

Структура планування стійкості інфраструктури (IRPF)

неофіційний
переклад

Цей текст є неофіційним перекладом документу, розміщеного на відкритому інформаційному ресурсі Агентства з кібербезпеки та безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки (CISA), та може використовуватись лише з інформаційною та науковою метою.

Посилання на офіційний оригінал документа:

https://www.cisa.gov/sites/default/files/2023-07/Infrastructure_Resilience_Planning_Framework_%28IRPF%29_v1.1_May2023.pdf

Структура планування стійкості інфраструктури (IRPF)

Агентство з кібербезпеки та безпеки інфраструктури (CISA) розробило Структуру планування стійкості інфраструктури (IRPF), щоб забезпечити врахування засад безпеки та стійкості при плануванні критичної інфраструктури та прийнятті інвестиційних рішень.

IRPF організований наступним чином:

Розділ 0. Загальний огляд

Розділ 1. Закладання основи

Розділ 2. Ідентифікація об'єктів критичної інфраструктури

Розділ 3. Оцінка ризиків

Розділ 4. Розробка дій

Розділ 5. Впровадження та оцінка

Всі джерела

Глосарій



0. Огляд

У цьому розділі розглядається наступне:

1. ВСТУП
2. ПЛАНУВАННЯ СТІЙКОЇ ІНФРАСТРУКТУРИ
3. СТРУКТУРА ПЛАНУВАННЯ СТІЙКОСТІ ІНФРАСТРУКТУРИ (IRPF)
4. ВІДПОВІДНІСТЬ ІНШИМ ПРОЦЕСАМ
5. ДЖЕРЕЛА ФІНАНСУВАННЯ ТА ТЕХНІЧНОЇ ДОПОМОГИ

0. Огляд

0.1 ВСТУП

Інфраструктура є основою наших громад, забезпечуючи не лише критично важливі послуги (такі як водопостачання, транспорт, електроенергія та комунікації), а також засоби для охорони здоров'я, безпеки та економічного зростання. Ці системи часто виходять за межі наших громад, надаючи послуги цілим регіонам і сприяючи виконанню національних критично важливих функцій. Враховуючи життєву важливість інфраструктури для нашого соціального та економічного добробуту, вкрай важливо, щоб наші мережі були міцними, безпечними та стійкими. Для того, щоб громади процвітали перед обличчям неконтрольованих обставин і адаптуватися до мінливих умов (наприклад, еволюції загроз безпеці, впливу екстремальних погодних умов, технологічного розвитку та соціально-економічних зрушень), ми повинні працювати над тим, щоб зробити нашу інфраструктуру більш стійкою.

Президентська політична директива 21 (PPD-21) "Безпека та стійкість критичної інфраструктури" визначає стійкість як здатність готуватися до мінливих умов та адаптуватися до них, а також витримувати та швидко відновлюватися після збоїв. Стійкість інфраструктури залежить як від фізичних характеристик інженерних інфраструктурних систем, так і від можливостей організацій, що впливають на експлуатацію та управління цими системами (наприклад, власників та операторів інфраструктури, регуляторних органів, а також постачальників та підрядників). На стійкість також впливають такі організаційні фактори, як наявність планів забезпечення безперервності бізнесу та реагування на надзвичайні ситуації, рівень підготовки персоналу та частота проведення навчань для тестування планів. Розвиток стійкості має важливе значення для управління широким спектром ризиків, з якими стикаються громади, в тому числі ризиків, пов'язаних із залежністю між інфраструктурними системами.¹

Агентство з кібербезпеки та безпеки інфраструктури (CISA) розробило Структуру планування стійкості інфраструктури (IRPF), щоб запропонувати підхід, за яким місцеві органи влади, регіони та приватний сектор можуть спільно працювати над плануванням безпеки та стійкості критично важливих інфраструктурних послуг в умовах численних загроз та змін.

Основною аудиторією IRPF є штати, місцеві, племенні та територіальні органи влади та пов'язані з ними регіональні організації; однак IRPF може гнучко використовуватися будь-якою організацією, яка прагне вдосконалити своє планування стійкості. IRPF надає ресурси для інтеграції критичної інфраструктури в планування, а також структуру для роботи на регіональному рівні та між системами і юрисдикціями.

Ця структура надає методи та ресурси для забезпечення безпеки та стійкості критичної інфраструктури через планування, допомагаючи громадам та регіонам:

- > **Розуміти та повідомляти** про те, як стійкість інфраструктури сприяє стійкості громади;
- > **Визначати**, як загрози та небезпеки можуть вплинути на нормальне функціонування інфраструктури громади та надання послуг;
- > **Підготувати** уряди, власників та операторів до протистояння та адаптації до нових загроз і небезпек;
- > **Інтегрувати** засади безпеки та стійкості інфраструктури, включаючи вплив залежностей та каскадних збоїв, у планування та інвестиційні рішення; та
- > Швидко **відновлюватися** після збоїв до нормального функціонування інфраструктури громади та регіону

У цьому документі під "громадою" слід розуміти не лише окремі міста чи селища, а й регіональні органи влади, що здійснюють планування, та зацікавлені сторони, які мають спільні інтереси або працюють над створенням спільного коридору з метою підвищення стійкості пов'язаних інфраструктурних систем.

0.2 ПЛАНУВАННЯ СТІЙКОЇ ІНФРАСТРУКТУРИ

IRPF не є остаточною дорожньою картою, а скоріше гнучким набором керівних документів і ресурсів, які допоможуть розпочати планування безпеки та стійкості інфраструктури та інтегрувати його в існуючі механізми планування.* Хоча IRPF структуровано як набір послідовних кроків, користувач може вибрати, які саме кроки і набори джерел більш повно враховуватимуть інфраструктуру в будь-якому існуючому або поточному процесі планування.

* У цьому посібнику ми надаємо посилання на джерела, розроблені іншими партнерами, окрім Федерального уряду. Ця інформація надається "як є" виключно в інформаційних цілях. CISA не надає жодних гарантій щодо цієї інформації. CISA не підтримує жодну організацію, продукт або послугу, включаючи будь-які об'єкти аналізу. Будь-яке посилання на конкретні комерційні продукти, процеси або послуги за допомогою знаків обслуговування, торгових марок, виробників або іншим чином не означає їх схвалення, рекомендацію або прихильність з боку CISA.

Громади можуть переглянути структуру, щоб визначити, де вони знаходяться в спектрі планування, і вибрати рекомендації та джерела, які найкраще відповідають їхнім потребам.

Громади з обмеженим часом і ресурсами, можливо, спочатку захочуть зосередитися на секторах інфраструктури, які підтримують критичні функції, такі як енергетика, зв'язок, транспорт, системи водопостачання та водовідведення, з потенціалом для подальшого розширення.

І навпаки, громади, які мають більше часу та ресурсів, можуть розглянути всі інші сектори критичної інфраструктури, які вважаються важливими та/або життєво необхідними для безперервного виконання ключових соціальних та економічних функцій, що є невід'ємною частиною процвітання громади або регіону.

IRPF допомагає користувачам досліджувати взаємозв'язки між інфраструктурними системами, щоб краще розуміти інфраструктурні ризики, розробляти проекти та стратегії для їх подолання, а також визначати фінансові та імплементаційні ресурси для вжиття заходів.

Зрештою, стійкість інфраструктури сприяє підвищенню життєздатності громади і може допомогти розвивати і підтримувати міцне, безпечне та економічно активне місце для життя і роботи. Це може допомогти сформувати самопідсилюючий цикл, в якому підвищена соціальна та економічна стійкість призводить до підвищення стійкості інфраструктури, і навпаки.

0.3 СТРУКТУРА ПЛАНУВАННЯ СТІЙКОСТІ ІНФРАСТРУКТУРИ (IRPF)

IRPF розроблений як проста у використанні структура для включення стійкості критичної інфраструктури в місцеві, регіональні та племінні плани. IRPF покликаний допомогти громадам, регіонам, власникам та операторам інфраструктури краще зрозуміти ризики критичної інфраструктури, визначити можливості для підвищення стійкості, а також надати інформацію для прийняття політичних та інвестиційних рішень.

Крок 1, Закладення основи. Громади визначають зусилля з планування та їхній обсяг, формують групу планування для виконання цих зусиль, а також аналізують наявні дані, плани, дослідження, карти та інші ресурси.

Крок 2, Ідентифікація критичної інфраструктури. Надає рекомендації громадам щодо того, як визначити та пріоритизувати інфраструктуру та оцінити залежність між інфраструктурними системами.

Крок 3, Оцінка ризику. Ознайомлює громади з процесом проведення оцінки ризиків для критичної інфраструктури, що включає оцінку вразливості до загроз і небезпек, а також наслідків, які можуть виникнути в результаті.

Крок 4, Розробка дій. Надає рекомендації щодо розробки стратегічного плану дій для подолання ризиків та підвищення стійкості інфраструктури шляхом визначення та пріоритизації потенційних рішень.

Крок 5, Впровадження та оцінка. Зосереджується на включенні проектів і стратегій інфраструктурної стійкості в громадські та регіональні плани, а також на процесах вимірювання успіху.



Щоб підтримати ці зусилля, IRPF також включає низку [ресурсів](#), які допоможуть громадам у проходженні різних етапів IRPF.

РЕСУРСИ ДОСТУПНІ!

У цьому посібнику IRPF надає допомогу, на яку вказують наведені нижче символи. Метою цього є надання вичерпного переліку ресурсів з планування стійкості, доступних для всіх юрисдикцій. IRPF визначає ресурси за суб'єктами (федеральні, штатів, неприбуткові тощо), критеріями відповідності, секторами інфраструктури тощо.



РЕСУРСИ



КОРОТКІ
ПОРАДИ



ПРИМІТКИ



ВИЗНАЧЕННЯ

IRPF закликає планувальників застосовувати функціональний, системний підхід при розгляді критичної інфраструктури. Окремі об'єкти інфраструктури важливі настільки, наскільки важлива функція, яку вони забезпечують:

може не мати значення, що під час інциденту виведено з ладу водоочисну станцію або насосну станцію, наприклад, якщо до цього часу існують адекватні альтернативи для забезпечення населення питною водою, система може бути відновлена. З іншого боку, інфраструктурні системи тісно пов'язані між собою, і порушення в одній з них може мати каскадний вплив на низку інших інфраструктурних систем. Враховуючи ці два фактори, IRPF закликає планувальників враховувати критичні функції, що забезпечуються інфраструктурними системами, а також залежності, які існують всередині і між цими системами. Глибоке розуміння цих двох факторів може допомогти планувальникам визначити стратегії та проекти для зменшення ризиків і зробити кращі інвестиції в стійкість.

IRPF може застосовуватися до всіх 16 секторів критичної інфраструктури, визначених [Президентською політичною директивою 21 \(PPD-21\) - Безпека та стійкість критичної інфраструктури](#), яка встановлює національну політику щодо зміцнення та підтримки безпечної, функціонуючої та стійкої критичної інфраструктури до фізичних та кіберзагроз. PPD-21 визначає 16 секторів критичної інфраструктури, чий активи, системи та мережі, як фізичні, так і віртуальні, вважаються настільки важливими для Сполучених Штатів, що їхня недієздатність або руйнування матиме виснажливий ефект на безпеку, національну економічну безпеку, охорону здоров'я або безпеку громадян, або будь-яку їх комбінацію. Ці сектори критичної інфраструктури перелічені в Таблиці 1, включаючи короткий опис типових компонентів, що входять до кожного з них. Хоча PPD-21 розглядає системи та об'єкти критичної інфраструктури з національної точки зору, ці сектори також мають значення на місцевому, державному та регіональному рівнях, і розуміння ризиків для цих систем може покращити безпеку, охорону здоров'я та безпеку громадян, а також економічне зростання у вашій громаді.

У кожній громаді та регіоні ці сектори забезпечують критично важливі функції через інфраструктурні системи. Ці системи складаються з активів, які пов'язані між собою і залежать один від одного, а безперервна робота цих систем залежить не лише від їхніх власних активів, але й від інших систем в інших секторах. Важливо, що майже всі сектори залежать від водопостачання та водовідведення, зв'язку та транспорту. IRPF допомагає користувачам дослідити ці інфраструктурні системи, визначити ключові залежності всередині них та між ними, а також врахувати ці знання при плануванні.

Таблиця 1. Сектори критичної інфраструктури

СЕКТОР КРИТИЧНОЇ ІНФРАСТРУКТУРИ	ТИПОВІ КОМПОНЕНТИ
1. Хімічний	Підприємства, що виробляють основні хімічні речовини, спеціальні хімічні речовини, сільськогосподарські хімікати, фармацевтичні препарати та споживчі товари.
2. Комерційні об'єкти	Державні та приватні об'єкти, які приваблюють великі натовпи людей для розваг та/або засобів масової інформації; ігор; проживання; заходів на відкритому повітрі; публічних зібрань; нерухомості; роздрібною торгівлі; та спортивних цілей.
3. Комунікаційний	Послуги голосового зв'язку та передачі даних і/або наземні, супутникові та бездротові мережі зв'язку.
4. Критичне виробництво	Об'єкти, що забезпечують виробництво первинних металів, машин, електрообладнання, приладів і компонентів, а також транспортного обладнання.
5. Дамби	Активи сектору включають проекти дамб, гідроелектростанції, судноплавні шлюзи, дамби, дамби, ураганні бар'єри, хвостосховища шахт та інші сховища промислових відходів. Національний реєстр дамб налічує понад 100 000 дамб по всій території Сполучених Штатів. Велика кількість різноманітних державних і приватних організацій володіють і експлуатують ці об'єкти під дуже розгалуженим регуляторним наглядом з боку федеральних, штатних і місцевих органів влади.
6. Оборонно-промислова база	Лабораторії, виробничі підприємства спеціального призначення, організації та ланцюги постачання, які здійснюють дослідження і розробку, проектування, виробництво, системну інтеграцію, технічне обслуговування та ремонт військових систем озброєнь, підсистем, компонентів, підкомпонентів або частин, які підтримують військові операції.
7. Служби екстреної допомоги	Об'єкти, комунікаційні споруди, інше спеціалізоване обладнання для підтримки/розміщення правоохоронних органів, пожежно-рятувальних служб, служб екстреної медичної допомоги, управління в надзвичайних ситуаціях, а також громадських робіт.
8. Енергетичний	Об'єкти та системи для виробництва, передачі та розподілу електроенергії, а також для видобутку, переробки та розподілу нафти і природного газу.
9. Фінансові послуги	Депозитарні установи, постачальники інвестиційних продуктів, страхові компанії, інші кредитні та фінансові організації, а також постачальники критично важливих фінансових послуг та сервісів, які підтримують ці функції.
10. Харчування та сільське господарство	Території або об'єкти, пов'язані з виробництвом, переробкою та доставкою споживчих продуктів (наприклад, ресторани, заклади харчування, харчові підприємства та ферми).
11. Державні установи	Об'єкти, що належать або орендовані федеральним урядом, урядами штатів, місцевими, територіальними та плеєніними урядами, а також державні та приватні навчальні заклади, національні пам'ятники та ікони.
12. Охорона здоров'я	Державні та приватні медичні заклади, дослідницькі центри, постачальники, виробники та інші фізичні активи.
13. Інформаційні технології	Фізичні активи та віртуальні системи і мережі, що беруть участь у створенні інформаційно-технологічних продуктів і послуг, таких як дослідження і розробка, виробництво, дистрибуція, модернізація та технічне обслуговування.
14. Ядерні реактори, матеріали та відходи	Ядерні енергетичні реактори та їхні установки, дослідницькі та випробувальні реактори, водойми-охолоджувачі та об'єкти паливного циклу.
15. Транспортні системи	Авіаційні, наземні або морські транспортні системи (наприклад, громадський транспорт, кораблі, залізничні, автомобільні та трубопровідні системи).
16. Системи водопостачання/водовідведення	Системи питної води, свердловини та системи очищення стічних вод.

