Пулу електроенергетики та централізованого теплопостачання дозволили виробити спільне бачення ризиків і цілей стійкості між державним і приватним секторами та зробили значний внесок у розробку переглянутого законодавства. Оператори та уряд погоджуються щодо важливості надійного електропостачання та забезпечення безперервності послуг, однак їхні погляди на рівні стійкості, які мають бути цільовими, і способи їх досягнення можуть відрізнятися. Система об'єднання забезпечує шлях до досягнення консенсусу щодо політики та цілей стійкості шляхом залучення промисловості до галузевих органів влади. Ця взаємодія виявилася важливою під час оновлення регуляторних стандартів у Законі про ринок електроенергії в 2013 році. Оператори

розподілу систем у Фінляндії відрізняються за розміром, можливостями та ресурсами, а об'єднуючи їх разом, як пул успішно досяг, допоміг стимулювати відкриті дискусії щодо того, як підвищити стійкість мереж. Велика участь у пулі демонструє його успіх у розвитку довіри між зацікавленими сторонами, які беруть участь, що відіграє ключову роль у досягненні спільних цілей. Це також допомагає уникнути потенційного ризику вільних поїздок, оскільки оператори можуть відчувати тиск з боку колег через участь у регулярних обговореннях. Відповідно до пулу оскільки оператори можуть відчувати тиск з боку колег через участь у регулярних обговореннях. Відповідно до пулу оскільки оператори можуть відчувати тиск з боку колег через участь у регулярних обговореннях. Відповідно до пулу учасники, його обговорення після шторму 2011 року були основоположними для розробки нового регулювання стійкості таким чином, щоб він узгоджувався з інвестиційними можливостями операторів, терміном служби інфраструктурних активів і середньою прибутковістю, а також іншими пріоритетами політики, пов'язаними з ефективністю , інновації та зміна клімату.

Заходи стійкості та їх впровадження

Оцінка ризиків і обмін інформацією між взаємозалежною критичною інфраструктурою

У той час як уряд Фінляндії проводить оцінку ризиків і прогнозний аналіз майбутніх загроз, немає детального відображення взаємозалежності.Уряд використовує кілька інструментів для підвищення обізнаності всього суспільства про ризики, що надає операторам електроенергії корисну інформацію, щоб передбачити основні загрози порушення роботи їхніх мереж. Фінська національна оцінка ризиків – це міжурядовий інструмент, який дозволяє кожні 3 роки визначати найбільш критичні ризики, з якими може зіткнутися країна, їхню ймовірність і потенційний вплив (вставка 4.2). Застосовуючи перспективний підхід, NESA розробило сценарії безпеки постачання до 2030 року, в якому представлено п'ять сценаріїв на майбутнє та їх вплив на безпеку постачання (NESA, 2018). Окрім підвищення обізнаності операторів та передбачення потенційних каскадних ефектів у цих наборах сценаріїв, картографування взаємозалежностей та оцінки критичності в секторах критичної інфраструктури ще не проводяться на національному рівні.

Оператори несуть відповідальність за проведення оцінки критичності своєї мережі, але єдиного підходу немає.Щоб відповідати нормам, оператори мають стимул проводити власну оцінку ризиків, щоб визначити пріоритетність заходів стійкості та розробити плани безперервності бізнесу.

Найбільші оператори запровадили передові методи моделювання ризиків у партнерстві з університетами, що дозволяє їм оцінювати вплив різних ризиків на свою мережу ймовірнісним методом, наприклад, для штормів або повеней. Міжнародні стандарти управління активами, такі як ISO 55 000, використовуються іншими для визначення критичних точок у мережі. Незважаючи на те, що NESA розробило керівні принципи для підтримки операторів у їх оцінці критичності, не існує єдиного підходу для визначення найбільш критичних точок, де збій може призвести до найбільших каскадних наслідків, у тому числі в інших секторах критичної інфраструктури.

Обмін інформацією в рамках Пулу електроенергії та централізованого теплопостачання надає операторам можливість дізнатися про найкращі підходи до оцінки ризиків у захищеному середовищі, але міжгалузевий обмін залишається обмеженим для аналізу взаємозалежності.Оцінку ризиків можна посилити за допомогою платформ обміну інформацією для обміну методами та технічним досвідом між операторами. Онлайн-платформа пулу сприяє простоті та безпеці обміну інформацією. Компанії можуть отримати доступ до цієї платформи онлайн-комунікації, тоді як NESA підтримує портал і гарантує, що добровільно надана інформація не поширюватиметься за межами безпечних кіл. Гарантія безпеки є важливим

фактором для заохочення обміну високоякісною інформацією та підтримки довіри до системи об'єднання. Інакше існує ризик того, що поширена інформація розкриє комерційну таємницю або потрапить до рук зловмисних зовнішніх організацій. Таким чином, учасники пулу повинні підписувати угоди про конфіденційність для доступу до платформи, а компанії, які хочуть, щоб інформація залишалася конфіденційною, можуть повідомити NESA про конфіденційність. Міжсекторальний обмін інформацією заохочується, але якість інформації, як правило, знижується між пулами. Буде важливо сприяти більш широкому діалогу між пулами для покращення розуміння та аналізу взаємозалежностей, особливо з огляду на критичність енергетичного сектора для всіх інших критично важливих інфраструктурних послуг, а також зростаючу перехресну залежність з IT-сектором.

Вставка 4.2. Національні процеси оцінки ризиків у Фінляндії

Фінська національна оцінка ризиків була вперше проведена в 2015 році Міністерством внутрішніх справ разом із міжсекторальною робочою групою. Національна оцінка ризиків визначає найважливіші ризики, що загрожують людям, навколишньому середовищу, власності та критичним системам і службам, до яких влада має бути готовою. На основі оцінки понад 60 сценаріїв ризику, що стосуються всіх небезпек і загроз, було обрано 21 можливу подію, визначену як широкомасштабні події, що впливають на суспільство, або як серйозні регіональні події. Надається інформація про їхній потенційний вплив, ймовірність і заходи, вжиті для усунення цих загроз. Варто зазначити, що в шести широкомасштабних подіях, які були оцінені, три сценарії пов'язані з електропостачанням: серйозне порушення енергопостачання, використання кібердомену для паралізування життєво важливих для суспільства систем, і ризик сонячної бурі. Подібним чином, серед оцінених серйозних регіональних подій, широкомасштабний зимовий шторм має найвищу ймовірність і найбільший вплив, а сценарій кількох одночасних великих лісових пожеж також розглядає перебої з електроенергією як потенційний вплив.

Фінські сценарії безпеки постачання до 2030 року були розроблені NESA як прогнозний підхід до майбутніх викликів. Його глобальні п'ять сценаріїв – Глобальна взаємозалежність, Політика збройної сили, Блокування та гібридний вплив, Технологічний світоустрій і Домінування Сходу – пропонують можливі шляхи розвитку на майбутнє з урахуванням геополітичних, економічних, демографічних і технологічних тенденцій. У документі детально описано, як ці сценарії можуть вплинути на безпеку постачання, і запропоновано вісім напрямків дій для обох галузей і NESO, щоб підготуватися до майбутніх викликів. Це, зокрема, прийняття системного підходу до безпеки постачання, уважність до підвищених ризиків кіберзагроз і гібридного впливу, а також підготовка до виснаження природних ресурсів.

Джерело: (Міністерство внутрішніх справ, 2016) (NESA, 2018)

Зважаючи на специфіку кіберризиків і швидкі темпи змін у цій сфері, пул створив спеціальну підгрупу для регулярного обговорення та системи раннього попередження при виявленні загроз.Останніми роками кіберзагрози привернули більше уваги, і вони продемонстрували, як вони потенційно можуть вплинути на системи передачі та розподілу

електроенергії. У той час як багато операторів електроенергетики проводять спеціальний аналіз ризиків і посилюють свої внутрішні заходи стійкості, співпраця може допомогти визначити найбільш відповідні методи в цьому швидко мінливому середовищі. Пул створив спеціальний форум з питань кібербезпеки з конкретними контактними особами в компаніях для обговорення оцінки, запобігання та поінформованості про ситуацію з інцидентами кібербезпеки, що впливають на передачу та розподіл електроенергії. У партнерстві з Агентством кібербезпеки та Управлінням енергетики, до якого оператори зобов'язані повідомляти про кіберінциденти, Розробляється важливий інвестиційний план для підвищення надійності електричної мережі, щоб відповідати новим нормам.

Щоб досягти цільових показників стійкості до 2028 року, DSO мають право самостійно вибирати підхід, якому вони віддають перевагу.Кожні два роки вони зобов'язані подавати інвестиційний план до Управління енергетики, демонструючи прогрес, досягнутий у досягненні проміжних цілей. За оцінками, загальні інвестиції для всіх DSO становлять 9,5 мільярдів євро, з яких 30% припадає на додатковий рівень стійкості, якого вимагає переглянутий регламент. Решта вкладень звичайна оновлення застарілої інфраструктури та витрати на технічне обслуговування. Наприклад, найбільший оператор Caruna інвестував 1,2 мільярда євро після штормів 2011 року в стійкість і оновлення мережі та планує інвестувати ще 1 мільярд до 2028 року. Ще один приклад – Хелен Сехкеверкко, оператор столичної зони Гельсінкі, для якої стійкість є пріоритетом. протягом тривалого часу, і хто каже, що нові правила не мали великого впливу на їхні інвестиції. Це можна пояснити тим фактом, що екстремальні шторми мало впливають на його переважно міську мережу. Пріоритетом тут є ризики повеней, для яких існує довгостроковий міський стратегічний план повеней, згідно з яким підстанції мають бути підняті під час оновлення (місто Гельсінкі, 2013).