0.4 ВІДПОВІДНІСТЬ ЗУСИЛЛЯМ З ПЛАНУВАННЯ ТА ВИЗНАНИМИ НА ФЕДЕРАЛЬНОМУ РІВНІ ПРОЦЕСАМИ

Важливо зазначити, що IRPF був розроблений з метою узгодження та інформування інших зусиль з планування на федеральному рівні, рівні штатів, місцевому, племінному та територіальному рівнях, за виконання яких може відповідати громада. У Таблиці 2 наведені деякі з існуючих заходів з планування, які можуть бути використані у IRPF.

Ці кроки та пов'язані з ними ресурси можна легко інтегрувати в інші процеси планування, такі як комплексне планування, пом'якшення наслідків надзвичайних ситуацій, екологічне планування, планування капітального ремонту та регіонального транспорту. Насправді, ключова перевага IRPF полягає в тому, що він може допомогти визначити проекти з підвищення стійкості, які можна включити до цих планів, що дозволить громаді розбудувувати свою стійкість у довгостроковій перспективі та надає пріоритетний перелік потенційних проектів, які можуть бути реалізовані за рахунок федерального фінансування після стихійного лиха. Крім того, IRPF підтримує Національну інвестиційну стратегію пом'якшення наслідків стихійних лих Федерального агентства з надзвичайних ситуацій (FEMA) та Рамкову програму стійкості до стихійних лих Управління державної звітності США (GAO), а також узгоджується з ними. Хоча FEMA створило низку "ліній життєзабезпечення громад", які на перший погляд можуть здатися такими, що суперечать секторальному підходу CISA, ці дві структури насправді доповнюють одна одну. Лінії життєзабезпечення громад, створені FEMA, узгоджують з інфраструктурними секторами CISA і призначені для підтримки операцій реагування, тоді як 16 секторів CISA можуть підтримувати стабільну діяльність.

Таблиця 2. Заходи з планування, про які може інформувати IRPF

ІСНУЮЧІ ФЕДЕРАЛЬНІ, ШТАТІВ, МІСЦЕВІ, ПЛЕМІННІ ТА ТЕРИТОРІАЛЬНІ ПЛАНИ

Плани капітального ремонту	Плани землекористування
Комплексні/загальні плани	Довгострокові плани відновлення
Плани економічного розвитку	Плани відновлення стану до катастрофи
Плани дій у надзвичайних ситуаціях	Плани розвитку конкретних територій
Інструмент сприяння розвитку (LCAT)	Ідентифікація загроз та небезпек
логістичного потенціалу FEMA	та оцінка ризику
Плани управління зростанням	Плани перевезень
Плани пом'якшення наслідків надзвичайних ситуацій	Плани управління водними ресурсами
Плани житлового будівництва	Інші місцеві та регіональні плани

ШВИДКА ПОРАДА



IRPF може підтримати майже на кожному етапі процесу пом'якшення наслідків надзвичайних ситуацій, забезпечуючи більш глибоке занурення в критично важливу інфраструктуру та її залежність, залучаючи власників інфраструктури до обговорення та аналізу ризиків, пов'язаних з небезпеками, що, в свою чергу, може бути використано громадою для подання заявки на отримання федерального грантового фінансування. Для отримання додаткових ресурсів, будь ласка, зверніться до [Ресурсів з планування стійкості інфраструктури](#).

ДЛЯ ЦЬОГО Є РЕСУРС!



Узгодження IRPF з федеральними процесами планування та управління ризиками

Ця матриця ілюструє, як IRPF узгоджується з іншими існуючими федеральними процесами та керівними принципами планування ризиків та/або стійкості та доповнює їх.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Методологія оцінки стійкості регіональної інфраструктури

На основі уроків, винесених з Програми оцінки регіональної стійкості CISA, ця методологія оцінки забезпечує загальний процес оцінки та вирішення складних питань стійкості інфраструктури, підтверджений десятирічним досвідом реалізації проектів RRAP.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Багато в чому IRPF доповнює та уточнює інші посібники та методології з питань стійкості. Наприклад, результати IRPF можуть бути використані в Кроці 3 "Оцінка ризиків та характеристика антропогенного середовища" Посібника з планування стійкості громади (CRPG) Національного інституту стандартів і технологій (НІСТ). Крім того, процес оцінки стійкості інфраструктури, задокументований у Методології оцінки стійкості регіональної інфраструктури CISA, тісно пов'язаний з етапами планування та рекомендаціями, викладеними в IRPF.

0.5 ДЖЕРЕЛА ФІНАНСУВАННЯ ТА ТЕХНІЧНОЇ ДОПОМОГИ

Ключовою особливістю планування є визначення наявності ресурсів для розробки та здійснення планування та реалізації. IRPF надає перелік цих ресурсів як у вигляді документа, так і у вигляді зручної для користувача матриці, що окреслює можливості фінансування та технічної допомоги, які можуть допомогти громадам втілити планування в життя.

ДЛЯ ЦЬОГО Є РЕСУРС!



Збірник програм та механізмів фінансування стійкості інфраструктури

Збірник програм та механізмів фінансування стійкості інфраструктури містить перелік потенційних джерел фінансування та технічної допомоги з посиланнями на них.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

1. Закладання основи

У цьому розділі розглядається наступне:

1. ВИЗНАЧИТИ ЧЕМПІОНА ПРОЄКТУ
2. ВИЗНАЧИТИ ЗУСИЛЛЯ ТА ЇХНІЙ ОБСЯГ
3. ЗБИРАТИ ТА ПЕРЕГЛЯДАТИ НАЯВНУ ІНФОРМАЦІЮ
4. СФОРМУВАТИ ГРУПУ СПІЛЬНОГО ПЛАНУВАННЯ
5. ВИЗНАЧИТИ ЦІЛІ ТА ЗАВДАННЯ

1. Закладання основи



Крок 1 IRPF закладає основу для успіху, надаючи рекомендації щодо того, як забезпечити початкову підтримку, сформувати спільну групу планування, а також зібрати та проаналізувати наявні дані, плани, дослідження, карти та інші технічні ресурси, які можуть бути корисними для інформування під час планування. Хоча цей розділ побудований як послідовний процес, багато з цих "кроків" відбуваються одночасно та ітеративно. Наприклад, після визначення лідера та групи планування користувачі можуть переглянути сферу своєї діяльності та переоцінити, які минулі оцінки та заходи з планування мають відношення до їх поточних зусиль. Планувальники повинні розглянути, як IRPF може найкращим чином доповнити їх поточний процес планування, і які кроки додадуть найбільшу цінність. Зрештою, система має бути гнучкою - користувачам пропонується адаптувати процес IRPF так, щоб він якнайкраще відповідав їхнім потребам.

1.1 ВИЗНАЧИТИ ЧЕМПІОНА ПРОЄКТУ

Для розвитку підтримки важливо, щоб окрема організація, яка відстоює важливість стійкості, надавала підтримку у вигляді часу та ресурсів для планування. Це може бути державний департамент, рада племені, місцева юрисдикція, відділ планування громади, регіональна організація планування, державна/приватна неприбуткова організація або інша організація, яка очолює розробку плану. Важливо, щоб ця організація була здатна активно підтримувати процес планування та зусилля з його реалізації.

1.2 ВИЗНАЧИТИ ЗУСИЛЛЯ ТА ЇХНІЙ ОБСЯГ

Перш ніж інтегрувати IRPF у процес планування, слід розглянути кілька питань, щоб визначити, які зусилля необхідно докласти для цього:

- > Що є рушійною силою бажання чи потреби у плануванні стійкості?
- > Які цілі та завдання громади у сфері стійкості?
- > Чи існують конкретні недоліки в інфраструктурі, що обслуговує громаду, які необхідно усунути?

Існує багато видів оцінок і аналізу, які можуть бути використані при плануванні: від аналізу загроз, вразливостей і критичності, картографування і побудови діаграм системи до моделювання та імітаційного аналізу. Визначення чітких цілей, завдань та обсягу може допомогти планувальникам визначити, які форми аналізу найкраще підтримають їхні зусилля. [Методологія оцінки стійкості регіональної інфраструктури](#) містить додаткову інформацію про аналітичні методи, які планувальники можуть використовувати для покращення розуміння інфраструктурних систем у своїй громаді, що ґрунтується на більш ніж 10-річному досвіді та понад 120 унікальних оцінках. Визначивши загальний напрямок зусиль, громада може більш ефективно розподілити час, кошти та персонал відповідно до обсягу зусиль.

ЗВЕРНІТЬ УВАГУ

Одним з найважливіших компонентів успіху процесу планування IRPF є документування процесу. На всіх етапах IRPF дуже важливо координувати керівництво і документувати всі зусилля з планування. Подбайте про те, щоб забезпечити належне ведення нотаток, і намагайтеся регулярно робити резервні копії (за можливості, дублюючи) всіх відповідних файлів.



1.2.1 Час і ресурси

Важливо належним чином укомплектувати штат і профінансувати зусилля з планування таким чином, щоб виділені ресурси відповідали цілям забезпечення стійкості та складності роботи, пов'язаної з їх досягненням. Враховуючи часові та ресурсні обмеження, які можуть існувати, IRPF розроблений для підтримки та доповнення існуючих або поточних заходів з місцевого та регіонального планування. Таким чином, очікується, що для включення концепцій стійкості інфраструктури, викладених у IRPF, знадобляться номінальні додаткові ресурси і час.

ШВИДКА ПОРАДА

Громади можуть заощадити кошти, інтегрувавши процеси та ресурси IRPF з існуючими практиками планування, що фінансуються за рахунок грантів або технічної допомоги, наприклад, зменшення небезпек, комплексне планування або планування економічного розвитку.



1.2.2 Визначте керівника групи планування

Протягом усього процесу інтеграції IRPF необхідне сильне керівництво, а керівник групи планування повинен виконувати функції менеджера проекту. У більшості випадків це буде особа з організації-лідера проекту. Як мінімум, керівник повинен звітувати перед лідером проекту, громадою. за необхідності, надавати інформацію про хід і результати різних видів діяльності, пов'язаних з процесом планування. У Таблиці 3 визначено кваліфікаційні вимоги до керівника групи планування.

Таблиця 3. Кваліфікація керівника групи планування

ЩО РОБИТЬ ХОРОШОГО ЛІДЕРА КОМАНДИ ПЛАНУВАННЯ?

1. Практичні знання місцевої та регіональної інфраструктури, наприклад громадських робіт.
2. Розуміння загроз і небезпек, ризиків і наслідків.
3. Здатність залучати широкий спектр зацікавлених сторін до участі в процесі планування та проведення експертизи з питань критичної інфраструктури.
4. Здатність виконувати адміністративні, координаційні функції та функції планування подій та сприяти плануванню сесій.

1.2.3 Проведення попередніх заходів

Після того, як визначено керівника групи планування, він/вона має провести попередні заходи, щоб закласти фундамент для успішної роботи. Ці заходи включають

- > Визначення мети зусиль та виявлення їхнього зв'язку з іншими зусиллями з планування в громаді
- > Визначення обсягу зусиль (включаючи область планування)
- > Формулювання цілей і завдань та окреслення стратегії зусиль
- > Розробка попереднього розкладу
- > Забезпечення безпеки приміщення для проведення зустрічей
- > Визначення фасилітатора для проведення дискусій під час зустрічей групи планування (за необхідності)
- > Визначення зацікавлених сторін, які мають інтерес або інформацію, критично важливу для зусиль

ЗВЕРНІТЬ УВАГУ

Зібрати разом усіх потрібних зацікавлених сторін і забезпечити врахування різноманітних думок та інтересів може бути складно. Може бути корисно провести оцінку або аналіз зацікавлених сторін разом з лідером проекту, щоб визначити, які організації слід залучити до участі в проекті. Повторення цього процесу в міру додавання зацікавлених сторін може створити ефект снігової кулі, що підвищить ефективність інформаційно-пропагандистської роботи.



ЗВЕРНІТЬ УВАГУ

Співпраця та захист інформації



Планувальники повинні усвідомлювати проблеми, пов'язані з обміном інформацією, і продумати, як захищати конфіденційні матеріали. Використовуйте загальноприйняті методи кібербезпеки, такі як захист документів паролем у поєднанні з угодами про нерозголошення. Існують такі ресурси, як затверджена Конгресом США Програма захисту інформації про критично важливу інфраструктуру (PCI), яка призначена для захисту інформації про інфраструктуру приватного сектору, що надається на добровільних засадах без розголошення конфіденційних даних, а також Програма SSI Адміністрації транспортної безпеки (TSA), яка захищає і редагує конфіденційну інформацію з питань безпеки (SSI).

1.3 ЗБИРАТИ ТА ПЕРЕГЛЯДАТИ НАЯВНУ ІНФОРМАЦІЮ

Щоб закласти міцний фундамент для учасників, важливо визначити попередні зусилля з планування, дослідження, картографування та інші дані, які можуть бути використані в роботі. Ці дані можуть надходити з державних, місцевих, племянних і територіальних (SLTT), регіональних або федеральних джерел.