Заходи для підвищення стійкості енергетичної мережі різноманітні, але більшість DSO обирають найпростіший, але дорогий варіант підземної кабельної розводки, особливо в приміських районах. Оператори можуть підвищити стійкість своєї мережі, зміцнивши надійність конструкції, як-от підземні кабелі, розширивши автоматизацію мережі та створивши більше резервування за допомогою кругових з'єднань (Pantelli and Mancarella, 2017). Багато DSO обирають підземну кабельну розводку ліній середньої та низької напруги. Підземна прокладка кабелю коштує дорого, але швидко підвищує стійкість мережі до збоїв, пов'язаних із погодними умовами. Мета на 2028 рік – забезпечити підземне розміщення 47% ліній середньої напруги. Оператори DSO можуть встановлювати власні цілі для своїх мереж – за оцінками, компанії, які працюють у сільській місцевості, переносять лише 15-20% мережі під землю та можуть обрати інші заходи. Інші економічно ефективні варіанти включають переміщення кабельних шляхів від лісів до відкритих доріг, або збільшення відстані між деревами та кабельними лініями шляхом вирубки деяких частин лісу (Рисунок 4.3). Це особливо важливо в сільській місцевості, де повітряні лінії розташовані у місцях, до яких важко дістатися та швидко відремонтувати їх. Інші більш дорогі варіанти включають будівництво більшої кількості підстанцій для збільшення резервування та зменшення масштабу збоїв. Для сільської місцевості, де мережі здебільшого радіальні, це може бути заходом для підвищення стійкості. Однак DSO можуть не мати достатніх ресурсів для їх реалізації. Хоча загальна перевага підземних кабелів відображає ринковий вибір, значні інвестиції, яких вони потребують, призвели до збільшення витрат для клієнтів (див. нижче). Масштабований підхід, що поєднує різний набір заходів, міг бути прийнятнішим. Це особливо важливо в сільській місцевості, де повітряні лінії розташовані у місцях, до яких важко дістатися та швидко відремонтувати їх. Інші більш дорогі варіанти включають будівництво більшої кількості підстанцій для збільшення резервування та зменшення масштабу збоїв. Для сільської місцевості, де мережі здебільшого радіальні, це може бути заходом для підвищення стійкості. Однак DSO можуть не мати достатніх ресурсів для їх реалізації. Хоча загальна перевага підземних кабелів відображає ринковий вибір, значні інвестиції, яких вони потребують, призвели до збільшення витрат для клієнтів (див. нижче). Масштабований підхід, що поєднує різний набір заходів, міг бути прийнятнішим. Це особливо важливо в сільській місцевості, де повітряні лінії розташовані у місцях, до яких важко дістатися

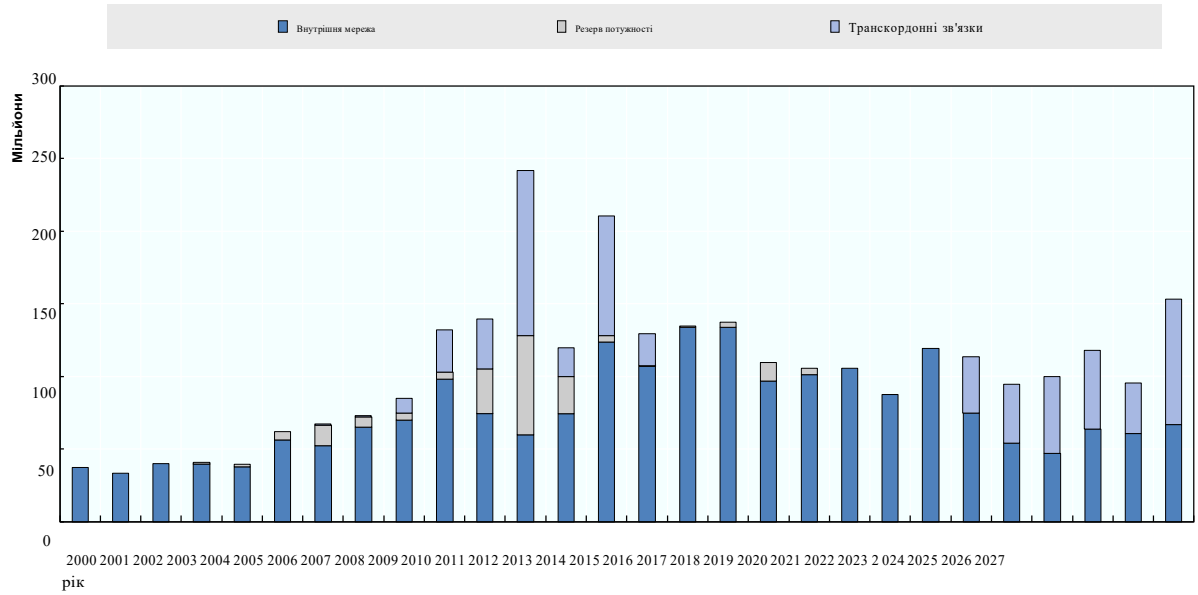
та швидко відремонтувати їх. Інші більш дорогі варіанти включають будівництво більшої кількості підстанцій для збільшення резервування та зменшення масштабу збоїв. Для сільської місцевості, де мережі здебільшого радіальні, це може бути заходом для підвищення стійкості. Однак DSO можуть не мати достатніх ресурсів для їх реалізації. Хоча загальна перевага підземних кабелів відображає ринковий вибір, значні інвестиції, яких вони потребують, призвели до збільшення витрат для клієнтів (див. нижче). Масштабований підхід, що поєднує різний набір заходів, міг бути прийнятнішим. Інші більш дорогі варіанти включають будівництво більшої кількості підстанцій для збільшення резервування та зменшення масштабу збоїв. Для сільської місцевості, де мережі здебільшого радіальні, це може бути заходом для підвищення стійкості. Однак DSO можуть не мати достатнього фінансування на такі дії.

Крім того, у фінську систему передачі та розподілу електроенергії здійснюються інші інвестиції в підвищення стійкості, в тому числі оператор передачі Fingrid для основної мережі, а також у кібервідмовостійкість.Відповідно до Закону про енергетичний ринок, Fingrid також подає свій інвестиційний план до Управління з енергетики. Відповідно до свого інвестиційного плану на

2017-2027 роки, Fingrid інвестуватиме в середньому 100 мільйонів євро на рік протягом наступного десятиліття, щоб підтримувати рівень стійкості та низькі витрати на передачу. Це незначне зниження порівняно з попереднім інвестиційним періодом, протягом якого з'єднання зі Швецією та Естонією значно збільшили фінансові потреби (Рисунок 4.4). Ці інвестиції будуть розподілені майже порівну між заміною існуючої інфраструктури та новими підстанціями та лініями електропередачі, в тому числі для міжнародних зв'язків із сусідніми північними країнами. DSO та Fingrid також впроваджують заходи стійкості для підвищення кібербезпеки, такі як посилення брандмауерів, заходи з підвищення обізнаності персоналу та створення груп реагування на кібербезпеку.

Малюнок 4.3. Заходи стійкості в електричній мережі

Малюнок 4.4. Рівень інвестицій Fingrid у 2000–2027 роках у мільйонах євро



Джерело: (Fingrid, ND)

Підтримка NESA у плануванні безперервності бізнесу та організації спільних навчань, тренінгів і вивчення уроків високо цінується операторами електроенергії для посилення їх стійкості.

Новий розподіл ролей між NESA та регулюючим органом щодо затвердження планів безперервної роботи операторів забезпечує ясність щодо їхніх відповідних ролей.Минулого року було прийнято рішення про те, що ці плани тепер будуть подані на затвердження до Управління з питань енергетики, а NESA та пул продовжуватимуть керувати прогресом і вдосконаленням цих планів.

Такий розподіл ролей між добровільним залученням і підтримкою з боку NESA та пулу з одного боку та наглядом за виконанням обов'язкових вимог з боку регулятора з іншого боку виглядає як ефективна модель управління для підтримки стійкості в секторі передачі та розподілу електроенергії. У майбутньому публічне оприлюднення деяких результатів порівняльного тесту може стати ще одним стимулом для операторів до подальшого вдосконалення своєї готовності.

Що стосується TSO Fingrid, то його надійний план забезпечення безперервності діяльності базується на меті відновити свою мережу протягом 24 годин після знеструмлення відповідно до мережевого кодексу ЄС щодо аварійних ситуацій та відновлення.Він включає заходи щодо готовності та швидкого відновлення у випадку великих аварій, таких як національне відключення електроенергії, втрата однієї диспетчерської та повна втрата ІКТ. План дозволяє Fingrid відключити великих споживачів у разі серйозних збоїв, а також діють спеціальні домовленості з операторами систем розподілу електроенергії щодо нормування електроенергії на основі квот.

Навчання, організовані NESA, допомагають операторам перевірити свої плани безперервності бізнесу та надають хороші можливості для вивчення уроків у пулі, особливо ті, що проводяться в реальних умовах.Тренування та тренування з реагування на надзвичайні ситуації можуть допомогти виявити слабкі місця та визначити пріоритетність покращень.

NESA співпрацює з пулами для регулярної координації спільних навчань і тренувань, як настільних, так і в реальних умовах. Короткий перелік нещодавно проведених навчань у Вставці 4.3 демонструє як високий попит на ці навчання, так і відкритість операторів для підготовки до збоїв, у тому числі з населенням. Додатковий обмін уроками, отриманими з реальних інцидентів, між операторами сприяє підвищенню стійкості та відображає сильну культуру прозорості серед учасників системи пулу.