До першої зустрічі з планування керівник групи планування повинен визначити та проаналізувати дані та інформацію, що стосуються інфраструктурних об'єктів, систем та мереж громади, а також дані та інформацію про загрози, небезпеки та події, пов'язані з надзвичайними ситуаціями, що відбуваються в громаді.

Також слід переглянути інші існуючі плани громади, щоб виявити інформацію, яка стосується поточного процесу планування. Перелік планів громад, які необхідно переглянути, наведено в Таблиці 2 в Розділі 0.2. Під час аналізу слід порівняти стратегії цих планів, щоб виявити будь-які невідповідності або конфлікти, які можна вирішити в процесі поточного планування.

ШВИДКА ПОРАДА



Хоча загальний обсяг і цілі будуть визначатися характером У процесі планування, що здійснюється, це може допомогти продумати цілі та підходи для більш глибокого врахування критичної інфраструктури в процесі планування. У цьому процесі можна допомогти за допомогою кількох кроків:

- > **Визначте прогалини в знаннях:** На самому початку може бути корисно сформулювати прогалини в знаннях про стійкість інфраструктури, які ви прагнете усунути. У багатьох випадках ці прогалини в знаннях включають визначення того, як критичні функції або послуги підтримуються системи інфраструктури, які залежності існують між системами та які системи є вразливими до збоїв. Цей процес не обов'язково має бути вичерпним, але він може допомогти планувальникам та учасникам широко осмислити інфраструктурні системи та питання, які слід розглянути під час планування.
- > **Уточнити сферу застосування:** Після визначення прогалин у знаннях, уточнення обсягу робіт може допомогти зосередити увагу на ролі врахування стійкості інфраструктури в процесі планування. Масштаб зусиль має бути достатньо широким, щоб забезпечити інформацію для планування, але достатньо вузьким, щоб відповідати часовим рамкам і ресурсам, пов'язаним з більшим проектом планування.
- > **Розробити стратегію збору даних:** На основі обсягу дослідження та виявлених прогалин у знаннях можна розробити стратегію, яка визначатиме, яку інформацію потрібно зібрати, як і коли її збиратимуть, а також яких учасників і партнерів слід залучити. Зрештою, мета стратегії збору даних полягає в тому, щоб визначити, що саме має бути зібрано для кращого розуміння інфраструктурних систем та питань їхньої стійкості.
- > **Розробіть стратегію аналізу:** Стратегія аналізу може допомогти визначити, як інформація буде використовуватися для підтримки цілей планування, а також які ресурси та методи будуть залучені до процесу планування.

ДЛЯ ЦЬОГО ІСНУЄ РЕСУРС!

Збір даних - Зразок переліку ресурсів

Зразковий список існуючих ресурсів містить загальний огляд потенційних довідкових ресурсів, відсортованих за власниками/створювачами ресурсів. До творців відносяться

- > Місцеві/окружні/регіональні агенції
- > Власники/оператори об'єктів критичної інфраструктури
- > Державні, племенні та територіальні органи
- > Федеральні агентства

Мета цього переліку - заохотити планувальників, які використовують систему IRPF, визначити всі попередні відповідні зусилля.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Порівняння існуючих планів розвитку громад

Система показників інтеграції планів для забезпечення стійкості - це метод оцінки планів, розроблений Департаментом науки і технологій Міністерства внутрішньої безпеки (DHS) спільно з партнером Центру передового досвіду з питань стійкості прибережних територій при Техаському університеті A&M. Система показників може допомогти громадам оцінити та скоординувати свої різноманітні плани (наприклад, транспорт, економічний розвиток, пом'якшення наслідків небезпек, управління надзвичайними ситуаціями тощо), щоб вони представляли узгоджені стратегії та працювали разом для зменшення вразливості до небезпек.

Ознайомтеся з ресурсом за цим [посиланням](#) та в розділі



1.4 СФОРМУВАТИ ГРУПУ СПІЛЬНОГО ПЛАНУВАННЯ

1.4.1 Ідентифікація учасників

Одним із підходів до включення питань стійкості критичної інфраструктури в планування є створення групи зовнішніх партнерів, які можуть надати інформацію для ширшого планування. Запрошення до участі представників груп, визначених у Таблиці 4, може забезпечити життєво важливу інформацію та перспективи, які сприятимуть плануванню та підвищенню стійкості. Співпраця є ключовим фактором і може принести переваги, зазначені на Рисунку 1.

Для цілей IRPF до зацікавлених сторін у сфері критичної інфраструктури належать партнери з громадського та приватного секторів, відповідальні за планування, проектування, розвиток, інвестування, експлуатацію та управління об'єктами і системами критичної інфраструктури. До них відносяться виборні посадові особи, лідери громад, планувальники, інженери, працівники громадських робіт, персонал з управління в надзвичайних ситуаціях, власники бізнесу та оператори інфраструктури. Партнери з ключових секторів можуть надавати оперативну інформацію про свої інфраструктурні системи, яка може допомогти виявити виклики стійкості та варіанти вдосконалення стратегій стійкості.

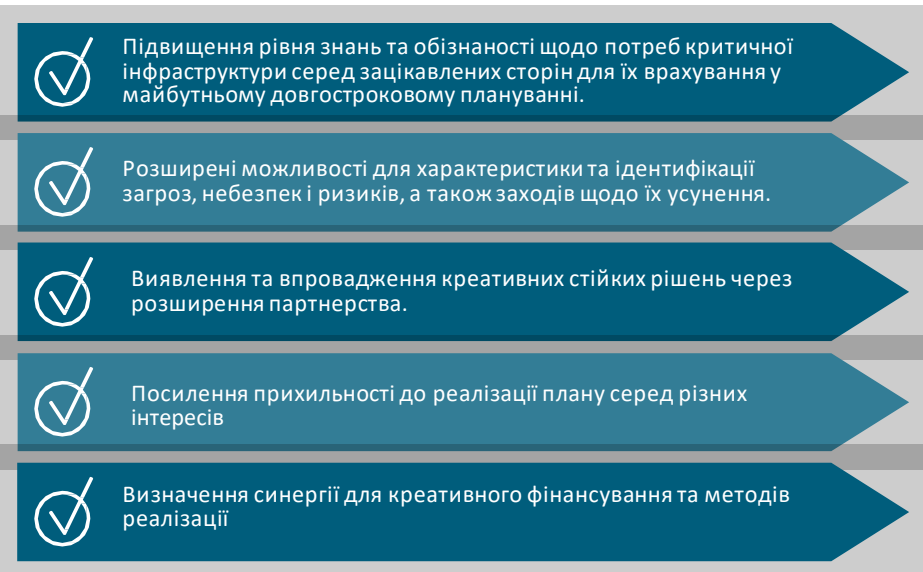


Рисунок 1. Результати ефективної співпраці

Таблиця 4. Потенційні учасники групи планування

ПОТЕНЦІЙНІ УЧАСНИКИ		
КЛЮЧОВІ СЕКТОРИ		
Комунікації	Співробітники з інформаційних технологій/безпеки для кожного суб'єкта сектору зв'язку Мережеві послуги на основі IP Провайдери супутникових послуг	Державні та місцеві департаменти громадської безпеки / управління з надзвичайних ситуацій Координатори загальнодержавної оперативної сумісності (SWIC) Провайдери телекомунікаційних послуг
Енергія	Інженер з електроенергетики та кооперативи Постачальник системи розподілу електроенергії Представники генерації електроенергії	Співробітники з інформаційних технологій/безпеки для кожного суб'єкта енергетичного сектору Дистриб'ютор рідкого палива
Транспортування	Інженери-мостобудівники Співробітники з інформаційних технологій/безпеки для кожного суб'єкта транспортного сектору Адміністрація портів/ аеропортів Органи влади/постачальники послуг громадського транспорту	Представники залізниці Регіональні транспортні органи/планувальники Державні та окружні департаменти транспорту Інженери дорожнього руху
Вода та стічні води	Співробітники з інформаційних технологій/безпеки для кожного суб'єкта сектору водопостачання/водовідведення Постачальники питної води Спеціальні комунальні райони	Зливова каналізація Оператори станцій/систем очищення стічних вод Водне управління
УРЯД ТА ІНШІ		
Будівлі та об'єкти життєзабезпечення	Власники будівель Будівельні компанії Менеджери критично важливих об'єктів	Розробники Представники лікарень та медичних закладів Місцеві керівники підприємств галузі
Міські/районні органи влади	Співробітники будівельних департаментів Міські менеджери Міські планувальники Персонал агенції економічного розвитку Виборні посадові особи	Управління в надзвичайних ситуаціях Департамент охорони здоров'я Правоохоронні органи Юридична або загальна рада Співробітники відділу громадських робіт
Регіональні/державні органи влади	Управління надзвичайними ситуаціями на державному/плеємінному/територіальному рівні Агентства з питань якості навколишнього середовища Відділи охорони здоров'я	Комісія з комунальних послуг Регіональна/міська агенція з планування
Федеральні агентства	CISA Міністерство енергетики (DOE) Міністерство охорони здоров'я та соціальних служб (HHS) Міністерство житлового будівництва та міського розвитку (HUD)	Міністерство транспорту (DOT) Агентство з охорони навколишнього середовища (EPA) FEMA Інженерний корпус армії США

Участь мають брати представники постачальників послуг, у тому числі енергетики, зв'язку, транспорту, водопостачання та водовідведення, а також представники громадськості, які можуть надати інформацію про об'єкти критичної інфраструктури, що мають важливе значення для нормального функціонування громади.

Представники федеральних, штатних, плеємінних і територіальних державних установ можуть надати цінні дані та інформацію, які будуть корисними при зборі та аналізі наявних даних, планів, досліджень і картографічних ресурсів; визначенні застосовних передових практик; а також при визначенні технічної допомоги та підтримки у впровадженні.

Крім того, їхня участь може забезпечити політичну підтримку. Якщо ці представники не можуть брати активної участі, громади можуть зв'язуватися з ними за потреби і надавати періодичну інформацію протягом усього процесу планування.

Кібербезпека також повинна враховуватися в процесі планування, і до участі в ньому слід запрошувати фахівців з інформаційних технологій/безпеки або експертів, які розуміють взаємозв'язок кіберінфраструктури з фізичною інфраструктурою. Інфраструктурні системи та об'єкти все більше покладаються на промислові системи управління та автоматизовані системи, які потребують знань з кібербезпеки для прийняття рішень щодо планування та інвестицій.

У процесі планування слід враховувати бізнес-ризик, щоб можна було врахувати залежність від критично важливих навичок, імпорту та інших ланцюгів постачання, які є важливими для довгострокової стійкості громади. Це може включати обговорення з операторами критичної інфраструктури та ключовими підприємствами.

Проактивний пошук шляхів диверсифікації джерел постачання дозволить громаді бути більш адаптивною до змін глобальних, національних чи місцевих економічних умов. У листопаді 2020 року Консультативний комітет з питань національної безпеки опублікував [звіт](#), в якому задокументовано, як бізнес-ризик можуть впливати на стійкість.

Важливо зазначити, що не всі учасники будуть залучені до всіх етапів процесу планування. Користувачам слід розглянути, коли участь буде найбільш цінною, щоб уникнути надмірного навантаження на зовнішніх партнерів і забезпечити ефективний збір відповідної інформації. Окрім активних учасників групи планування, до процесу можуть бути залучені й інші зацікавлені сторони. Стейкхолдери - це особи або групи осіб, на яких впливає інфраструктура громади, які залежать від неї та взаємодіють з нею.

Ці зацікавлені сторони повинні бути залучені, щоб отримати підтримку процесу планування та кінцевих результатів. Однак, на відміну від учасників,

Зацікавлені сторони можуть бути залучені не на всіх етапах процесу планування, але вони надають цінну інформацію з певної теми або інформацію з різних точок зору громади. До зацікавлених сторін можуть належати

- > Місцевий бізнес та представники промисловості
- > Власники та оператори систем критичної інфраструктури
- > Представники соціальних інститутів громади (наприклад, громадські організації, неурядові організації, бізнес/промислові групи, заклади охорони здоров'я, освіти, охорони довкілля тощо).
- > Зацікавлені громадяни громади

Керівник групи планування може скласти список розсилки/розсилки для цих інших зацікавлених сторін, щоб періодично інформувати їх про хід і результати процесу планування та надавати їм можливість висловити свою думку/відгук. Керівник групи планування може також проводити інтерв'ю з конкретними зацікавленими сторонами або групами зацікавлених сторін для збору інформації на етапах ідентифікації критичної інфраструктури, оцінки ризиків та розробки заходів.

ДЛЯ ЦЬОГО Є РЕСУРС!

Лист з контактною інформацією учасника планування

Ця електронна таблиця надає посадовим особам, які займаються плануванням, місце для відстеження контактної інформації різних зацікавлених сторін (включаючи контактні особи, номери телефонів, адреси електронної пошти тощо). Ці зацікавлені сторони відсортовані за типами відомств/секторів.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

1.4.2 Запросіть до участі та отримайте зобов'язання

Після визначення потенційних учасників і збору відповідної контактної інформації, керівник групи планування повинен запросити їх до участі.

Зацікавлені сторони, особливо багато з них у приватному секторі, можуть спочатку неохоче брати участь у плануванні. Це може бути пов'язано з низкою причин, зокрема

- > Занепокоєння щодо потенційного регулювання
- > Бізнес-чутливість та занепокоєння щодо обміну комерційною інформацією
- > Конкуруючі точки зору конкурентів або інших ключових партнерів

У спілкуванні з партнерами з приватного сектору часто важливо підкреслити переваги покращеного планування для учасників. До них відносяться більш швидке та ефективне реагування і відновлення як для їхнього бізнесу, так і для клієнтської бази, потенційна економія на страхуванні та зниження витрат, пов'язаних з ліквідацією наслідків катастроф, покращення заходів з пом'якшення наслідків, які можуть бути спрямовані на підвищення стійкості їхніх залежностей у верхній та нижній течії, а також можливість краще зрозуміти пріоритети громади завдяки плануванню.

ДЛЯ ЦЬОГО Є РЕСУРС!