Вставка 4.3. Навчання щодо безпеки постачання електроенергії, нещодавно проведені NESA і порушення розподілу

Настільні вправи включали, наприклад, відключення електроенергії в одному місті з метою збалансування виробництва та споживання. Ще одне навчання, проведене у 2017 році, полягало в тому, щоб протягом двох тижнів перевірити, як влада відреагує у разі перебоїв з електроенергією, з акцентом на методи та канали зв'язку. У 2019 році подібні навчання будуть проведені на регіональному рівні. У 2014 році в Лапландії було проведено навчання з реальними умовами, коли в одному місті було організовано відключення електроенергії на одну годину, в результаті чого було зроблено висновок, що відновлення електропостачання в країні може зайняти день. У Гельсінкі незабаром будуть проведені навчання з відключення електроенергії від півгодини до кількох годин у значній частині міста.

Джерело: Інтерв'ю проведено OECD, 2018

Транскордонне співробітництво з країнами Північної Європи та Європою є основними елементами підходу Фінляндії до безпеки постачання в електроенергетиці.

NESA та Fingrid беруть участь у двосторонньому та багатосторонньому співробітництві для підтримки стійкості електроенергетичної системи Фінляндії через її значну залежність від імпорту електроенергії взимку та через необхідність співпраці у разі транскордонної кризи. Північне співробітництво з планування на випадок надзвичайних ситуацій та управління кризовими ситуаціями в енергетичному секторі (NordBER) забезпечує основу для готовності до збоїв у електропостачанні в Данії, Фінляндії, Ісландії,

Норвегії та Швеції (NordBER, 2015). NordBER сприяє регулярним зустрічам між TSO та відповідними національними органами влади, відповідальними за питання передачі та розподілу електроенергії в надзвичайних ситуаціях і готовності до обміну інформацією, регіональних навчань і координації політики. Структура NordBER дозволила створити механізм транскордонної координації випадок великомасштабного дефіциту енергії, що впливає на одного з його членів. Fingrid є частиною оптового ринку електроенергії Nord Pool і бере участь у співтоваристві TSO із сусідніми країнами щодо балансування потужностей. Компанія також працює зі своїми сусідами над посиленням транскордонних взаємозв'язків. Фінські та шведські оператори ГТС вирішили продовжити впровадження третього з'єднання змінного струму з метою ввести його в експлуатацію до кінця 2025 року. Розглядається заміна інтерконектора Fenno-Skan 1 між Швецією та Фінляндією. інвестиція наприкінці 2020-х років.

Ефективність управління для стійкості та виклики на майбутнє

Переглянута модель управління стійкістю електропостачання у Фінляндії демонструє чудові результати в перші роки впровадження

Модель управління Фінляндії для стійкості її системи передачі та розподілу електроенергії поєднує потужність сильної нормативної бази та добре налагоджену модель співпраці між державним і приватним секторами для досягнення амбітних цілей стійкості.Закон про ринок електроенергії 2013 року, система об'єднання та підтримка NESA надають комплексний набір стимулів для операторів електроенергії інвестувати в стійкість. Чітке визначення ролей між регулюючим органом і NESA демонструє узгодженість цього підходу батога і пряника для сприяння стійкості: з одного боку, Управління з питань енергетики контролює дотримання правил стійкості, а з іншого боку NESA сприяє добровільному залученню операторів до стійкості дій за допомогою серії інструментів обміну інформацією, настанов і експертної оцінки. Це виглядає як хороша політична відповідь на масштабні збої, спричинені штормом Тапані в 2011 році, а також як адаптація до динамічного ландшафту ризиків, позначеного посиленням взаємозалежностей, зміною клімату та зростанням занепокоєння щодо кібер- та гібридних загроз.

Поточна реалізація цієї політики стійкості свідчить про велику залученість різних операторів, які, здається, дотримуються як її цілей, так і підходу.Система пулу функціонує добре та дозволяє безпечно обмінюватися інформацією, а також спільно створювати політики та інструменти впровадження. Керівництво та інструменти NESA використовуються операторами, які значною мірою беруть участь у його діяльності. Оператори інвестують у надійність своєї мережі згідно з положенням, яке добре розроблено для сприяння цим інвестиціям: деякі оператори підрахували, що рівень компенсації, яку вони, можливо, повинні будуть виплатити клієнтам, може сягнути однієї чверті їхнього обороту в разі шторму. схожий на Тапані. Крім того, нова політика створила імпульс для інвестицій у стійкість, спрямованих на інші ризики, такі як кібернетичні.

Оскільки цей підхід починає мати фінансові наслідки для клієнтів, збалансування суспільних очікувань щодо стійкості та підвищення ціни вимагатиме ретельного моніторингу економічної ефективності інвестицій у стійкість.

Інвестиції в стійкість починають мати фінансові наслідки для клієнтів, які потрібно буде ретельно контролювати, щоб забезпечити постійне схвалення громадськістю цієї амбітної політики безпеки країни.Що стосується компенсації, нова схема була вперше активована під час зимового шторму в січні 2018 року, який залишив 40 000 людей без електрики на півночі Фінляндії - деякі до тижня. У результаті 10 000 клієнтів отримали компенсацію на загальну суму до 5 мільйонів євро. З іншого боку, інвестиції, зроблені в надійність, призвели до того, що DSO паралельно покращили якість своїх послуг, що, згідно з положенням, дозволило їм підвищити ціни на розподіл. У своєму щорічному звіті за 2017 рік Управління з питань енергетики вказало, що для побутових споживачів ціни на розподіл електроенергії зросли в середньому на 5,4% порівняно з попереднім роком (Energy Authority, 2017). У деяких випадках підвищення сягало 30%. Сильна громадська та політична реакція призвела до внесення змін до Закону про ринок електроенергії, щоб обмежити річне підвищення ціни на 15%, що може створити проблеми з грошовими потоками для деяких операторів. Хоча витрати на передачу залишаються низькими за європейськими стандартами, за останні 10 років зросли вдвічі.

Це демонструє важливість ретельного розгляду очікувань громадськості та їх зміни з часом під час розробки інструментів політики стійкості, а також ведення тісного діалогу з операторами щодо найбільш доступних способів підвищення стійкості.Повинен бути

оптимальний баланс між витратами, інвестиціями та надійністю послуг, щоб забезпечити як очікування суспільства щодо надійності електроенергії, так і те, що збільшення вартості залишається прийнятним. Після штормів 2010 і 2011 років суспільство висловило високий попит на підвищення рівня надійності. Політики відповіли амбітними цілями, встановленими в переглянутому Законі про ринок електроенергії, які оператори виконали, інвестуючи в стійкість. Оскільки пам'ять про цю катастрофу поступово зникає, зникає і готовність платити. Хоча важливо підтримувати стабільне нормативне середовище в цьому секторі, де потрібні довгострокові інвестиції, може бути спосіб обговорити з операторами економічну ефективність заходів стійкості, які вони вживають. Додаткові рішення для підземних кабелів можуть бути дешевшими.

Відмінності між ресурсами та потужностями операторів транспортування мають наслідки для того, як вони впроваджують заходи стійкості по всій країні та її загальну стійкість

Велике розмаїття серед 77 DSO, що працюють у Фінляндії, означає, що вони мають різні можливості та ресурси для досягнення цілей стійкості до 2028 року.Найбільші оператори часто охоплюють густонаселені міські райони. Вони мобілізували значні ресурси для інвестування в стійкість і перебувають на хорошому шляху до досягнення цілей. З іншого боку, найменші оператори в сільській місцевості та віддалених частинах країни стикаються з фінансовими обмеженнями та технічними труднощами. Великі оператори, зокрема з приватним пакетом акцій, максимізують свою прибутковість у рамках нової нормативної бази. Це пояснює, чому підземна кабельна розводка в найбільш густонаселеній частині країни досі була найпоширенішим варіантом і добре відповідає пріоритету, встановленому для найбільш критичних точок мережі. Тим не менш, існує занепокоєння щодо зростаючих відмінностей щодо стійкості розподільчих мереж на території Фінляндії. У віддалених районах можливі відключення електроенергії створюють значний вплив на популяцію з тривалим часом відновлення, що може поставити під сумнів загальні переваги нового регулювання. З іншого боку, невеликі DSO отримують повну вигоду від обміну передовою практикою від своїх колег у системі пулу, щоб покращити свою обізнаність і структурувати свої плани безперервності бізнесу, включно з кіберризиками.

У майбутньому підготовка до майбутніх оновлень моделі управління може відобразити шляхи підтримки стійкості невеликих операторів систем передачі даних.Окрім підземної прокладки кабелю, доступні й інші економічно ефективні варіанти, такі як встановлення більшої кількості резервів, видалення дерев з ліній або інші інноваційні рішення. У цьому випадку можна розглянути варіанти співфінансування, щоб доповнити ринкові рішення, як спосіб гарантувати, що всі DSO мають можливість досягти цільових показників стійкості.

Розраховане на майбутнє енергопостачання у Фінляндії вимагатиме більше спільних дій із взаємозалежними секторами, а також подальшого об'єднання програм політики щодо інновацій, клімату та стійкості.

Прагнення NESA до системного підходу до управління стійкістю критичної інфраструктури ще не матеріалізується в міжгалузевій співпраці, яка особливо важлива між секторами електроенергетики та ІКТ.Як зазначено в сценарії безпеки постачання NESA 2030, сектор електроенергетики зараз переживає трансформаційні зміни, які вплинуть на безпеку постачання (NESA, 2018).

Взаємна взаємозалежність між передачею та розподілом електроенергії та сектором ІКТ швидко зростає завдяки розгортанню систем автоматизованого керування та

інтелектуальних мереж операторами систем передачі електроенергії та операторами систем передачі електроенергії. Однак вимоги до безперервності відрізняються між двома секторами, строки інвестицій і доходи не узгоджуються, а обмін інформацією між відповідними пулами не є оптимальним. Карту взаємозалежності можна покращити, щоб спільно посилити стійкість цих секторів до загальних ризиків, від відключень телекомунікацій чи електроенергії до кібератак. У світлі збоїв, які виникли після шторму Тапані в 2011 році, Інші трансформаційні зміни в енергетичному секторі, спричинені інноваціями та зміною клімату, створюють можливості для підвищення стійкості, але також можуть поставити під сумнів безпеку поставок і бізнес-моделі операторів.Кліматична стратегія Фінляндії пропонує значне збільшення відновлюваної енергії замість вугільної генерації, а розгортання інтелектуальних систем є центральним у її інноваційній стратегії. З одного боку, ці зміни можуть призвести до збільшення гнучкості та резервних можливостей для збалансування попиту та пропозиції та полегшення роботи мережі. З іншого боку, більш переривчасте виробництво та позамережне місцеве виробництво та розподіл викликають занепокоєння щодо безпеки постачання. Існує ризик того, що віддача від поточних інвестицій у стійкість електромережі може бути нижчою, ніж очікувалося, якщо ці нові потужності не будуть використані за планом. Необхідно, щоб усі зацікавлені сторони в пулі, а також на рівні політики ретельно обміркували, як ці зміни можуть вплинути на бізнес-моделі стійкості операторів систем передачі даних та систем передачі даних.

Вставка 4.4. Рекомендація для Фінляндії

Для посилення стійкості своєї критичної інфраструктури в секторі передачі та розподілу електроенергії Фінляндія могла б розглянути наступний набір рекомендацій:

- Підтримуйте постійний діалог з операторами щодо економічної ефективності заходів стійкості, які вони вживають для сприяння диверсифікації рішень.
- Підвищення обізнаності населення про ризики збоїв у роботі мережі та інформування про прогрес, досягнутий щодо стійкості, щоб полегшити суспільство прийняття зростання витрат.
- Вивчіть варіанти подальшої підтримки невеликих операторів у їхніх зусиллях досягти цілей стійкості.
- Використовуйте кооперативну модель системи об’єднання для посилення аналізу взаємозалежності та спільних дій між секторами електроенергетики та ІКТ.
- Сприяти розробці угод про взаємодопомогу між операторами на добровільній основі.

Список літератури

Asgary, A. та ін. (2017), «Розробка критеріїв взаємної допомоги при катастрофах для електроенергетичної галузі», Запобігання стихійним лихам та управління ними: міжнародний журнал, Вип. 26/2, стор. 230-240, https://www.emeraldinsight.com/doi/pdfplus/10.1108/DPM-05-2016-0107 .

Місто Гельсінкі (2013),Інструкції міста Гельсінкі щодо запобігання та боротьби з повенями: Захист мешканців і майна в районах, що небезпечні для повені в Гельсінкі, https://www.hel.fi/static/helsinki/julkaisut/Tulvaohje_eng_17062013.pdf .

Управління енергетики (2017),Національна доповідь за 2017 рік Агентству з енергетичного співробітництва, Енергія Орган, Фінляндія, https://www.energiavirasto.fi/documents/10191/0/ National_Report_2017_Finland_1469-401-2017.pdf/6b783563-e997-4c4c-ace9-826d68447c9b .

Fingrid (2018),Ризик дефіциту електроенергії у Фінляндії в четвер, 19 липня, https://www.fingrid.fi/en/pages/news/news/2018/risk-of-electricity-shortage-in-finland-on-thursday-19- july/ .

Fingrid (Північна Дакота),Основний план розвитку електромереж на 2017-2027 роки, https://www.fingrid.fi/globalassets/dokumentit/fi/kantaverkko/kantaverkon-kehittaminen/main- griddevelopment-plan-2017-2027.pdf .

Форссен, К. (2016),Стійкість фінських електромереж проти, https://aaltodoc.aalto.fi/bitstream/handle/123456789/19983/master_Forss%E9n_Kim_2016.pdf?sequ ence=1 .

Куфеоглу, С. і М. Лехтонен (2014),Циклон Дагмар 2011 року та його наслідки у Фінляндії, http://dx.doi.org/10.1109/ISGTEurope.2014.7028868 .

Міністерство економіки та зайнятості (2013),Закон про ринок електроенергії 588/2013 [Sähkömarkkinalaki],https://www.finlex.fi/fi/laki/alkup/2013/20130588 (дата доступу: 28 листопада 2018 р.).

Міністерство зайнятості та економіки (2013),Постанова Уряду про безпеку постачання Цілі,https://s3-eu-west-1.amazonaws.com/huoltovarmuuskeskus/app/uploads/ 2016/08/31144502/2013-12-05 Government_decision_on_the_security_of_supply_goals.pdf? AWSAccessKeyId=AKIAITCZY CPQYFESGSAQ&Expires= 1543875271&Signature=M5SLweaiUDfXX0gsE77JXW84EPc%3D .

Міністерство внутрішніх справ (2016),Національна оцінка ризиків 2015,http://dx.doi.org/978-952-324-060-5 .

Міністерство охорони навколишнього середовища (2017),Урядовий звіт щодо середньострокового плану політики щодо зміни клімату до 2030 року: до повсякденного життя з урахуванням клімату, http://julkaisut.valtioneuvosto.fi/handle/10024/80703 .

NESA (2018),Безпека постачання: Сценарії 2030,https://s3-eu-west-1.amazonaws.com/huoltovarmuuskeskus/app/uploads/2018/09/06091431/Eng-Scenarios-2030.pdf? AWSAccessKeyId=AKIAITCZYCPQYFESGSAQ&Expires=1543553617&Signature=G kvOd%2BzJLB1BqTw2oPq gCKqzEQE%3D

NordBER (2015),Дефіцит енергії Скоординоване поводження з потенційними збуреннями в скандинавських країнах система живлення,https://www.energimyndigheten.se/globalassets/trygg-energiforsorjning/el/ energyshortage---coordinated-handling-of-a-potential-disturbance-in-the-nordic-power-system.pdf .

OECP (2014),Рекомендація Ради з управління критичними ризиками, видавництво OECD, http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf .

Bugliarello, G. and C. Arenberg (eds.) (2007),Критична інфраструктура, взаємозалежності та Стійкість, Національна інженерна академія,https://www.nae.edu/File.aspx?id=7405&v=70df971 .

Pantelli, M. and P. Mancarella (2017), «Моделювання та оцінка стійкості критичних електричних Енергетична інфраструктура для екстремальних погодних явищ»,IEE Systems Journal, Вип. 11/3, стор. 1733-1742, https://www.researchgate.net/profile/Mathaios_Panteli/publication/272364268_Modeling_and_Evaluating_the_Resilience_of_Critical_Electrical_Power_Infrastructure_to_Extreme_Weather_Events/links/57356e6408ae9ace8409609a/Modeling -i-Оцінка-стійкості- .

Комітет безпеки (2017),Стратегія безпеки суспільства,https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf .

Закон, Т. (ред.) (2018),Регулювання електроенергетики у Фінляндії,https://uk.practicallaw.thomsonreuters.com/7-629-2923?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 .

5. Інструментарій політики щодо управління стійкістю критичної інфраструктури

У цьому розділі представлено інструментарій політики ОЕСР щодо управління стійкістю критичної інфраструктури, який може надихнути уряди на реформи політики щодо покращення безперервності цих основних послуг. Цей Інструментарій, розроблений у контексті Форуму ризиків високого рівня ОЕСР, забезпечує комплексну політичну основу для посилення стійкості критичної інфраструктури та подолання пов'язаних із цим викликів управління. Інструментарій наголошує на важливості прийняття системного підходу для стійкості критичної інфраструктури на основі партнерства між урядами та операторами критичної інфраструктури.

Контекст для розробки Інструментарію ОЕСР

У цьому розділі представлено Політичний інструментарій ОЕСР щодо управління стійкістю критичної інфраструктури, розроблений Форумом високого рівня ризиків ОЕСР (HLRF). HLRF об'єднує державних службовців для визначення та обміну передовими практиками щодо поглиблення розуміння нових і складних ризиків, а також для обміну передовими практиками в їх управлінні. Він запрошує експертів із приватного сектору, громадянського суспільства, аналітичних центрів та академічних кіл для виявлення прогалин в управлінні ризиками та пошуку рішень для поточних і майбутніх проблем. HLRF використовує інклюзивний підхід до аналізу політики, який відображає запропоновану найкращу практику, як це втілено в Рекомендаціях ОЕСР щодо управління критичними ризиками, прийнятих Радою ОЕСР у 2014 році (OECD, 2014).[1]).

Через високі економічні витрати та соціальну шкоду, яку спричиняють збої в роботі критичної інфраструктури, Рекомендація ОЕСР підкреслює важливість для урядів посилення стійкості та безпеки мереж критичної інфраструктури. У 2016 році ОЕСР провела опитування, щоб оцінити виконання Рекомендації ОЕСР прихильниками. Результати опитування показали, що основною перешкодою для впровадження Рекомендації є розподіл відповідальності між урядами та бізнесом за захист активів критичної інфраструктури та забезпечення швидкого відновлення обслуговування (OECD, 2018).[2]).