Лист-запрошення для зацікавлених сторін

Цей зразок листа надає керівнику проекту та/або керівнику групи планування приклад змісту для використання при запрошенні та заохоченні до участі в процесі планування. Можна використовувати весь текст або окремі його частини так, як це найкраще підходить для різних типів зацікавлених сторін, яких ви запрошуєте.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

1.5 ВИЗНАЧИТИ ЦІЛІ ТА ЗАВДАННЯ

Постановка чітких цілей і завдань є важливою основою для будь-якого успішного планування, оскільки вона визначає і підтримує бачення громади щодо того, "куди вона хоче йти" або "що вона хоче робити" стосовно безпеки і стійкості критичної інфраструктури. Рекомендується, щоб керівник групи планування визначив початкові цілі та завдання на основі цілей високого рівня, визначених лідером проекту, а також на основі аналізу інших планів громади.

Розробка цілей і завдань повинна включати весь спектр факторів планування, які стосуються систем критичної інфраструктури, а також інших результатів діяльності громади, таких як якість життя, сталість, економіка, навколишнє середовище та справедливість. Важливо враховувати цілі громади

а також для економічної безпеки та стійкості. Стала зайнятість та продуктивна місцева економіка є фундаментальними ресурсами для підтримки місцевої влади та збереження життєздатних інфраструктурних ресурсів.

Початкові цілі та завдання можуть бути високого рівня. Після виконання [Кроку 2 "Ідентифікація критичної інфраструктури"](#) можна внести корективи в ці цілі та завдання, щоб зробити їх більш конкретними для тієї критичної інфраструктури, яку визначила група. Обов'язково перевірте ці оновлені цілі з лідером проекту. Ці цілі та завдання також можуть бути доопрацьовані на пізніших етапах процесу планування IRPF (наприклад, паралельно з розробкою плану дій на [Кроці 4](#)).

Під час ітеративного процесу планування громаді можуть стати доступними нові дані, факти та інформація, і тоді цілі та завдання можуть бути відповідно скориговані. Учасники/-ці зацікавлені сторони матимуть можливість підтвердити та уточнити цілі та завдання на основі висновків та визначень, отриманих на етапах [ідентифікації критичної інфраструктури](#) та [оцінки ризиків IRPF](#).

ВИЗНАЧЕННЯ ЦІЛІ ТА ЗАВДАНЬ



Цілі - це широкі твердження, які описують бажаний кінцевий стан, те, чого прагне досягти громада, впроваджуючи рішення щодо забезпечення стійкості критично важливої інфраструктури.

Завдання - це конкретні, вимірювані твердження, які сприяють досягненню цілі.

ДЛЯ ЦЬОГО Є РЕСУРС!



Приклади цілей та завдань

Цей шаблон списку містить приклади цілей, якими можна керуватися при обговоренні стійкості інфраструктури.

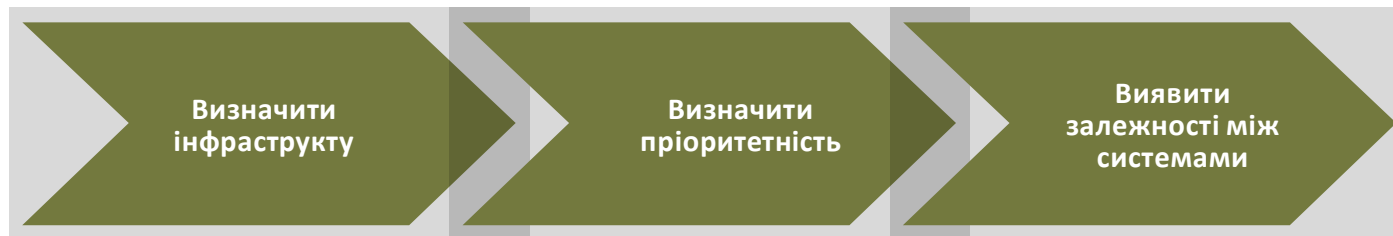
Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

2. Ідентифікація критичної інфраструктури

У цьому розділі розглядається наступне:

1. [ВИЗНАЧИТИ ІНФРАСТРУКТУРУ](#)
2. [ВИЗНАЧИТИ ПРІОРИТЕТНІСТЬ ІНФРАСТРУКТУРИ](#)
3. [ВИЯВИТИ ЗАЛЕЖНОСТІ](#)

2. Ідентифікація критичної інфраструктури



Крок 2 включає визначення та встановлення пріоритетів критично важливої інфраструктури в громаді та взаємозалежності між інфраструктурними системами.

2.1 ВИЗНАЧИТИ ІНФРАСТРУКТУРУ

Під час планування важливо визначити інфраструктурні системи та активи, які є критично важливими для нормального функціонування громади чи регіону.

Сюди слід віднести такі фундаментальні системи, як енергетика, водопостачання та водовідведення, зв'язок і транспорт, а також інфраструктуру, яка має вирішальне значення для безпеки, здоров'я та економічної життєздатності громади. На додаток до цих секторів, NIST CRPG також визначає низку соціальних функцій, які сприяють процвітанню громади, зокрема: Громадські роботи, економіка, освіта, сім'я, уряд, охорона здоров'я, засоби масової інформації, релігійні та культурні переконання.

Кожна з цих функцій включає власний набір систем критичної інфраструктури - від лікарень і будинків престарілих до шкіл і церков, підприємств і громадських центрів. Працюючи над визначенням систем критичної інфраструктури у вашій громаді, вам слід подумати, які об'єкти та системи підтримують ці суспільні функції.

ДОДАТКОВІ МІРКУВАННЯ ЩОДО ВИЗНАЧЕННЯ ІНФРАСТРУКТУРИ



- > Майбутні системи та активи критичної інфраструктури, які плануються або передбачаються для підтримки потенційного майбутнього розвитку громади.
- > Інфраструктура, розташована в межах і за межами відповідних географічних районів, але забезпечує життєво важливі послуги для громади (наприклад, лінії електропередач і трубопроводи).
- > Об'єкти критичної інфраструктури, системи або мережі, розташовані в межах громади, які можуть не надавати прямих послуг населенню, не є критично важливими для громади як такої, але є критично важливими для регіону чи країни в цілому.

Групи планування повинні розглянути можливість створення бази даних/матриці з переліком об'єктів критичної інфраструктури громади, щоб допомогти каталогізувати та проаналізувати інфраструктурні активи. Окрім того, що це може слугувати джерелом інформації для створення

Для визначення залежностей між інфраструктурою громади можна використовувати базову інвентаризацію інфраструктури:

- > Описати характеристики існуючої інфраструктури
- > Сформувати основу для більш комплексних зусиль з ідентифікації інфраструктури

> Розробляти картографічні продукти та інші візуалізації

Збираючи інформацію про системи та об'єкти критичної інфраструктури у вашій громаді, ви можете вводити її в місцеві та регіональні геопросторові платформи, що дасть змогу візуалізувати її та проводити додатковий аналіз.

ДЛЯ ЦЬОГО Є РЕСУРС!



Матриця інфраструктурних активів: Посібник із запропонованих полів даних

У цьому Посібнику наведено запропоновані поля даних для включення до бази даних/матриці, а також опис та ключові міркування щодо збору інформації про об'єкти інфраструктури.

Заповнення всіх запропонованих полів даних допоможе полегшити проведення аналізів, які громада, можливо, захоче провести в майбутньому за підтримки федерального бюджету. Однак поля даних можуть бути змінені, щоб найкраще відповідати потребам учасників/зацікавлених сторін та громади у зборі інформації.

Переглянути [ресурс](#) у розділі [Планування стійкості інфраструктури](#).

Набори даних для ідентифікації інфраструктури

У цьому документі представлені різні набори даних для вивчення, відсортовані за категоріями (зв'язок, енергетика, транспорт, вода, інше, безпеки).

Переглянути [ресурс](#) у розділі [Планування стійкості інфраструктури](#).

2.1.1 Визначення кіберінфраструктури

Громади повинні розуміти свою залежність від інформаційних технологій і систем зв'язку, необхідних для експлуатації та моніторингу критично важливої інфраструктури, а також для підтримки ключових соціально-економічних функцій, таких як надання основних державних послуг і забезпечення безперебійної роботи.

Кіберінфраструктура має важливе значення для експлуатації та обслуговування об'єктів критичної інфраструктури, таких як електростанції, водопостачання та водовідведення об'єкти, лікарні, телекомунікаційні системи, нафто- і газопереробні заводи та транспортні мережі. Через взаємозв'язок фізичної та кіберінфраструктури фахівці з громадського планування та зацікавлені сторони, які беруть участь у процесі планування, повинні мати уявлення про активи кіберінфраструктури, системи та мережі кібербезпеки, які підтримують і забезпечують безперервну роботу інфраструктурних систем.

Кіберінфраструктура включає в себе широкий спектр систем, які слід враховувати, наприклад, такі:

- > Комп'ютерні системи;
- > Системи управління, що використовуються для моніторингу та управління заводом або обладнанням (наприклад, диспетчерське управління та збір даних (SCADA));
- > Мережі, такі як Інтернет;
- > Кібер-послуги (наприклад, керовані послуги безпеки);
- > Системи зберігання та обробки даних, включаючи мейнфрейми, хмарні провайдери, серверні ферми, дата-центри;
- > Апаратне та програмне забезпечення, яке обробляє, зберігає та передає інформацію, або будь-яка комбінація цих елементів в електронних інформаційно-комунікаційних системах; та
- > Дані та інформація в електронних інформаційно-комунікаційних системах.

Розглядаючи кіберінфраструктуру, планувальникам важливо враховувати такі фактори, як вік, походження, технічне обслуговування та місцезнаходження віддалених постачальників послуг, щоб визначити весь спектр викликів для стійкості громади.

2.2 ВИЗНАЧИТИ ПРІОРИТЕТНІСТЬ ІНФРАСТРУКТУРИ

Склавши перелік об'єктів критичної інфраструктури в громаді, керівник групи планування або призначений фасилітатор має очолити групу планування у визначенні пріоритетності визначених об'єктів інфраструктури. Рекомендується, щоб група планування зосередилася на впливі, який кожна система/об'єкт критичної інфраструктури має на громаду, щоб визначити їхню критичність та пріоритетність. У Таблиці 5 наведено ключові впливи, які слід враховувати. Вони можуть бути використані як критерії для визначення пріоритетності визначених об'єктів критичної інфраструктури.

Громади можуть вирішити використовувати всі ключові міркування, перелічені в Таблиці 5, як критерії або просто вибрати ті, які є найбільш прийнятними для їхніх громад. Крім того, громади можуть змінювати ключові міркування або додавати власні критерії, які найкраще відповідають їхнім потребам.

Таблиця 5. Ключові міркування щодо визначення пріоритетності інфраструктурних систем/активів

КЛЮЧ МІРКУВАННЯ	ОПИС
Вплив на безпеку	Вплив системи/об'єкта на людські жертви, добробут людей у громаді, навколишнє середовище та фізичний стан інших інфраструктурних систем/об'єктів
Контекст	Цінність системи / активу для ідентичності громади, регіону або нації; важливість системи / активу як пріоритетного атрибуту громади, регіону або нації (наприклад, основна галузь, ідентифікаційна ознака, культурний символ тощо).
Операційний вплив	Вплив системи/об'єкта на загальну здатність мережі працювати; функціональний вплив системи/об'єкта, пов'язаний із залежностями, що існують всередині та між системами/об'єктами.
Економічний вплив	Потенційний вплив на економічну безпеку населеного пункту, регіону або країни, якщо ця інфраструктура зазнає довготривалого руйнування або деградації
Вплив на обслуговування	Вплив порушення роботи системи/об'єкта на громаду, регіон або більшу систему критичної інфраструктури на основі послуг, які вона надає цим суб'єктам

2.3 ВИЯВЛЕННЯ ЗАЛЕЖНОСТЕЙ МІЖ ІНФРАСТРУКТУРНИМИ СИСТЕМАМИ

Національний план захисту інфраструктури (НПЗІ)³ стверджує, що "ефективне управління ризиками вимагає розуміння критичності активів, систем і мереж, а також пов'язаних з ними залежностей критичної інфраструктури, що має важливе значення для посилення безпеки та стійкості критичної інфраструктури".

Залежності - це відносини довіри всередині та між інфраструктурними системами, які необхідно підтримувати для того, щоб ці системи могли функціонувати або надавати послуги.⁴ Залежності мають мультиплікативний ефект, оскільки загроза або небезпека може призвести до втрати послуг (наприклад, відключення електроенергії), що може вплинути на інші об'єкти критичної інфраструктури, які використовують ці ресурси, що в подальшому вплине на інші об'єкти критичної інфраструктури, які залежать від цих ресурсів, і, як наслідок, на безпеку та стійкість на них. Вплив на один вузол або лінію зв'язку може призвести до значних економічних і фізичних збитків у масштабах міста, регіону та країни.⁵ Покращене розуміння залежностей, особливо для ключових інфраструктурних систем, може стати основою для оцінки ризиків і призвести до визначення нових пріоритетів для підвищення стійкості.

Для того, щоб визначити залежності між інфраструктурними системами, учасники повинні розглянути:

- > **Первинні та вторинні джерела/постачальники ресурсів та послуг, необхідних для функціонування інфраструктурного об'єкта.** Наприклад, при розгляді енергетичної залежності інфраструктурного об'єкта, громада має визначити, хто є постачальником послуг з розподілу електроенергії та де розташовані основні та допоміжні підстанції для інфраструктурного об'єкта.
- > **Резервні джерела ресурсів для підтримання роботи об'єкта інфраструктури у випадку руйнівної події.** Наприклад, розглядаючи залежність об'єкта інфраструктури від енерго- та водопостачання, громада має визначити резервні генератори на місці та ємності для зберігання води на місці на випадок значних інцидентів або змін у ланцюгах постачання.
- > **Вплив на інфраструктурні активи та основні послуги, що знаходяться нижче за течією, у разі порушення або деградації.** Наприклад, відключення електроенергії може зупинити роботу об'єктів водопостачання/водовідведення, оскільки насоси не зможуть працювати, а кібернетичні та інформаційні системи не зможуть здійснювати моніторинг операцій.

У Таблиці 6 наведено приклади залежностей, які є поширеними серед систем критичної інфраструктури.

Таблиця 6. Приклади типових залежностей

ПРИКЛАДИ ЗАЛЕЖНОСТЕЙ

Системи питної води потребують електроенергії для роботи насосів

Фінансові послуги покладаються на комунікації для полегшення транзакцій, а комунікаційні системи потребують енергії для роботи

Бригади, які ремонтують системи розподілу електроенергії, потребують доступу до доріг

Надання екстрених послуг залежить від комунікацій та доріг

Інфраструктура кібер- та інформаційних технологій використовується для експлуатації та моніторингу енергетичних систем, систем водопостачання/водовідведення, транспортних мереж тощо.

Потреба у стабільному постачанні сировини, товарів і послуг, а також робочої сили для функціонування підприємств та інфраструктури

ЗВЕРНІТЬ УВАГУ



Деякі постачальники послуг (наприклад, енергетики та зв'язку) можуть вагатися, чи надавати інформацію про системні залежності в не можна говорити в групі з міркувань безпеки та відповідальності за обмін інформацією. Кілька підходів до виявлення взаємозалежності від життєво важливих зв'язків представлені в дискусії, інтерв'ю та робочих таблицях для виявлення залежності, які допоможуть врахувати цю обставину.

Перегляньте ресурси в розділі [Ресурси планування стійкості інфраструктури](#).

ДЛЯ ЦЬОГО ІСНУЄ РЕСУРС!



Посібник з інфраструктурної залежності

Цей посібник - це інформаційний веб-ресурс, який забезпечує основу для розуміння критично важливої інфраструктури, виявлення залежностей та їхнього впливу на ризики для громад, а також використання цих знань у плануванні заходів з підвищення стійкості.

Онлайн-праймер знаходиться у відкритому доступі на сайті <https://www.cisa.gov/idp>.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#)

Робочий аркуш ідентифікації залежностей

Робочий аркуш ідентифікації залежностей може допомогти в документуванні залежностей інфраструктури громади від інших визначених об'єктів критичної інфраструктури.

Робочий аркуш для виявлення залежностей допомагає громадам відповісти на низку запитань щодо залежностей інфраструктурних об'єктів, зосереджуючись на енергетиці (включаючи електроенергію та природний газ), а також на питаннях, пов'язаних з газ), послуги зв'язку, доступ до ключових транспортних систем, водопостачання та водовідведення. Додаткові питання в Таблиці ідентифікації залежностей включають кібернетичні міркування, такі як системи та послуги з обробки даних, а також розгляд критично важливих продуктів, необхідних для функціонування/операцій, таких як хімічні речовини, паливо, сировина та видалення побічних продуктів і відходів.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Посібник для обговорення залежності від систем спільнот

Цей посібник можна використовувати для полегшення обговорення питань залежності з групою планування, іншими учасниками або групами зацікавлених сторін. Посібник містить перелік запитань, які допоможуть розпочати розмову та визначити критичні функції громади та/або залежність об'єктів від інфраструктурних систем.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#)

ДЛЯ ЦЬОГО Є РЕСУРС!



Посібник для проведення співбесіди з власником системи/ оператором щодо залежності

Цей посібник містить низку запитань, які можна використовувати для проведення індивідуальних інтерв'ю з власниками та/або операторами систем критичної інфраструктури. Запитання допоможуть визначити та зрозуміти залежність системи та її здатність надавати послуги під час аварійних подій.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Посібник з фасилітації зустрічей

Цей посібник може бути використаний для проведення зустрічі з учасниками планування з метою визначення функцій громади, об'єктів, інфраструктурних систем та взаємозалежностей, які є найбільш важливими для забезпечення стійкості громади до надзвичайних ситуацій.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

3. Оцінка ризику

У цьому розділі розглядається наступне:

1. [ІДЕНТИФІКУВАТИ ЗАГРОЗИ ТА НЕБЕЗПЕКИ](#)
2. [ОЦІНИТИ ВРАЗЛИВІСТЬ](#)
3. [ОЦІНИТИ НАСЛІДКИ](#)
4. [ІНФРАСТРУКТУРНІ СИСТЕМНІ РИЗИКИ](#)

3. Оцінка ризику



Етап оцінки ризиків - це процес, під час якого збирається інформація та присвоюються значення ризикам з метою визначення пріоритетів, розробки та порівняння планів дій, а також прийняття рішень. Зацікавлені сторони критичної інфраструктури використовують широкий спектр методологій оцінки ризиків, щоб зрозуміти найбільш ймовірні та серйозні інциденти, які можуть вплинути на інфраструктурні активи, системи та мережі. Інформація, отримана в результаті оцінки, використовується для підтримки заходів з планування та розподілу ресурсів.

Методологія оцінки ризиків, що використовується для IRPF, передбачає:

- 1) виявлення загроз і небезпек для інфраструктури,
- 2) оцінка вразливості пріоритетних об'єктів інфраструктури, аналіз наслідків та взаємодії між об'єктами інфраструктури системи та
- 4) визначення пріоритетності ризиків для інфраструктурних систем.

Після завершення оцінки ризиків буде розроблено та впроваджено заходи розробки та імплементації заходів.

При оцінці ризиків для критичної інфраструктури часто використовують гіпотетичні ситуації або сценарії, щоб розділити виявлені ризики на компоненти, які можна оцінити та проаналізувати окремо. Ці ситуації або сценарії складаються з ідентифікованої загрози або небезпеки, об'єкта, на який впливає ця загроза або небезпека, і пов'язаних з нею умов, включаючи вразливості та наслідки.

РОЗУМІННЯ РИЗИКУ*.



Ризик у контексті національної безпеки визначається як потенційна можливість небажаного результату в результаті інциденту, події або

Стійкість - це здатність організації протистояти певній події, яка визначається її ймовірністю (функцією загроз і вразливостей) та пов'язаними з нею наслідками. Стійкість є частиною рівняння ризику, оскільки вона може впливати на вразливість (або схильність) організації до різних загроз і небезпек, а також на наслідки, які можуть виникнути в результаті події. Зрештою, процес аналізу ризику є важливим, оскільки він формує прийняття рішень щодо способи управління ризиком шляхом його прийняття, уникнення, передачі або контролю до прийнятного рівня за прийнятну ціну. Таким чином, стійкість є фундаментальною частиною ширшої стратегії управління ризиками в громаді.⁶

Загроза: Природне, техногенне або технологічне явище, особа, організація або дія, що має або вказує на потенційну можливість завдати шкоди життю, інформації, операціям, навколишньому середовищу та/або майну.

Вразливість: Характеристика дизайну, розташування, стану безпеки, функціонування або будь-якої їх комбінації, яка робить об'єкт, актив, систему, мережу або географічну територію вразливими до підризу, знищення або використання.

Наслідок (або вплив): Вплив інциденту, події чи явища, прямий чи опосередкований.

*Національний план захисту інфраструктури

3.1 ВИЯВЛЯТИ ЗАГРОЗИ ТА НЕБЕЗПЕКИ ДЛЯ ІНФРАСТРУКТУРИ

Існує безліч загроз і небезпек, на які можуть наражатися інфраструктурні системи/об'єкти. У Таблиці 7 визначено потенційні природні, навмисні та випадкові загрози і небезпеки, які слід розглянути на предмет їхньої актуальності та застосовності до пріоритетних об'єктів критичної інфраструктури в майбутньому.

Таблиця 7. Приклади загроз та небезпек за категоріями

НАТУРАЛЬНИЙ	ВИПАДОК	ОБДУМОВАНО
Лавина	Авіакатастрофа	Збройний напад
Посуха	Кіберінцидент	Підпал/запалювальний напад
Землетрус	Аварія на дамбі	Біологічний
Екстремальний холод	Викид небезпечних речовин	агент Хімічний агент
Екстремальна спека	Промислова аварія	Громадянські заворушення
Повінь	Аварія на дамбі	Звичайна бомба/саморобний вибуховий пристрій
Ураган	Аварія на шахті	Кіберінцидент
Зараження комахами	Зсуви	Перешкоди в радіочастотному спектрі
Зсуви	Пандемії	Диверсія з використанням радіоактивних речовин
Торнадо	Цунамі	Крадіжка
Торнадо	Виверження вулкану	
Лісова пожежа	Лісова пожежа	
Зимовий шторм	Зимовий шторм	

**Випадкові небезпеки можуть бути окремими інцидентами або результатом навмисної загрози чи стихійного лиха.*

Хоча можна врахувати всі небезпеки та загрози, громадам, можливо, варто оцінити ймовірність виникнення кожної з них, щоб визначити ті, які потребують подальшої оцінки ризику. Ймовірність небезпеки може

визначатися на основі визначених коефіцієнтів повторюваності небезпеки, частоти зафіксованих історичних подій або об'єктивних оцінок. Джерела інформації для визначення ймовірності загрози/небезпеки визначені в Розділі 3.1.1 і включають федеральні, державні, місцеві, племенні або територіальні органи, а також коледжі та університети. Ще одним цінним джерелом інформації про небезпеку є досвід та історичні знання учасників планування та зацікавлених сторін. Хоча доцільно визначати пріоритетність загроз/небезпек, які є найбільш вірогідними та ймовірними, можна оцінити всі небезпеки, якщо дозволяють час і ресурси.

ЗВЕРНІТЬ УВАГУ



Важливо визнати, що вплив загрози/небезпеки буде змінюватися з часом, а тип, частота і масштаби впливів можуть відрізнятися від попереднього досвіду. Такі фактори, як клімат, соціальні Політичні та економічні умови, антропогенне середовище і технології є динамічними, і їх слід врахувати при розробці описів контексту загроз і небезпек. Врахування майбутніх умов дасть змогу розробити надійні та стійкі інфраструктурні рішення, які можуть змінити ландшафт ризиків.

3.1.1 Джерела інформації про загрози та небезпеки

Джерела інформації про загрози та небезпеки включають

- > Національні онлайн-ресурси, пов'язані з погодою, такі як Національний центр кліматичних даних та База даних про події та збитки, пов'язані з просторовими небезпеками, для США (SHELDUS)
- > Місцеві або регіональні відділення Національної метеорологічної служби
- > Місцеві ресурси, такі як газети, торговельна палата, місцеве історичне товариство або інші ресурси, що містять записи про минулі події.
- > Історія оголошення стихійних лих на федеральному рівні та на рівні штатів
- > Регіональні представництва FEMA

- > Відомства з надзвичайних ситуацій/національної безпеки
- > Регіональні радники CISA з питань захисної безпеки
- > Регіональні радники CISA з питань кібербезпеки
- > Регіональні радники Міжвідомчого комітету з питань безпеки CISA
- > Хімічні інспектори CISA
- > Координатори комунікацій у надзвичайних ситуаціях CISA
- > Команда комп'ютерної готовності до надзвичайних ситуацій США (US-CERT)
- > Команда реагування на кібернетичні надзвичайні ситуації в промислових системах управління (ICS-CERT)
- > Офіси зменшення небезпеки SLTT
- > Центри злиття штатів і великих міських районів
- > Племінні уряди
- > Коледжі/університети та інші дослідницькі організації, які мають програми, пов'язані із загрозами та небезпеками, або консультаційні служби

ДЛЯ ЦЬОГО Є РЕСУРС!

Інформаційні та аналітичні ресурси про небезпеку

Надає зовнішні посилання на інформацію про небезпеку та аналітичні ресурси, включаючи дані про одну або декілька небезпек, а також інструменти для моделювання та аналізу. Включає посилання на федеральні програми, такі як NOAA, USGS, NIFC та інші.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Посуха та інфраструктура: Посібник з планування

Цей посібник, розроблений CISA спільно з Національним партнерством зі стійкості до посух, містить огляд небезпеки посух, приклади прямих і непрямих впливів, які вони можуть мати на інфраструктурні системи, а також інформацію про федеральні ресурси для оцінки та пом'якшення ризиків посух.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

3.1.2 Облік кіберзагроз

Сфера кіберпростору та її базова інфраструктура вразливі до широкого спектру ризиків, що виникають як через фізичні, так і через кіберзагрози та небезпеки. Крім того, системи фізичної інфраструктури все частіше включають автоматизовані системи управління, які піддаються ризику тих самих кіберзагроз. Зловмисники намагаються використати вразливості для крадіжки інформації або грошей, а також для порушення, знищення або загрози наданню основних послуг.

Суб'єкти кіберзагрози можуть бути різними:

- > Хакери
- > Організована злочинність
- > Терористичні угруповання
- > Державні спонсоровані / іноземні розвідувальні служби

Типи кібератак можуть бути наступними:

- > Атака на веб-додатки
 - Ін'єкція SQL
 - Міжсайтовий скриптинг
- > Фішинг
- > Розсилка спаму
- > Атаки на специфічні додатки
- > Просунуті постійні загрози
 - Рекламне ПЗ
 - Бот
 - Програми-вимагачі
 - Руткіт
 - Шпигунське програмне забезпечення
 - Троянський кінь
 - Вірус
 - Черв'як.
- > Розподілена відмова в обслуговуванні (DDoS) та відмова в обслуговуванні (DoS)

3.2 ОЦІНИТИ ВРАЗЛИВІСТЬ ІНФРАСТРУКТУРИ

Учасники/зацікавлені сторони повинні оцінити вразливість пріоритетної інфраструктури громади до виявлених загроз/небезпек. Оцінка вразливості передбачає оцінку конкретних загроз і небезпек для інфраструктури з метою виявлення слабких місць, які можуть призвести до наслідків, що викликають занепокоєння.

Оцінка вразливості може допомогти у розробці рішень щодо забезпечення стійкості, визначаючи внутрішні та зовнішні фактори, які можуть бути використані зловмисниками або на які можуть вплинути загрози та потенційні точки відмови. Виявлення проблемних заяв допомагає в розробці заходів для посилення безпеки та стійкості. Ключовими елементами вразливості, які слід враховувати під час оцінювання, є

- > **Доступність:** вразливість об'єкта інфраструктури, що ґрунтується на його загальній доступності для громадськості.
- > **Впізнаваність:** вразливість об'єкта інфраструктури залежить від того, наскільки легко він може бути впізнаним для громадськості.
- > **Відновлюваність:** здатність інфраструктурного об'єкта легко відновлюватися після руйнівної події; якісна оцінка здатності об'єкта повернутися до нормальної роботи, беручи до уваги його залежність від зовнішніх послуг, потужність, на якій він працює, і його власну надійність.
- > **Сприйнятливість:** загальна вразливість, що базується на заходах і процедурах безпеки, які діють на об'єкті інфраструктури.
- > **Близькість:** вразливість, що базується на близькості активу до інших вразливих активів.
- > **Надмірність:** вразливість, що базується на тому, чи є актив єдиною точкою відмови в загальній системі, чи ні.