Щоб вирішити цю проблему, Форум високого рівня ризиків закликав ОЕСР провести дослідження та розробити звіт про ефективну практику щодо того, як уряди та підприємства можуть структурувати ефективні партнерства для створення більш безпечної та стійкої критичної інфраструктури. На додаток до цього заклику ОЕСР провела міжкраїнове опитування щодо стійкості критичної інфраструктури, організувала тематичні семінари, провела регіональні дослідницькі проекти та пілотні тематичні дослідження в країнах, а також внесла свій внесок у відповідну міждисциплінарну діяльність ОЕСР. Ці заходи допомогли поглибити доказову базу щодо стійкості критичної інфраструктури, представлену в цьому звіті, і розширити мережу політиків ОЕСР, відповідальних за критичну інфраструктуру, а також регуляторів, операторів з державного та приватного секторів і дослідників, які працюють над цією темою.

Процес розпочався зі звіту про підведення підсумків, який обговорювався на Форумі високого рівня ризиків у 2017 році та є основою цього звіту. Форум погодився з ОЕСР організувати спеціальний семінар на тему «Системне мислення для стійкості та безпеки критичної інфраструктури» у партнерстві зі Спільним дослідницьким центром Європейської Комісії (ОЕСР та ЄС JRC, 2018 р.).[41]). Семінар відбувся 23-24 вересня 2018 року з акцентом на інструментах, методологіях і вимогах до даних для оцінки стійкості системи та на інструментах політики, які уряди можуть мобілізувати для стійкості критичної інфраструктури. Учасники запропонували Форуму високого рівня ризиків ОЕСР розробити «Набір політичних інструментів щодо управління стійкістю критичної інфраструктури» на основі обговорень семінару та аналізу ОЕСР.

Проблеми політики для стійкості критичної інфраструктури

Недавні шокові події, спричинені стихійними лихами, промисловими аваріями, кіберзагрозами чи іншими ризиками для безпеки, ілюструють, як збої в ключових системах і основних послугах, таких як водопостачання, енергетика, транспорт або інформаційно-телекомунікаційні системи, можуть призвести до значних економічних збитків у Крім втрати життя в деяких випадках. Взаємозв'язок ланцюгів постачання, технологічних і фінансових систем, які є основою світової економіки, збільшує критичну інфраструктуру та вразливість до

таких непередбачуваних подій, спричиняючи негативний вплив у різних секторах і на кордонах, який часом може мати глобальний резонанс. Цей гіперзв'язок між інфраструктурні активи, сектори та країни вимагає комплексної державної політики для посилення стійкості критичної інфраструктури та обмеження ризику збоїв у основних послугах, які вони надають.

Починаючи з 2000-х років, кілька урядів запровадили державну політику для сприяння захисту критичної інфраструктури та дії для її реалізації. Загалом це включає зусилля щодо визначення секторів критичної інфраструктури, розробку переліку активів критичної інфраструктури та прийняття нормативних актів, національних програм або механізмів стимулювання для посилення стійкості цих активів. Однак політика захисту критичної інфраструктури не завжди виявляється достатньо ефективною для вирішення проблем 21-го вулландшафт ризику століття.

Різноманітність і складність шокових подій, посилення взаємозалежності та взаємозв'язку, зміна клімату, швидкі темпи інновацій, які докорінно трансформують сектори критичної інфраструктури, а також старіння інфраструктури є одними з викликів, з якими доводиться боротися політикам стійкості критичної інфраструктури. Багато дослідників цієї теми приходять до висновку, що зміщення акценту із захисту на стійкість допомогло б політикам краще враховувати невизначеність шляхом інтеграції таких концепцій, як адаптивність, гнучкість і надійність у проект критичної інфраструктури та її нормативно-правової бази.

Після прийняття Рекомендації OECP щодо управління критичними ризиками кілька міжнародних форумів визнали важливість стійкості інфраструктури. Принципи Ісе-Шіми G7 щодо сприяння інвестиціям у якісну інфраструктуру наголошують на стійкості проти стихійних лих, тероризму та ризиків кібератак для забезпечення надійної роботи та економічної ефективності з огляду на вартість життєвого циклу (G7, 2016 р.).[38]). Подібним чином Сендайська рамкова програма ООН щодо зменшення ризику стихійних лих закликає країни «суттєво зменшити шкоду, завдану критичній інфраструктурі внаслідок стихійних лих, і збої в роботі основних послуг» (Управління ООН зі зменшення ризику стихійних лих, 2015 р.[39]).

Рамкова програма OECP щодо управління інфраструктурою також висвітлює стійкість інфраструктури як одну з 10 основних проблем управління (OECD, 2017).[11]).

Сьогодні існує великий попит на практичні політичні вказівки для підвищення стійкості протягом життєвого циклу критичної інфраструктури. Уряди та зацікавлені сторони інфраструктури стикаються з ключовими проблемами управління, коли йдеться про інвестиції в стійкість і розробку відповідної політики. Рекомендації, засновані на фактичних даних, і обмін передовим досвідом між країнами можуть дати корисну інформацію у відповідь на такі складні питання, як:

- *Яка належна роль урядів у підвищенні стійкості критичної інфраструктури?*
- *Як уряди можуть ефективно залучати операторів критичної інфраструктури – державних іприватних – до зміцнення своїх зусиль щодо стійкості?*
- *Які найбільш відповідні механізми для обміну конфіденційною інформацією проризики, вразливі місця та заходи стійкості між урядом і операторами?*
- *Як розподілити витрати та вигоди від інвестицій у стійкість між урядами, операторами такінцевими користувачами?*

Нещодавнє збільшення інвестицій у інфраструктуру в усьому світі, цифровізація та мінливий ландшафт ризиків дають можливість переосмислити політику щодо критичної інфраструктури в країнах OECP та за її межами, а також інтегрувати стійкість у завчасне планування та проекти.

Графа 5.1. Системний підхід до політики критичної інфраструктури

Щоб перейти від стратегії, орієнтованої на захист, до стратегії, яка акцентує увагу на стійкості, політика критичної інфраструктури повинна мати такі якості з точки зору системного мислення:

- **Усі небезпеки та загрози**: Політики щодо однієї небезпеки недостатньо для створення стійкості інфраструктури. Прогнозний підхід до стійкості та безпеки критичної інфраструктури, який орієнтованийна всі небезпеки та загрози, дозволяє розробникам політики та операторам краще підготуватися до несподіванок.
- **Системний рівень**: Інфраструктурні активи зазвичай є лише компонентами ширшої складної системи, яку слід розглядати в повному обсязі в комплексній стратегії стійкості. Системний підхід дозволяє визначити пріоритетність найбільш критичних компонентів і усувати слабкі місця, які створюють критичні вразливості для всієї системи.
- **Міжгалузева координація**: Вирішення взаємозалежностей у політиках вимагає від політиківта операторів вийти за рамки індивідуального підходу та спільно націлитися на сектори критичної інфраструктури. Хоча оператори, як правило, добре усвідомлюють свою власну залежність від критичних секторів, вони можуть не настільки усвідомлювати залежність інших від їхніх власних послуг.
- **Державно-приватне співробітництво**: Хоча уряди продовжують володіти, інвестувати та експлуатувати критичну інфраструктуру в деяких секторах, велика частка критичної інфраструктури знаходиться у приватній власності або під керуванням. Стійкість цих систем залежить від партнерства урядів з операторами інфраструктури з державного та приватного секторів у зусиллях з підвищення стійкості шляхом створення відповідних механізмів управління.
- **Підхід життєвого циклу**: різні заходи стійкості можуть застосовуватися на різних етапах життєвого циклу інфраструктури: надійність і резервування потребують інвестицій на етапі проектування, тоді як планування безперервності бізнесу та обслуговування стосується операцій, а адаптивність може базуватися на модернізації інфраструктури. Таким чином, важливо встановити комплексну політику, яка забезпечує стійкість протягом життєвого циклу інфраструктури.
- **Весь цикл управління ризиками**: комплексна політика стійкості має включати заходи протягом усього циклу управління ризиками, від оцінки ризиків до запобігання ризикам, готовності до надзвичайних ситуацій, реагування, відновлення та реконструкції.
- **Ризик-орієнтований та багаторівневий підхід**: Враховуючи значний ступінь невизначеності щодо майбутніх ризиків, різноманітні виміри вразливості систем інфраструктури та всі взаємозв’язки між цими системами, пріоритетність заходів стійкості є важливою. Багатошаровий підхід, що грунтується на оцінці ризиків, допомагає врахувати складні взаємозалежності, всі небезпеки та життєвий цикл інфраструктури.
- **Транскордонний вимір**: Ризики, що виникають від взаємозалежності і взаємозв'язок не можна повністю пом'якшити без включення їх міжнародного виміру.Сприяння міжнародній співпраці є ключовим фактором стійкості інфраструктури.

Цілі Інструментарію політики

Метою Посібника з управління стійкістю критичної інфраструктури є допомога урядам у розробці національних політик стійкості критичної інфраструктури та впровадження їх через ефективне партнерство з операторами.