3.3 ОЦІНИТИ НАСЛІДКИ ДЛЯ ІНФРАСТРУКТУРНИХ СИСТЕМ

Після визначення загроз і небезпек учасники/зацікавлені сторони повинні розглянути ймовірні наслідки цих небезпек, щоб визначити пріоритети для критичної інфраструктури. Наслідки - це ефект події, інциденту або явища, який зазвичай вимірюється чотирма способами:

1. **Людина** (травма, хвороба або втрата життя)
2. **Економічні** (витрати, пов'язані з втратою безперервності роботи інфраструктури, та витрати на заміну)
3. **Місія** (здатність організації або групи досягати стратегічної мети або виконувати функцію)
4. **Психологічний** (психічний або емоційний стан окремих осіб або груп, що призводить до зміни сприйняття та/або поведінки)

Фактори наслідків, які слід враховувати при оцінці ризиків для інфраструктури громади, включають питання безпеки (витрати, пов'язані з втратою інфраструктури, що підтримує безпеку або оборонну місію) і додаткові змінні, які можуть призвести до того, що локальні події перетворяться на більш масштабні порушення (залежність). Для оцінки наслідків перебоїв у роботі критично важливої інфраструктури можна використовувати історичні події.

3.4 ІНФРАСТРУКТУРНІ СИСТЕМНІ РИЗИКИ

Після виявлення загроз, оцінки вразливостей і наслідків їхнього впливу їх можна об'єднати, щоб визначити ризик для пріоритетних об'єктів інфраструктури. Група планування повинна спільно порівняти кожну загрозу/небезпеку, вразливість і сценарій наслідків, щоб визначити їхню пріоритетність, виходячи з того, які з них становлять найбільший ризик.

ДЛЯ ЦЬОГО Є РЕСУРС!

Методології оцінки ризиків

Цей ресурс узагальнює різні методи аналізу ризиків і надає посилання на зовнішні ресурси для проведення аналізу ризиків.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

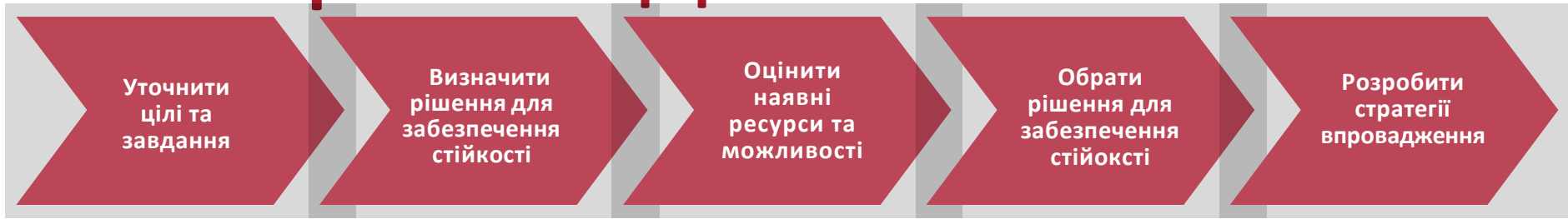


4. Розробка дій

У цьому розділі розглядається наступне:

1. УТОЧНИТИ ЦІЛІ ТА ЗАВДАННЯ
2. ВИЗНАЧИТИ РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ
3. ОЦІНИТИ НАЯВНІ РЕСУРСИ ТА МОЖЛИВОСТІ
4. ОБРАТИ РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ
5. РОЗРОБИТИ СТРАТЕГІЇ ВПРОВАДЖЕННЯ

4. Розробка дій



На цьому етапі IRPF допомагає громадам пройти процес визначення та відбору проектів і рішень для підвищення стійкості критичної інфраструктури та розробки стратегій їх реалізації.

1. УТОЧНИТИ ЦІЛІ ТА ЗАВДАННЯ

Перш ніж визначити та впроваджувати рішення щодо забезпечення стійкості, громади повинні переглянути своє бачення та уточнити свої початкові цілі та завдання щодо забезпечення стійкості критичної інфраструктури більш детально, спираючись на результати [Ідентифікації критичної інфраструктури](#) та [оцінки ризиків](#).

2. ВИЗНАЧИТИ РІШЕННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ДЛЯ ЗМЕНШЕННЯ РИЗИКІВ

Основним результатом IRPF є рішення щодо зменшення ризиків для інфраструктури громад. Рішеннями щодо підвищення стійкості можуть бути політики, стратегії, плани, кодекси та постанови, програми підвищення стійкості та/або реальні інфраструктурні проекти. Нижче наведено перелік заходів з підвищення стійкості діяльності. Він не є вичерпним, а радше пропонує можливі відправні точки.

- > **Використовуйте інструменти планування землекористування.** Громади можуть запроваджувати накладки або нові постанови про зонування, щоб обмежити розвиток інфраструктури/будівництво в зонах підвищеної небезпеки.
- > **Оновлення кодексів і стандартів.** На основі загроз, небезпек і вразливостей, виявлених у процесі оцінки ризиків, громади можуть оновити кодекси і стандарти, щоб пом'якшити найбільші з них.

ризиків для інфраструктури громади. Усі регуляторні зміни повинні включати супровідні положення щодо правозастосування.

- > **Інвестувати в надійну інфраструктуру.** Громади можуть використовувати інформацію, отриману в процесі оцінки ризиків, для визначення заходів, які зменшать вразливість ключових об'єктів інфраструктури до загроз і небезпек. Потенційні варіанти включають створення резервних сервісних потужностей, диверсифікацію сервісних мереж, диверсифікацію ланцюгів постачання, розробку гнучких систем і зменшення попиту на послуги за рахунок розумного використання ресурсів.
- > **Оновлення програм обслуговування та капітального ремонту інфраструктури.** Громади можуть використовувати перелік пріоритетних об'єктів інфраструктури громади та перелік пов'язаних з ними залежностей для визначення пріоритетів обслуговування та оновлення для постачальників послуг. Існуючі програми перевірок можна доповнити, щоб визначити інфраструктурні системи, які потребують покращення, і які можуть бути пріоритетними для технічного обслуговування.
- > **Розробіть плани безперервності та реагування на надзвичайні ситуації.** Власники та оператори об'єктів критичної інфраструктури можуть використовувати інформацію про залежності для створення винахідливих, рефлексивних і гнучких планів безперервності, які допоможуть підтримувати надання комунальних послуг об'єктам критичної інфраструктури під час надзвичайних ситуацій. Громади також можуть використовувати цю інформацію для розробки ефективних планів на випадок надзвичайних ситуацій.
- > **Включити зелену інфраструктуру.** Врахування "зеленої" інфраструктури може зменшити кліматичні ризики, підвищити енергоефективність та зменшити потребу в ресурсах, що призведе не лише до екологічних, але й до соціальних та економічних переваг.

- > **Створити Раду з питань інфраструктури.** Рада з питань інфраструктури, до складу якої входять як місцеві органи влади, так і державні та приватні власники та оператори інфраструктури, є форумом для ключових зацікавлених сторін, на якому вони можуть обговорювати такі питання та поточну діяльність і проблеми, взаємозалежності, майбутній розвиток, а також можливості для партнерства та креативного фінансування.

ДЛЯ ЦЬОГО Є РЕСУРС!

Джерела для відмовостійких рішень

Перелік джерел для пошуку ідей стійких рішень наведено в [Ресурси для планування стійкості інфраструктури](#).



РЕСУРСИ МОМ ДЛЯ ПОМ'ЯКШЕННЯ НАСЛІДКІВ СТИХІЙНИХ ЛИХ

Потенційні заходи з пом'якшення наслідків висвітлені в наступних ресурсах FEMA (розташовані в розділі "[Ресурси для заходів з пом'якшення наслідків](#)").

- > **Ідеї пом'якшення наслідків: Ресурс для зменшення ризиків природних загроз**" містить приклади заходів зі зменшення наслідків, які підвищують стійкість інфраструктури громади до різноманітних і специфічних природних загроз.
- > **Портфолію найкращих практик з пом'якшення наслідків стихійних лих** містить історії та тематичні дослідження, які дають уявлення про те, як інші громади вживали заходів для пом'якшення наслідків стихійних лих.
- > **Планування зменшення ризиків: Практика планування землекористування та забудови поблизу трубопроводів** містить огляд ризиків, пов'язаних з системами магістральних та розподільчих трубопроводів, а також стратегії пом'якшення наслідків, які можна впровадити для зменшення цих ризиків.
- > **Публікації Сектора будівельних наук** надають рекомендації щодо впровадження заходів зі зменшення наслідків різних видів небезпек та ідеї щодо заходів зі зменшення наслідків.
- > Іншим ресурсом є Портфолію дій зі зменшення наслідків FEMA, доступне для завантаження з веб-сайту Building Resilient Infrastructure and Communities (BRIC).

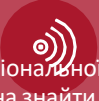


4.2.1 Врахування кібербезпеки при визначенні рішень для забезпечення стійкості

Оскільки значна частина фізичної інфраструктури громади сьогодні повністю або частково контролюється комп'ютерами і підключена до Інтернету, планування має враховувати обґрунтовану політику і процедури для включення заходів з кібербезпеки в життєвий цикл розвитку інфраструктури. Нижче наведено деякі ресурси, які допоможуть громадам розглянути кіберзагрози та вжити відповідних заходів для захисту своєї критичної інфраструктури.

РЕСУРСИ З КІБЕРБЕЗПЕКИ

- > **CISA** відповідає за підвищення безпеки, стійкості та надійності національної кібер- та комунікаційної інфраструктури. За цим посиланням можна знайти інформацію про тренінги та навчання з кібербезпеки, публікації та рекомендації CISA, оповіщення та інформаційні бюлетені, технічну допомогу, програми та послуги.
- > **CISA** пропонує широкий спектр продуктів і технічних послуг з оцінки кібербезпеки. Партнери можуть запросити проведення безкоштовних добровільних оцінок, які варіюються від самостійних опитувань до візитів на місце.
- > CISA розробляє та надає широкий спектр продуктів для обміну інформацією та підвищення обізнаності, починаючи від інформації про індикатори загроз і закінчуючи бюлетенями та рекомендаціями. CISA також спонсорує галузеві центри обміну інформацією та аналізу, а також організації з обміну інформацією та аналізу з метою сприяння обміну кіберінформацією та кращими практиками. Додаткову інформацію можна знайти за цим посиланням.
- > Рамкова концепція кібербезпеки NIST надає добровільні рекомендації, засновані на існуючих стандартах, настановах і практиках, які допомагають організаціям краще управляти питаннями кібербезпеки, знижувати ризики кібербезпеки та пом'якшувати вразливості.
- > Добровільна програма кіберспільноти CISA з питань критичної інфраструктури допомагає власникам та операторам об'єктів критичної інфраструктури узгодити наявні ресурси, щоб допомогти їм у використанні Рамкової концепції кібербезпеки та управлінні своїми кіберризиками, а також надає галузеві рекомендації та практики.



4.3 ВИЗНАЧИТИ НАЯВНІ РЕСУРСИ ТА МОЖЛИВОСТІ

План дій може включати звернення до інших державних і приватних організацій з проханням підтримати реалізацію з метою отримання взаємної вигоди від систем стійкої інфраструктури. Визначення та оцінка ресурсів і спроможності як громади, так і власників та операторів об'єктів критичної інфраструктури допоможуть громаді визначити пріоритетність переліку рішень щодо забезпечення стійкості для впровадження.

На Рисунок 2 показано деякі з найпоширеніших типів наявних ресурсів та можливостей, які слід враховувати при визначенні пріоритетності рішень щодо ідентифікації.

	Органи планування та регулювання	Громада часто зобов'язана дотримуватися або забезпечувати їх виконання для забезпечення громадської безпеки, дотримання екологічних стандартів тощо. Наприклад, постанови, кодекси тощо.
	Наявні плани, політики та програми	Можуть бути використані як інструменти для включення нових рішень з підвищення стійкості та прискорення впровадження, якщо вони узгоджуються з цілями та завданнями або планами, політиками та програмами. Наприклад, комплексні плани, плани капітального ремонту
	Адміністративні та технічні навички в громаді	Знання наявних можливостей у громаді допомагає визначити, чи потрібні додаткові навички або досвід для впровадження рішень щодо забезпечення стійкості, і якщо так, то які саме.
	Фінансові ресурси	Знати наявні фінансові можливості та ресурси, які існують для управління та визначення пріоритетів у плануванні, щоб визначити, яке потенційне зовнішнє фінансування знадобиться для реалізації рішень з підвищення стійкості. Наприклад, гранти, плата за вплив тощо.

Рисунок 2. Поширені типи спроможностей громади

ДЛЯ ЦЬОГО Є РЕСУРС!

Зразок робочого аркуша з оцінки спроможності



Зразок робочого аркуша з оцінкою потенціалу надається для того, щоб допомогти громаді оцінити наявні ресурси та можливості. Зразок таблиці спроможностей може бути переглянутий громадою відповідно до її потреб.

У цьому робочому аркуші групі планування пропонується визначити всі відповідні програми та політики, які можуть допомогти в процесі нагляду за забезпеченням стійкості. Ці можливості сортуються за наступними категоріями: Регуляторні, адміністративні/технічні, фінансові та комунальні. На останніх сторінках робочої таблиці учасникам групи планування пропонується самостійно оцінити ступінь своєї спроможності на основі попередніх робочих таблиць, а також ставиться низка додаткових запитань, які допоможуть у процесі самооцінки.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

4.4 ОБИРАЙТЕ РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ДЛЯ ВПРОВАДЖЕННЯ

Після складання переліку рішень щодо забезпечення стійкості та визначення потенціалу, громада повинна зосередити свої зусилля на визначенні того, які державні та приватні структури повинні вжити заходів для досягнення поставлених цілей.

Процес оцінки та визначення пріоритетів може допомогти зважити всі "за" і "проти" різних визначених рішень щодо забезпечення стійкості. Першим кроком є розробка критеріїв оцінки для аналізу переліку рішень щодо забезпечення стійкості. Критерії повинні включати критичність інфраструктури, вразливості та ймовірність загроз/небезпек, а також здатність відповідати цілям, завданням та показникам ефективності громади.

Додаткові міркування при оцінці рішень для забезпечення стійкості можуть включати наступні моменти:

- > Планування та операційні вимоги громади, власників та операторів об'єктів критичної інфраструктури (наприклад, комплексні/загальні плани, плани дій у надзвичайних ситуаціях, плани безперервності роботи, плани перевірок та технічного обслуговування тощо).
- > Обмеження фінансування, в тому числі операційної діяльності та технічно
- > Можливості партнерства
- > Відповідні політичні пріоритети
- > Проблеми громади
- > Економічні наслідки

Інші критерії оцінки описані в [Посібнику FEMA з планування пом'якшення наслідків стихійних лих на місцевому рівні](#). Якби критерії оцінки не використовувалися, вони повинні бути узгоджені учасниками планування/зацікавленими сторонами.

ДЛЯ ЦЬОГО ІСНУЄ РЕСУРС!



Питання для оцінки альтернатив пом'якшення

Цей набір запитань може бути використаний для підтримки фасилітованих дискусій та якісного аналізу альтернативних варіантів підвищення стійкості.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

Економічна оцінка рішень

NIST розробив програмне забезпечення для прийняття економічних рішень (EDGe\$), щоб допомогти громадам оцінити [Перегляньте ресурс у розділі Ресурси планування стійкості інфраструктури](#).

Інструментарій аналізу вигод і витрат (ABB)

FEMA має Інструментарій аналізу вигод і витрат (BCA), який можна використовувати для визначення економічної ефективності проекту зі зменшення наслідків стихійних лих шляхом зіставлення вигод від зниження ризиків від проекту із загальною вартістю проекту.

[Перегляньте ресурс у розділі Ресурси планування стійкості інфраструктури](#).

КРИТЕРІЇ ОЦІНКИ РІШЕНЬ



Посібник FEMA з планування пом'якшення наслідків надзвичайних ситуацій на місцевому рівні, березень 2013 року, пропонує наступні критерії оцінки при аналізі потенційних рішень:

- > **Вигоди-Витрати:** Чи є передбачувані витрати обґрунтованими порівняно з можливими вигодами?
- > **Соціальний:** Чи вплине запропонована дія негативно на одну з груп населення? Чи зруйнує дія усталені райони, розділить виборчі округи або спричинить переселення людей з низьким рівнем доходу?
- > **Безпека життєдіяльності:** Наскільки ефективно дії захищатимуть життя та запобігатимуть травматизму?
- > **Захист власності:** Наскільки значними будуть заходи щодо усунення або зменшення шкоди, завданої структурам та інфраструктурі?
- > **Технічні:** Чи є рішення щодо забезпечення стійкості технічно здійсненним? Чи це довгострокове рішення?
- > **Адміністративний:** Чи має громада кадрові та адміністративні можливості для впровадження рішення з підвищення стійкості та його підтримки, або ж знадобиться допомога ззовні?
- > **Політичний:** Чи підтримує громадськість рішення щодо підвищення стійкості? Чи є політична воля для його підтримки?
- > **Правові:** Чи має громада повноваження впроваджувати рішення з підвищення стійкості?
- > **Екологія:** Яким є потенційний вплив рішення щодо забезпечення стійкості на навколишнє середовище? Чи буде воно відповідати екологічним нормам?
- > **Місцевий чемпіон:** Чи є сильний прихильник дії або проекту серед місцевих департаментів та агентств, які підтримають реалізацію дії?
- > **Інші цілі громади:** Чи сприяє дія іншим цілям громади, таким як капітальний ремонт, економічний розвиток, якість довкілля чи збереження відкритих просторів? Чи підтримує вона політику комплексного плану?

4.5 РОЗРОБКА СТРАТЕГІЙ ІМПЛЕМЕНТАЦІЇ

Після того, як рішення з підвищення стійкості оцінені та визначені пріоритети, громада може приступити до розробки стратегій впровадження. Стратегії впровадження описують, як кожне пріоритетне рішення щодо забезпечення стійкості буде впроваджуватися та адмініструватися громадою. Нижче коротко описані елементи, які мають бути включені до плану впровадження:

- > **Відповідальна сторона:** Для реалізації рішення щодо забезпечення стійкості має бути призначена конкретна установа, відділ або посада/особа.
 - > **Співробітники/партнерські організації/партнери з приватного сектору:** Інші партнерські організації або співробітники, які допомагають у впровадженні рішення щодо забезпечення стійкості.
 - > **Попередні кроки впровадження:** Опис попередніх кроків для впровадження рішення з підвищення стійкості. Відповідальна особа/відомство/департамент та будь-які співробітники/партнерські організації можуть внести свій вклад у попередні кроки для впровадження. Ці кроки можуть бути переглянуті з часом, за необхідності, на основі змін умов, ситуацій, ресурсів тощо.
 - > **Орієнтовний графік:** Часові рамки для впровадження рішення щодо забезпечення стійкості. Часові рамки можуть деталізувати, коли рішення щодо забезпечення стійкості буде розпочато і коли воно має бути повністю впроваджене.
- Ресурси, необхідні для реалізації:** Ресурси включають фінансування, технічну допомогу, персонал і матеріали.
- > **Потенційні бар'єри для впровадження та можливі рішення:** Опис потенційних бар'єрів на шляху впровадження та можливі рішення для подолання цих бар'єрів.

ДЛЯ ЦЬОГО Є РЕСУРС!



Робочий аркуш "Стратегія відмовостійкого рішення"

Робоча таблиця "Стратегія рішення щодо забезпечення стійкості" - це зразок робочої таблиці, яку громади можуть використовувати для заповнення елементів стратегії впровадження для кожного рішення щодо забезпечення стійкості.

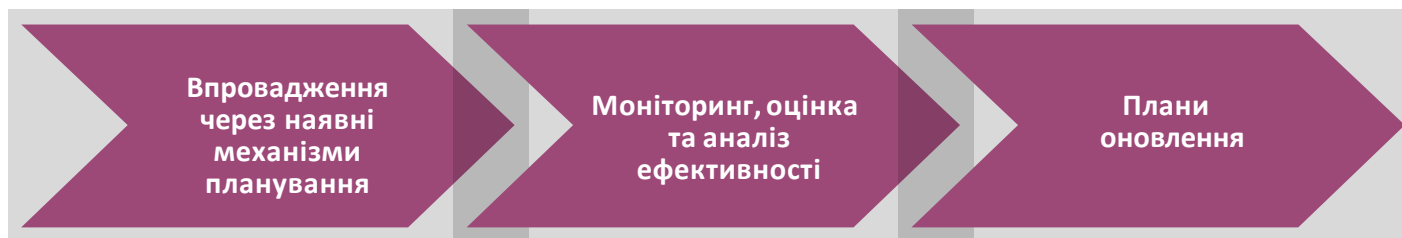
Переглянути ресурс у розділі Ресурси планування стійкості інфраструктури

5. Впровадження та оцінка

У цьому розділі розглядається наступне:

1. [ВПРОВАДЖУВАТИ ЧЕРЕЗ НАЯВНІ МЕХАНІЗМИ ПЛАНУВАННЯ](#)
2. [МОНІТОРИНГ ТА ОЦІНКА ЕФЕКТИВНОСТІ](#)
3. [ПЛАНИ ОНОВЛЕННЯ](#)

5. Впровадження та оцінка



Цей розділ містить інформацію про те, як громади можуть впроваджувати пріоритетні рішення щодо підвищення стійкості за допомогою існуючих механізмів громадського планування, а також потенційних джерел фінансування та технічної допомоги.

ДЛЯ ЦЬОГО Є РЕСУРС!

Інтеграція плану IRPF

У цьому документі представлено огляд можливих інтеграцій з іншими процесами планування розвитку громад.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).



5.1 ВПРОВАДЖЕННЯ ЧЕРЕЗ НАЯВНІ МЕХАНІЗМИ ПЛАНУВАННЯ

Одним з найкращих способів для громад досягти успіху у зниженні ризиків від загроз і небезпек у довгостроковій перспективі є інтеграція пріоритетних рішень щодо забезпечення стійкості в існуючих планах, політиках та програмах громади.

Учасники планування та інші зацікавлені сторони в громаді повинні проаналізувати діяльність, пріоритети та існуюче планування в громаді.

механізми, щоб побачити, як і куди можна інтегрувати проекти та стратегії стійкості. Ось деякі приклади існуючих планів і програм, в які можна інтегрувати рішення щодо забезпечення стійкості:

- > Плани капітального ремонту
- > Комплексні/загальні плани
- > Плани економічного розвитку
- > Плани екстренного зв'язку
- > Плани дій у надзвичайних ситуаціях
- > Плани зменшення небезпеки FEMA
- > Ідентифікація загроз і небезпек та оцінка ризику FEMA (THIRA)
- > Плани управління зростанням
- > Плани житлового будівництва
- > Плани землекористування
- > Довгострокові плани відновлення
- > Інші плани для конкретних громад
- > Плани відновлення стану до катастрофи
- > Плани розвитку конкретних територій
- > Плани перевезень
- > Плани управління водними ресурсами

5.1.1 Потенційні джерела фінансування та технічної допомоги для реалізації

Існує кілька способів, як громада може профінансувати реалізацію визначених нею стійких рішень. Джерела можуть включати традиційні інфраструктурні механізми, такі як податки, збори та облігації, а також гранти від федеральних і державних органів влади та благодійних організацій.

В умовах обмеженості ресурсів на всіх рівнях влади громадам слід також розглянути можливість державно-приватного партнерства для розробки інноваційних механізмів фінансування. Ці механізми залучають додаткові ресурси для розвитку інфраструктури і можуть підвищити ефективність за рахунок розподілу ризиків між багатьма сторонами.

Технічну допомогу також можуть надавати різні департаменти та відомства на федеральному рівні та рівні штатів, а також некомерційні та професійні організації. Технічна допомога - це надання технічної експертизи з метою сприяння громаді у розробці та розвитку інфраструктурних проєктів, що включають найкращі практики підвищення стійкості.

5.2 КОНТРОЛЮВАТИ, ОЦІНЮВАТИ ТА АНАЛІЗУВАТИ ЕФЕКТИВНІСТЬ

Усі плани повинні мати процедури підтримки, розроблені громадою для моніторингу, оцінки та аналізу ефективності рішень щодо забезпечення стійкості у досягненні цілей і завдань громади. Вимірювання ефективності забезпечує основу для подальшої модифікації рішень і планів у майбутньому.

Навчання можуть бути одним із способів оцінити ефективність оперативних планів та рішень щодо забезпечення стійкості. [Пакет настільних навчань CISA \(СТЕР\)](#) - це ресурс, який може бути використаний громадами та зацікавленими сторонами критичної інфраструктури для розробки та проведення навчань з відпрацювання планів та процедур.



ДЛЯ ЦЬОГО ІСНУЄ РЕСУРС!

Збірник програм та механізмів фінансування стійкості інфраструктури

Збірник програм та механізмів фінансування стійкості інфраструктури містить перелік потенційних джерел фінансування та технічної допомоги з посиланнями на них.

Переглянути ресурс у розділі [Ресурси планування стійкості інфраструктури](#).

На додаток до цього збірника, сторінка "[Гранти FEMA](#) на пом'якшення наслідків стихійних лих" містить додаткову інформацію про гранти FEMA.



КЛЮЧОВІ МІРКУВАННЯ ДЛЯ ОЦІНКИ ПЛАНІВ

- > Чи змінився характер або масштаб загроз чи небезпек?
- > Чи існують нові загрози або небезпеки, що впливають на громаду?
- > Чи враховують визначені цілі, завдання та рішення поточні та очікувані умови ризику?
- > Чи були впроваджені та завершені рішення щодо забезпечення стійкості?
- > Чи призвело впровадження рішень до очікуваних результатів?
- > Чи достатньо поточних ресурсів для реалізації рішень?
- > Які ще ресурси потрібні для реалізації рішень?
- > Які фактори сприяли успішному впровадженню рішень?
- > З якими перешкодами на шляху реалізації ви зіткнулися? Що можна зробити для подолання цих перешкод?

5.2.1 Розробити структуру для моніторингу, оцінки та аналізу ефективності рішень щодо забезпечення стійкості

Громади повинні розробити систему моніторингу, оцінки та аналізу ефективності зусиль з планування. Як мінімум, планувальники повинні визначити:

- > **Відповідальна сторона:** Хто або яка установа буде відповідати за моніторинг впровадження? Хто або яка установа координуватиме процес моніторингу та оцінки?
- > **Графік:** Коли буде проводитися оцінка планування та впровадження заходів з підвищення стійкості?
- > **Процес:** Яким є процес або метод, за допомогою якого буде здійснюватися моніторинг та оцінка планів? Які критерії будуть використовуватися для оцінки ефективності рішень щодо забезпечення стійкості?

5.3 ПЛАНУЄМО ОНОВЛЕННЯ

Громади повинні передбачити процес оновлення своїх планів. Оскільки громада здійснює моніторинг, оцінку та аналіз ефективності своєї діяльності з планування, вона отримує зворотний зв'язок, який базується на успіхах, перешкодах, що виникли, та отриманих уроках, які можуть бути враховані в подальшій роботі. Громада повинна вирішити, хто або яка установа буде очолювати і координувати процес оновлення плану, а також як і коли слід розпочати процес оновлення.

Графік оновлення може бути прискорений після катастрофи або паралельно з розробкою відновлення або після катастрофи план відновлення. Це дозволяє громаді врахувати подальші зміни у вразливості та пріоритетах, цілях і завданнях після катастрофи. Після катастрофи з'являться додаткові джерела фінансування, які громади зможуть використати для реалізації наступних заходів рішень для забезпечення стійкості. Громади також повинні використовувати більшу обізнаність та інтерес громадськості до питань стійкості після катастрофи і включати питання стійкості інфраструктури в додаткові зусилля та стратегії планування на рівні громади.

КЛЮЧОВІ ПРИЧИНИ ДЛЯ ОНОВЛЕННЯ ПЛАНІВ



- > Зміни у розвитку громади, такі як нові, нещодавні або потенційні забудови чи демографічні зміни, які можуть вплинути на вимоги до інфраструктури.
- > Виникнення серйозного інциденту/катастрофи.
- > Зміни в операційних ресурсах (політика, персонал, приміщення, обладнання або організаційна структура), які можуть вплинути на розвиток або обслуговування/експлуатацію інфраструктурних систем.
- > Зміни в інструкціях або стандартах для розробки, обслуговування та експлуатації інфраструктурних систем.
- > Зміни в політичних пріоритетах, які можуть вплинути на залучення або підтримку впровадження стійких рішень для покращення інфраструктурних систем громади.
- > Зміни в прийнятності різних ризиків і серйозні перебої в роботі інфраструктурних систем.