У ньому пропонуються практичні рекомендації, підкріплені передовою практикою в країнах та орієнтовними контрольними показниками, які уряди можуть використовувати для:

- *Визначте критичну інфраструктуру, окресліть (взаємо)залежності та визначте пріоритетність критичних послуг і функцій, систем і активів, де інвестиції в стійкість і безпеку найбільше потрібні.*
- *Налагодьте ефективне партнерство з операторами критичної інфраструктури для побудови взаємної довіри, обміну інформацією про ризики та вразливі місця та узгодження спільного бачення та політичних цілей.*
- *Розподіліть відповідальність за захист активів критичної інфраструктури та забезпечення швидкого відновлення роботи.*

Набір політичних інструментів пропонує урядам прийняти системний підхід до стійкості критичної інфраструктури, тобто їхня політика повинна розглядати всі небезпеки та загрози, забезпечувати міжгалузеву координацію та державно-приватну співпрацю, інтегрувати планування для всього життєвого циклу інфраструктури, цільові заходи для всіх цикл управління ризиками та сприяння транскордонному співробітництву (вставка 5.1).

У майбутньому ОЕСР співпрацюватиме з Форумом високого рівня ризиків, щоб підтримувати впровадження країнами цього Посібника з політики та оцінювати їхній прогрес у підвищенні стійкості критичної інфраструктури.

Політичний інструментарій щодо управління стійкістю критичної інфраструктури

визначення

Пропонується використовувати такі визначення:

- ***Критична інфраструктура**: Критична інфраструктура – це системи, активи, об'єкти та мережі, які надають необхідні послуги для функціонування економіки та безпеки та добробуту населення. Хоча визначення критичної інфраструктури відрізняються в різних країнах, це визначення не є обов'язковим і має на меті охопити найбільший набір визначень, визначених в Огляді ОЕСР щодо стійкості критичної інфраструктури.*

- ***Стійкість**: здатність систем поглинати збурення, відновлюватися після збоїв і адаптуватися до мінливих умов, зберігаючи, по суті, ту саму функцію, що й до руйнівного шоку (адаптовано з ОЕСР, 2014 р.).[20]). Це визначення включає здатність протистояти ударам із якомога меншою втратою функціональності законкретних обставин,*

обмеження тривалості потенційного переривання обслуговування шляхом мінімізації часу відновлення, а також адаптацію до нових умов і покращення функціональності систем.

Сім кроків політики стійкості критичної інфраструктури

Щоб підвищити стійкість критичної інфраструктури, всеосяжна політична основа повиннавирішувати наступні сім взаємопов'язаних проблем управління:

1. Створення багатогалузевої структури управління для стійкості критичної інфраструктури
2. Розуміння складних взаємозалежностей і вразливостей у системах інфраструктури для визначення пріоритетів заходів щодо стійкості
3. Встановлення довіри між урядом та операторами шляхом забезпечення обміну інформацією, пов'язаною з ризиком
4. Побудова партнерства для узгодження спільного бачення та досяжних цілейстійкості
5. Визначення комплексу стратегій для визначення пріоритетів економічно ефективних заходів стійкості протягом життєвого циклу
6. Забезпечення підзвітності та моніторинг впровадження політики стійкості критичної інфраструктури
7. Розгляд транскордонного виміру систем інфраструктури

1. Створення багатогалузевої структури управління для стійкості критичної інфраструктури

Уряди повинні прийняти загальнодержавний підхід до стійкості критичної інфраструктури. В ідеалі таке управління мало б включати галузеві міністерства та відомства, які контролюють створення і регулювання інфраструктури в багатьох критичних секторах, а також тих, хто відповідає за стійкість до всіх небезпек і загроз. Координація в Урядовому центрі дозволить керувати інтересами всіх зацікавлених сторін і робити відповідні компроміси для ефективної політики стійкості.

Чому це важливо?

Уряди відіграють ключову роль у забезпеченні стійкості критичної інфраструктури. Вони несуть відповідальність за забезпечення безпеки громадян і часто є регуляторами інфраструктури. Уряди на центральному чи субнаціональному рівні також можуть

бути власниками та операторами критичної інфраструктури безпосередньо або через державні компанії. Крім того, інвестиції в основну інфраструктуру часто залежать від великих державних коштів. Нарешті, уряди також є важливими користувачами або клієнтами критичної інфраструктури, від яких очікується їх надійність для безперервності діяльності уряду.

Це ставить перед урядами численні та складні ролі в секторах критичної інфраструктури та для багатьох небезпек і загроз. Менеджери ризиків і посадовці, відповідальні за управління критичними ризиками, повинні координувати роботу кількох функцій в уряді та гарантувати, що від імені загальних інтересів політичні цілі можуть бути досягнуті з точки зору стійкості, збалансовуючи відповідні компроміси.

Ключові питання політики:

- *Чи існує національна стратегія або політичний документ щодо стійкості критичноїінфраструктури?*
- *Чи є визначення критичної інфраструктури?*
- *Чи існує заздалегідь визначений перелік секторів критичної інфраструктури?*
- *Чи існує загальнодержавний підхід до розвитку стійкості критичної інфраструктури?*
- *Чи всі відповідні небезпеки та загрози враховані в політиці стійкості критичної інфраструктури?*
- *Чи існує спеціальний координаційний орган, відповідальний за розробку, моніторинг та коригування національної політики стійкості критичної інфраструктури?*

Еталонні показники

- *Національна політика щодо стійкості критичної інфраструктури*
- *Міжвідомчий/міністерський комітет/платформа для розробки політики стійкості КІ*
- *Координаційний орган при Центрі Уряду*

Приклади хорошої практики

- *У Сполучених Штатах Президентська політична директива щодо безпеки та стійкості критичної інфраструктури доручає Міністерству внутрішньої безпеки координувати політику КІ на федеральному рівні з галузевими агентствами в 16 секторах КІ.*
- *У Франції Генеральний секретаріат оборони та національної безпеки під керівництвом прем'єр-міністра координує політику стійкості КІ у 8 галузевих міністерствах для 12 секторів інфраструктури та з підходом до багатьох небезпек..*

2. Розуміння складних (взаємозалежних) залежностей і вразливостей у системах критичної інфраструктури для визначення пріоритетів заходів щодо стійкості

Уряди повинні прийняти методології та показники для визначення критичних функцій, систем і активів, які мають бути пріоритетними для інвестицій у розвиток стійкості. Для цього потрібне добре розуміння того, як збої можуть вплинути на інфраструктурні активи та де виявлені залежності та взаємозалежності, які можуть посилити їхній вплив. Після визначення пріоритетних вузлів і концентраторів у взаємозалежних системах необхідно оцінити їх стійкість за допомогою відповідних показників і порівняти фактичні та очікувані результати, щоб побачити, де є прогалини.

Чому це важливо?

Визначення методологій для оцінки ризиків, які зацікавлені сторони критичної інфраструктури з боку уряду та операторів можуть використовувати на практиці, і роз'яснення відповідних вимог до даних є фундаментальними кроками для визначення пріоритетів інвестицій у стійкість. Розуміння ризиків і вразливостей критичної інфраструктури є складним завданням, враховуючи основні взаємозалежності, і вимагає системного погляду. Існує різноманітний набір інструментів для ідентифікації критично важливих активів, розуміння їхньої вразливості до шокових подій і моделювання потенційних каскадних впливів через взаємопов'язані мережі. Останні дослідження зосереджені на складності системи, моделюванні ризиків і відображенні взаємозалежностей, що забезпечує багатий аналітичний матеріал.

Тим не менш, уряди та оператори критичної інфраструктури стикаються з необхідністю вибору правильних інструментів для ідентифікації найбільш критичних концентраторів і вузлів систем інфраструктури та оцінки рівня їх стійкості. На практиці такий аналіз використовує трирівневий підхід, для якого необхідно стандартизувати методології та інструменти. По-перше, відображення взаємозалежностей (фізичних, цифрових, географічних, логічних) між активами та системами критичної інфраструктури є ключовим для оцінки повного впливу втрати послуг у разі збою. По- друге, проведення оцінки критичності дозволяє класифікувати системи, мережі та активи, які є справді критичними, на основі впливу їх збоїв на низку попередньо встановлених критеріїв. по- третє, аналіз стійкості та стрес-тести допомагають виявити слабкі місця, де потенційні збої можуть статися з більшою ймовірністю.

Розвиток

відповідні показники для інфраструктурних активів і систем дозволяють найкраще порівняти рівень їх стійкості.

Ключові питання політики:

- *Чи існує відображення залежностей і взаємозалежностей між різними секторами критичної інфраструктури?*
- *Чи існують визначені критерії для оцінки критичності інфраструктур?*
- *Чи проводяться стрес-тести на численні небезпеки для виявлення слабких місць критичної інфраструктури?*

Еталонні показники

- *Ідентифікація критичних активів*
- *Наявність показників стійкості*

Приклади хорошої практики

- *У Нідерландах Національний координатор з питань безпеки та боротьби з тероризмом (NCTV) розробив 3-етапну методологію, щоб спочатку визначити критичну інфраструктуру та класифікувати її відповідно до критичності (A або B), по-друге, оцінити їхню вразливість до численних ризиків і, по-третє, встановити пріоритети для інвестиції в стійкість.*

- *Служба громадської безпеки Канади (PSC) провела високорівневий аналіз взаємозалежності окремих секторів CI з вивченням каскадних впливів. PSC оцінює інструменти моделювання взаємозалежності критичної інфраструктури, розроблені дослідницьким співтовариством.*

3. Встановлення довіри між урядами та операторами та забезпечення обміну інформацією про ризики та вразливі місця

Уряди повинні створити платформи для обміну інформацією з операторами критичної інфраструктури, щоб усі зацікавлені сторони інфраструктури отримали повне та спільне розуміння ризиків і вразливостей для проведення аналізу стійкості. Вкрай важливо переконатися, що дизайн цих платформ забезпечує безпеку та конфіденційність інформації, що надається, з чіткими правилами доступу, щоб забезпечити довірений обмін конфіденційною інформацією.

Чому це важливо?

Обмін інформацією є фундаментальним для урядів, щоб отримати всебічне розуміння вразливостей критичної інфраструктури. Це також допомагає операторам зрозуміти власні вразливості, свою залежність від інших інфраструктур і те, як збої в їхніх послугах можуть вплинути на інші інфраструктури або навіть на них самих.

Проблема сприяння обміну інформацією полягає в тому, щоб побудувати довіру між сторонами, щоб безпека та конфіденційність інформації, яка надається добровільно, не розголошувалася. Оператори не схильні ділитися конфіденційною інформацією про свої вразливості, критичні залежності та будь-які руйнівні інциденти за межами безпечних кіл, оскільки розголошення певної інформації може призвести до відповідальності, бути важливим для конкурентоспроможності на ринку або завдати шкоди репутації фірми. З боку уряду обмін інформацією може включати секретну інформацію, коли вона стосується національної безпеки. Ризики кіберзагроз також викликають занепокоєння, оскільки вони також можуть посилити небажання ділитися інформацією на спільних платформах, якщо гарантії їх безпеки не забезпечені належним чином.

У деяких випадках розкриття інформації про ризики може посилити відповідальність операторів і посилити заходи стійкості, наприклад, щодо кліматичних ризиків. У світі, який характеризується взаємопов’язаними системами, стійкість взаємозалежних інфраструктур така ж сильна, як і їх найслабша ланка. Таким чином, обмін інформацією суттєво сприяє доведенню операторів інфраструктури до подібного розуміння того, що потрібно для досягнення прийнятного рівня безпеки та стійкості.

Ключові питання:

- *Чи існують обов'язкові чи добровільні закони, нормативні акти та політики щодо обміну інформацією про ризики та вразливі місця?*
- *-Чи існують платформи для обміну інформацією для урядів та операторів критичної інфраструктури?*
- *Чи існують стимули для операторів інфраструктури ділитися якісною інформацією про свої залежності та вразливі місця з політичною спільнотою?*
- *Чи існують запобіжні заходи для забезпечення конфіденційності спільної інформації?*

Еталонні показники

- *Наявність захищеного механізму обміну інформацією*
- *Частота, кількість і якість спільної інформації від операторів інфраструктури*
- *Використання/задоволення платформи обміну інформацією*

Приклади хорошої практики

- *Інструмент даних та аналітики для національної інфраструктури Великобританії (DAFNI) надаєплатформа даних, моделей і технічних інструментів для комплексного аналізу інфраструктури для аналізу продуктивності системи та здійснення розумних інвестицій.*
- *Австралійська довірена мережа обміну інформацією (TISN) для критичної інфраструктури забезпечує форуми національного рівня для операторів критичної інфраструктури для обміну важливою інформацією про ризики та пом'якшеннястратегії в безпечному, неконкурентному середовищі та для розробки колективних рішень спільних проблем.*

4. Побудова партнерства для узгодження спільного бачення та досяжних цілей стійкості

Уряди повинні співпрацювати з операторами критичної інфраструктури з державного та приватного секторів, щоб узгодити спільне бачення стійкості критичної інфраструктури в масштабах країни та спільні та досяжні цілі щодо стійкості. Розвиток розуміння громадських очікувань щодо потенційної втрати послуг інфраструктури може бути корисним способом ініціювання діалогу.

Чому це важливо?

Крім обміну інформацією про ризики та вразливі місця, стійкість критичної

інфраструктури залежить від партнерства урядів з операторами інфраструктури з державного та приватного секторів у зусиллях щодо стійкості. У той час як оператори та уряди погоджуються щодо необхідності захисту критично важливих активів і підтримки своїх послуг, погляди можуть відрізнятися щодо необхідного рівня стійкості, засобів її досягнення та нормативних вимог, які мають застосовуватися. Ці заходи мають фінансові наслідки та викликають питання про те, хто візьме на себе додаткові витрати, щоб інвестувати в стійкість.

Встановлення партнерства між урядами та операторами (державними та приватними) для заохочення діалогу з цих питань є корисним підходом для розробки спільного бачення стійкості критичної інфраструктури та визначення спільних цілей. Питання політики, які необхідно розглянути, включають прийняття рішення про прийнятну тривалість «часу простою», підтримку рівних умов між операторами та уникнення ситуацій безнадійного користування в конкурентних секторах. Забезпечення залучення зацікавлених сторін, у тому числі громадськості, на регулярних зустрічах, інституціоналізованих діалогах і спільних навчаннях може сприяти досягненню консенсусу.

Ключові питання політики:

- *Чи існують інституційні діалоги для залучення операторів критичної інфраструктури до розробки політики стійкості?*
- *Чи існують процеси для розуміння суспільних очікувань щодо стійкості критичної інфраструктури?*
- *Чи існує спільне бачення стійкості критичної інфраструктури, визначене через багатосекторний діалог?*
- *Чи встановлені цілі стійкості для підтримки реалізації бачення?*

Еталонні показники

- *Існування консультацій із зацікавленими сторонами критичної*
- *інфраструктури Частота консультаційних форумів і рівень участі*
- *оператора Якість участі процес*

Приклади хорошої практики

- *У Швейцарії національна стратегія CIP, координована Федеральним відомством цивільного захисту, базується на партнерстві та різноманітних платформах з операторами CI, федеральні та субнаціональні органи влади. Окрім аналізу ризиків та обміну інформацією, Керівництво з KI розробляється спільно й дозволяє встановлювати цілі стійкості для операторів KI.*
- *У Німеччині UP KRITIS є національною ініціативою між державою та носіями CriticalІнфраструктури захисту критичних інформаційних інфраструктур. UP KRITIS складається з понад 450 співробітників.*

5. Визначення комплексу стратегій для визначення пріоритетів економічно ефективних заходів стійкості протягом життєвого циклу

Уряди повинні визначити поєднання інструментів політики для стимулювання інвестицій операторів у стійкість і досягнення спільних цілей щодо стійкості. Такі заходи повинні стосуватися всього життєвого циклу інфраструктури від планування до експлуатації, технічного обслуговування та оновлення або модернізації. Пріоритезація заходів стійкості урядом повинна ґрунтуватися на аналізі рентабельності з урахуванням наслідків для вартості послуг.

Чому це важливо?

Уряди можуть вибирати з різноманітних політичних інструментів і механізмів для просування реалізації цілей стійкості, від добровільних рамок і механізмів стимулювання до регуляторних або правових інструментів. Оператори дуже зацікавлені в збереженні безперервності своїх послуг і своєї репутації шляхом інвестування в стійкість. Однак інвестиції в стійкість часто передбачають авансові витрати, навіть якщо вони повинні бути компенсовані з точки зору більшої надійності обслуговування та стійкості до потрясінь. Питання в тому, як знайти правильний баланс. Додаткові вимоги, висунуті урядами для посилення стійкість може призвести до додаткових витрат, які в кінцевому рахунку несуть клієнти, громадяни та підприємства. Важливо пристосувати інструменти державної політики, щоб забезпечити ефективні стимули для операторів інвестувати в стійкість, одночасно керуючи фінансовими наслідками.

Регуляторний підхід має сильні сторони в тому, що він передбачає чіткі та вимірні зобов'язання, наприклад, встановлення вимог до надійності або вимогу до планів безперервності бізнесу, механізмів страхування та мінімальних стандартів безпеки. Однак, якщо використовувати приписи, це також може виявитися дорогим, не відповідати швидким технологічним розробкам і може створити проблеми з відповідністю. Запровадження компенсаційної схеми для клієнтів, чиї послуги були порушені, або інші типи штрафів можуть бути ефективними для стимулювання інвестицій у стійкість, зокрема, у державно-приватному партнерстві. Такий підхід також надає операторам можливість вибору шляхів підвищення своєї стійкості. Добровільні рамки, такі як розробка керівних принципів стійкості, заходи з підвищення обізнаності або обмін передовим досвідом, часто є кращим варіантом для залучення зацікавлених сторін, але має важливі невизначеності. Знаходячи баланс між державною фінансовою підтримкою та приватними інвестиціями для таких заходів стійкості, можна використовувати методи аналізу витрат і вигод, щоб визначити пріоритетність найбільш ефективних способів розподілу витрат на загальні колективні зусилля для досягнення спільних цілей стійкості.

Ключові питання політики:

- *Чи визначені заходи стійкості для підвищення рівня захисту, надійності, резервування або адаптивності протягом життєвого циклу критичної інфраструктури?*
- *Чи існують мінімальні стандарти безпеки, які гарантують, що оператори інвестують у стійкість?*
- *Чи відіграють галузеві регулятори певну роль у стимулюванні стійкості критичної інфраструктури?*
- *Чи використовується аналіз витрат і вигод для визначення*

пріоритетності заходів стійкості, оцінки їх впливу на вартість послуг і пошуку домовленостей про розподіл витрат?

Еталонні показники

- *Плани впровадження щодо стійкості критичної інфраструктури*
- *Положення нормативних актів інфраструктури щодо стійкості*
- *Оцінка витрат і вигод від заходів стійкості*

Приклади хорошої практики

- *У Фінляндії Управління з питань енергетики встановлює вимоги до стандартів безперервності роботи та надійності в секторі електроенергії, а Національне агентство аварійного постачання надає операторам інструменти, вказівки та методи для дотримання цих правил.*
- *У Франції держава, оператори КІ та місцеві органи влади погодили заходи для підвищення стійкості КІ до ризику великої повені в Парижі. Це включає в себе обмін інформацією, готовність до надзвичайних ситуацій і зниження вразливості існуючої та майбутньої інфраструктури.*

6. Забезпечення підзвітності та моніторинг впровадження політики стійкості критичної інфраструктури

Уряд повинен контролювати впровадження та оцінювати прогрес у досягненні цілей стійкості, а також визначити рамки підзвітності для операторів критичної інфраструктури. Перегляд ефективності інструментів політики стійкості має дозволити коригувати динамічний ландшафт ризиків та інновації в інфраструктурі, беручи до уваги потребу в передбачуваній та стабільній нормативній базі, яка сприятиме інвестиціям в інфраструктуру.

Чому це важливо?

Комплексна політична основа є першим кроком до підвищення стійкості критичної інфраструктури. Чи дійсно критична інфраструктура буде стійкою, залежить від реалізації цілей і вимог, висунутих у цій політиці. Необхідно налаштувати механізми підзвітності, щоб забезпечити виконання операторами передбачених заходів стійкості, таких як оцінка критичності та вразливості, плани безперервності бізнесу, резервні операційні системи, навчання та стрес-тести, угоди про взаємодопомогу, модернізація активів або механізми ризикового фінансування.

Впровадження моніторингу може набувати різноманітних форм, включаючи регулярні звіти, інспекції та оцінки ефективності або експертні оцінки. Щоб посилити підзвітність, штрафи за невідповідність, визнання/нагороди за впровадження передових практик і тиск з боку колег через використання оцінок/рейтингів відкритого доступу є іншими доступними стимулами, які можуть спонукати операторів віддавати пріоритет інвестиціям у заходи стійкості. Регулярні оцінки також корисні для оцінки ефективності політичних інструментів для посилення стійкості критичної інфраструктури та їх адаптації, щоб не відставати від темпів інновацій і моделей ризиків, що виникають.

Ключові питання політики:

- *Чи здійснюється регулярний моніторинг впровадження заходів стійкості операторами критичної інфраструктури?*
- *Чи існують рамки підзвітності, щоб забезпечити впровадження заходів стійкості?*
- *Чи проводяться аналізи ефективності інструментів політики стійкості, запланованих для пристосування до динамічного середовища ризиків?*
- *Чи проводяться спільні навчання для перевірки механізмів управління кризою та безперервністю?*

Еталонні показники

- *Рамки підзвітності для зацікавлених сторін критичної інфраструктури*
- *Перегляд політики щодо критичної інфраструктури*

Приклади хорошої практики

- *У Кореї Міністерство внутрішніх справ і безпеки щороку оцінює спроможність операторів критичної інфраструктури реагувати на катастрофи та оприлюднює рейтинг. Тиск з боку колег створює важливі стимули для операторів підтримувати свій суспільний імідж.*
- *Через 10 років після прийняття Європейська Комісія оцінює свою Директиву про європейську критичну інфраструктуру, щоб визначити, чи залишається вона актуальною та ефективною.*

7. Розгляд транскордонного виміру систем інфраструктури

Уряд повинен координувати національну політику стійкості критичної інфраструктури з сусідніми країнами та за їх межами, щоб вирішити проблему транскордонної залежності. Необхідно створити міжнародні механізми обміну інформацією для оцінки ризиків і вразливостей через кордони, а також для розробки спільних підходів до стійкості критичної інфраструктури.

Чому це важливо?

Взаємопов'язані та взаємозалежні інфраструктури перетинають кордони, надаючи важливий міжнародний вимір стійкості. Небезпеки та загрози не зупиняються на національних кордонах, і інтегровані ланцюги поставок можуть поширювати їхні наслідки. У деяких випадках критична інфраструктура надає послуги в кількох країнах і різних юрисдикціях. Це робить більш переконливим інтегрувати міжнародне співробітництво в політику стійкості критичної інфраструктури. Обмін інформацією та передовим досвідом, прийняття спільних

підходів, розробка спільних стандартів стійкості критичної інфраструктури є одними з варіантів політики, які можуть сприяти міжнародному та транскордонному співробітництву в цій сфері.

Ключові питання:

- *Чи існують міжнародні форуми для сприяння обміну передовим досвідом і розробці спільних підходів до політики стійкості критичної інфраструктури?*
- *Чи існують міжнародні платформи обміну інформацією про ризики та вразливість для взаємозалежної критичної інфраструктури?*
- *Чи існують механізми співпраці для визначення спільних стандартів стійкості критичної інфраструктури з сусідніми країнами?*

Еталонні показники

- *Основи міжнародної політики щодо стійкості критичної інфраструктури*
- *Спільні плани стійкості критичної інфраструктури*

Приклади хорошої практики

- *Канадсько-американський план дій щодо критичної інфраструктури сприяє комплексному підходу до захисту та стійкості критичної інфраструктури шляхом покращення координації діяльності та сприяння постійному діалогу між транскордонними зацікавленими сторонами.*
- *Європейська програма захисту критичної інфраструктури (EPCIP) — це довгострокова програма, яка охоплює різні інструменти захисту критичної інфраструктури в ЄС, включаючи регулярні зустрічі національних контактних осіб CIP. Його зовнішній вимір включає регулярні зустрічі зі стратегічними партнерами та нещодавно був розширений за рахунок співпраці з сусідніми країнами.*

Список літератури

G7 (2016),Декларація лідерів G7 Ісе-Сіма, *https://www.mofa.go.jp/files/000160266.pdf* (дата доступу: 25 лютого 2019 р.). [38]

OECP (2018),Оцінка глобального прогресу в управлінні критичними ризиками, Огляди OECP політики управління ризиками, OECD Publishing, Париж, *https://dx.doi.org/10.1787/9789264309272-en* . [2]

OECP (2017),Правильна інфраструктура: основа для кращого управління, OECP Видавництво, Париж, *https://dx.doi.org/10.1787/9789264272453-en* . [11]

OECP (2014),Підвищення стійкості за допомогою інноваційного управління ризиками, OECD Reviews of: Політика управління ризиками, OECD Publishing, Париж, *ttps://dx.doi.org/10.1787/9789264209114-en* . [20]

OECP (2014),Рекомендація Ради з управління критичними ризиками, *http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf (дата доступу: 25 лютого 2019 р.).* [1]

OECP та ЄС JRC (2018),Системне мислення для стійкості та безпеки критичної інфраструктури - Семінар *OECD/ JRC - OECD,http://www.oecd.org/gov/risk/workshop-oecd-jrc-systemthinking- for-critical-infrastructure-resilience-and-security.htm* (дата доступу: 25 лютого 2019 р.). [41]

Управління ООН зі зменшення ризику стихійних лих (2015),Сендайська структура ризику стихійних лих [39]

Скорочення 2015 - 2030 рр,*https://www.unisdr.org/files/43291_sendaiframeworkfordrren.pdf*

(дата доступу: 25 лютого 2019 р.).

ОРГАНІЗАЦІЯ ЕКОНОМІЧНОГО СПІВРОБІТНИЦТВА І РОЗВИТОК

ОЕСР є унікальним форумом, де уряди спільно працюють над вирішенням економічних, соціальних та екологічних викликів глобалізації. ОЕСР також знаходиться в авангарді зусиль, спрямованих на те, щоб зрозуміти та допомогти урядам реагувати на нові події та проблеми, такі як корпоративне управління, інформаційна економіка та виклики старіння населення. Організація забезпечує середовище, де уряди можуть порівнювати політичний досвід, шукати відповіді на спільні проблеми, визначати передову практику та працювати над координацією внутрішньої та міжнародної політики.

Країни-члени ОЕСР: Австралія, Австрія, Бельгія, Канада, Чилі, Чехія, Данія, Естонія, Фінляндія, Франція, Німеччина, Греція, Угорщина, Ісландія, Ірландія, Ізраїль, Італія, Японія, Корея, Латвія, Литва, Люксембург, Мексика, Нідерланди, Нова Зеландія, Норвегія, Польща, Португалія, Словацька Республіка, Словенія, Іспанія, Швеція, Швейцарія, Туреччина, Великобританія та Сполучені Штати. Європейський Союз бере участь у роботі ОЕСР.

ОЕСР Publishing широко поширює результати збору статистичних даних і досліджень Організації з економічних, соціальних і екологічних питань, а також конвенцій, інструкцій і стандартів, узгоджених її членами.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
ISBN 978-92-64-53346-2 – 2019

Огляд ОЕСР політики управління ризиками

Ефективне управління для стійкості критичної інфраструктури

Критичні інфраструктури є основою сучасних взаємопов'язаних економік. Збій у роботі ключових систем і основних послуг, таких як телекомунікації, енерго- та водопостачання, транспорт чи фінанси, може завдати значних економічних збитків. У цьому звіті розглядається, як підвищити стійкість критичної інфраструктури в умовах динамічного ризику, а також обговорюються варіанти політики та моделі управління для стимулювання початкових інвестицій у стійкість. Базуючись на міжнародному опитуванні, у звіті аналізується поступовий перехід політики критичної інфраструктури від захисту активів до стійкості системи. Отримані результати відображені в запропонованому наборі інструментів політики для управління стійкістю критичної інфраструктури, який може скеровувати уряди щодо застосування більш узгодженого, превентивного підходу до захисту та підтримки основних послуг.

Зверніться до цієї публікації онлайн за адресою ***https://doi.org/10.1787/02f0e5a0-en***.

Ця робота опублікована в OECD iLibrary, яка збирає всі книги, періодичні видання та статистичні бази даних OECD. Відвідайте ***www.oecd-ilibrary.org*** для отримання додаткової інформації.

ISBN 978-92-64-53346-2