Всі джерела



Цей розділ містить джерела для:

[ОГЛЯД](#)

КРОК 1: ЗАКЛАДАННЯ ОСНОВИ

[КРОК 2: ІДЕНТИФІКАЦІЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ](#)

КРОК 3: ОЦІНКА РИЗИКУ

КРОК 4: РОЗРОБЛЕННЯ ДІЙ

[КРОК 5: ВПРОВАДЖЕННЯ ТА ОЦІНКА](#)

Огляд

ВИРІВНЮВАННЯ IRPF ДО ПРОЦЕСІВ ФЕДЕРАЛЬНОГО ПЛАНУВАННЯ ТА УПРАВЛІННЯ РИЗИКАМИ

Формат: Матричний

Тип: PDF

Сторінок: 2

Короткий зміст: Ця матриця ілюструє, як Рамкова програма планування стійкості інфраструктури узгоджується з доповненням до різних інших існуючих федеральних процесів і керівних принципів [планування](#) ризиків та/або стійкості.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

МЕТОДОЛОГІЮ ДЛЯ ОЦІНКА РЕГІОНАЛЬНОЇ ІНФРАСТРУКТУРИ СТІЙКІСТЬ

Формат: Документ

Тип: PDF

Сторінки: 118

Короткий зміст : На основі уроків, отриманих в рамках Програми CISA з оцінки регіональної стійкості, ця методологія оцінки забезпечує загальний процес оцінки та вирішення складних питань стійкості інфраструктури, підтверджений десятирічним [досвідом](#) реалізації проектів RRAP.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

Крок 1. Закладання основ

ЗРАЗОК ЗБОРУ ДАНИХ СПИСОК РЕСУРСІВ

Формат: Таблиця

Тип: PDF-документ з вбудованими таблицями

Сторінки: 2

Короткий зміст: Надає загальний огляд потенційних довідкових ресурсів, відсортованих за власниками/творцями ресурсів. Творці включають: Місцеві/окружні/регіональні агенції, власники/оператори критичної інфраструктури, державні агенції, федеральні агенції. Перелік допомагає планувальникам у процесі використання IRPF визначити [всі](#) попередні відповідні зусилля.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

ПОРІВНЯННЯ ІСНУЮЧИХ ПЛАНІВ ГРОМАД

Формат: Посібник

Тип: Онлайн PDF

Сторінок: 116

Короткий зміст: Система оцінки інтеграції планів для забезпечення стійкості - це метод оцінки планів, розроблений Науково-технічним відділом Департаменту внутрішньої безпеки США спільно з партнером Центру передового досвіду з питань стійкості прибережних територій Техаського університету A&M. Система показників може допомогти громадам оцінити та скоординувати різні плани (наприклад, транспортний, економічного розвитку, пом'якшення наслідків небезпек, управління надзвичайними ситуаціями тощо), щоб вони могли представити узгоджені стратегії та спільно працювати над зменшенням вразливості до небезпек.



[\[ПОСИЛАННЯ\]](#)

ЛИСТ З КОНТАКТНОЮ ІНФОРМАЦІЄЮ УЧАСНИКА ПЛАНУВАННЯ

Формат: Шаблон

Тип: документ PDF

Сторінок: 2

Короткий зміст: ця електронна таблиця надає посадовим особам з планування місце для відстеження контактної інформації для різних учасників групи планування (включно з контактними особами, номерами телефонів, адресами електронної пошти тощо). Ці зацікавлені сторони відсортовано за типом агентства/сектору.



[\[VIEW PDF\]](#)

СТЕЙКХОЛДЕР ЛИСТ-ЗАПРОШЕННЯ

Формат: Шаблон (лист)

Тип: PDF документ

Сторінок: 1

Короткий зміст: Цей зразок листа надає керівнику проекту та/або керівнику групи планування приклад змісту, який можна використовувати для запрошення та заохочення до участі в процесі планування. Можна використовувати весь зразок або його частину оскільки це найкраще [підходить](#) для різних типів запрошених стейкхолдерів.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

ПРИКЛАДИ ЦІЛЕЙ І ЗАВДАНЬ

Формат: Шаблон (перелік)

Тип: PDF документ

Сторінок: 2

Резюме: У цьому шаблоні перераховано більше цілей, які можуть спрямовувати дискусії щодо стійкості інфраструктури.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

Крок 2. Ідентифікація критичної інфраструктури

МАТРИЦЯ ІНФРАСТРУКТУРНИХ АКТИВІВ: ЗАПРОПОНОВАНІ ПОЛЯ ДАНИХ

Формат: Таблиця

Тип: PDF-документ з вбудованою таблицею

Сторінки: 3

Короткий зміст: У цій таблиці наведено ключові пропозиції щодо збору даних для оцінки об'єктів критичної інфраструктури. Поля даних включають відповідну контактну інформацію, імена власників, широту/довготу, тип, статус тощо.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

ПРАЙМЕР ІНФРАСТРУКТУРНОЇ ЗАЛЕЖНОСТІ

Формат: вебсайт

Тип: онлайн вебсайт

Сторінки: -

Короткий зміст: Посібник з інфраструктурної залежності - це онлайнвий освітній додаток до IRPF, який має на меті відповісти на основні питання, які можуть виникнути у планувальників та осіб, що приймають рішення:

- > *Що таке інфраструктурна залежність і чому мене це має хвилювати?*
- > *Що таке стійкість, як вона пов'язана із залежностями і як її планувати?*
- > *Які ресурси допоможуть мені зменшити ризики залежності та підвищити стійкість моєї громади?*

Цей веб-ресурс є загальнодоступним для самостійного вивчення користувачами відповідно до їхніх інтересів та потреб. Для того, щоб користуватися контентом, не потрібно мати попередньої підготовки або знань.



[\[ПОСИЛАННЯ НА РЕСУРС\].](#)

НАБОРИ ДАНИХ ДЛЯ ІДЕНТИФІКАЦІЯ ІНФРАСТРУКТУРИ

Формат: Тип

документа: PDF

документ **Сторінок:** 7

Короткий зміст: Цей ресурс зосереджений на даних базового рівня інфраструктури країни (HIFLD). Документ містить різні набори даних для вивчення, відсортовані за категоріями (зв'язок, енергетика, транспорт, вода, інше, загрози).



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

ЗАЛЕЖНІСТЬ ІДЕНТИФІКАЦІЙНИЙ АРКУШ

Формат: Робочий аркуш

Тип: Змінна форма PDF

Сторінок: 7

Резюме: У цьому робочому аркуші учасникам планування пропонується визначити такі потенційні залежності для кожного інфраструктурного активу: енергія, природний газ, зв'язок, транспорт, водопостачання, водовідведення, [кіберпростір](#) та критично важливі продукти.



[\[ПЕРЕГЛЯНУТИ PDF\].](#)

ЗАЛЕЖНІСТЬ ВІД СИСТЕМ ГРОМАДИ ПОСІБНИК ДЛЯ ОБГОВОРЕННЯ

Формат: Путівник

Тип: PDF-документ

Сторінки: 2

Резюме: Цей посібник можна використовувати для полегшення обговорення проблеми залежності з групою планування, іншими учасниками або групами зацікавлених сторін. Посібник містить перелік запитань, які допоможуть розпочати дискусію та спрямувати її в потрібне русло визначення критично [важливих](#) функцій громади та/або об'єктів, що залежать від інфраструктурних систем.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ВЛАСНИК СИСТЕМИ/ ПОСІБНИК ДЛЯ ПРОВЕДЕННЯ СПІВБЕСІДИ ІЗ ЗАЛЕЖНИМИ ВІД ОПЕРАТОРА

Формат: Путівник

Тип: PDF-документ

Сторінки: 1

Короткий зміст: Цей посібник містить низку запитань, які можна використовувати для проведення індивідуальних інтерв'ю з власниками та/або операторами систем критичної інфраструктури. Запитання допоможуть визначити та зрозуміти залежності системи та її здатність надавати послуги під час надзвичайної ситуації.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ПОСІБНИК З ФАСИЛІТАЦІЇ ЗУСТРІЧЕЙ

Формат: Путівник

Тип: PDF-документ

Сторінки: 2

Короткий зміст: Цей посібник може бути використаний для полегшення проведення зустрічі з учасниками планування з метою визначення функцій громади, об'єктів, інфраструктурних систем та взаємозалежностей, які є найбільш важливими для забезпечення стійкості громади до надзвичайних ситуацій.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

Крок 3. Оцінка ризику

ІНФОРМАЦІЯ ПРО НЕБЕЗПЕКУ ТА АНАЛІТИЧНІ ДЖЕРЕЛА

Формат: Таблиця із зовнішніми посиланнями

Тип: PDF документ із вбудованою таблицею

Сторінок: 5

Короткий зміст: Надає зовнішні посилання на інформацію про небезпеки та аналітичні джерела, включаючи дані про одну та декілька небезпек, а також інструменти для моделювання та аналізу. Включає посилання на федеральні програми, такі як NOAA, USGS, NIFC та інші.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ДОЩ І ІНФРАСТРУКТУРА: ПОСІБНИК З ПЛАНУВАННЯ

Формат: Путівник

Тип: PDF-документ

Сторінки: 10

Короткий зміст: Цей посібник, розроблений CISA спільно з Національним партнерством зі стійкості до посух, містить огляд небезпек посух, приклади прямих і непрямих впливів, які вони можуть мати на інфраструктурні системи, а також інформацію про федеральні ресурси для оцінки та пом'якшення ризиків посух.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

МЕТОДОЛОГІЇ ОЦІНКИ РИЗИКІВ

Формат: Путівник

Тип: PDF-документ із зображеннями та зовнішніми посиланнями

Сторінки: 6

Короткий зміст: Підсумовує процес аналізу ризиків NIST CRPG. Надає посилання на зовнішні ресурси для проведення аналізу ризиків, зокрема:

- > [Сейсмічна безпека](#)
- > [Підвищення рівня моря та прибережні повені](#)
- > [Повені](#)
- > [Зсуви](#)
- > [Аналіз ризиків "Що, якщо"](#)
- > [Аналіз секторальних планів](#)
- > [Інструмент дослідження інфраструктури \(IST\)](#)
- > [Інтегрований швидкий візуальний скринінг \(IRVS\)](#)
- > [HAZUS-MH від FEMA](#)
- > [Методологія оцінки стійкості регіональної інфраструктури](#)



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

Крок 4. Розробка дій

ДЖЕРЕЛА СТІЙКИХ РІШЕНЬ

Формат: Таблиця із зовнішніми посиланнями

Тип: PDF документ із вбудованою таблицею

Сторінок: 9

Короткий опис: Надає список джерел із зовнішніми посиланнями на ідеї щодо рішень для забезпечення стійкості, відсортованих за типами катастроф. Надає короткий опис для кожного посилання.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ЗРАЗОК РОБОЧОГО АРКУША ДЛЯ ОЦІНКИ СПРОМОЖНОСТІ

Формат: Робочий аркуш

Тип: Форма PDF, яку можна заповнити

Сторінки: 6

Короткий зміст: У цій таблиці учасникам планування пропонується визначити всі відповідні програми та політики, які можуть допомогти в процесі нагляду за забезпеченням стійкості. Ці можливості сортуються за наступними категоріями: Регуляторні, адміністративні/технічні, фіскальні та Комунальні послуги. На останніх сторінках робочого аркуша пропонується спланувати. Тренер пропонує учасникам самостійно оцінити ступінь їхньої спроможності на основі попередніх робочих таблиць і ставить низку додаткових запитань, щоб допомогти в процесі самооцінки.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ПОСІБНИК З ОЦІНКИ АЛЬТЕРНАТИВ ПОМ'ЯКШЕННЯ

Формат: Посібник

Тип: Документ PDF

Сторінок: 1

Короткий зміст: Питання, які можуть бути використані для підтримки фасилітованих дискусій та якісного аналізу альтернатив для підвищення стійкості.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ- ПОСІБНИК З ПРИЙНЯТТЯ ЕКОНОМІЧНИХ РІШЕНЬ NIST (EDGE\$)

Формат: Програмне забезпечення

Тип: Онлайн програмне забезпечення

Сторінок: -

Короткий зміст: NIST створив програмне забезпечення для прийняття економічних рішень (EDGE\$), щоб допомогти оцінити економічний вплив інвестицій. Ресурс допомагає визначити та порівняти відповідні поточні та майбутні витрати на забезпечення стійкості та вигоди, пов'язані з новими капітальними інвестиціями. EDGE\$ можна знайти за адресою edges.nist.gov



[\[ПОСИЛАННЯ НА РЕСУРС\]](#)

ТАБЛИЦЯ СТРАТЕГІЇ СТІЙКОГО РІШЕННЯ

Формат: Таблиця

Тип: Форма PDF, яку можна заповнити

Сторінок: 3

Короткий зміст: Цей зразок робочого аркуша може бути використаний громадами для заповнення елементів стратегії впровадження для кожного визначеного рішення щодо забезпечення стійкості.



[\[ПЕРЕГЛЯНУТИ PDF\]](#)

Крок 5. Впровадження та оцінка

ІНТЕГРАЦІЯ ПЛАНІВ

Формат: Таблиця

Тип документ PDF з вбудованою таблицею

Сторінки: 3

Короткий зміст: Надає огляд можливих інтеграцій з іншими зусиллями/процесами громадського планування. Загальні пропозиції.

[\[ПЕРЕГЛЯНУТИ PDF\]](#)

ЗБІРНИК ПРОГРАМ ТА МЕХАНІЗМІВ ФІНАНСУВАННЯ СТІЙКОСТІ ІНФРАСТРУКТУРИ

Формат: Посібник

Тип PDF

Сторінок: 40

Короткий зміст: IRPF надає зведення доступного фінансування та ресурсів у документі, в якому описуються можливості фінансування та технічної допомоги, які можуть допомогти громадам втілити планування в реальність.

[\[ПЕРЕГЛЯНУТИ PDF\]](#)

Глосарій

Цей розділ включає в себе наступне:

[КЛЮЧОВІ ТЕРМІНИ](#)

[АБРЕВІАТУРИ ТА СКОРОЧЕННЯ](#)

[КРИТИЧНІ СЕКТОРИ ІНФРАСТРУКТУРИ](#)



Ключові терміни

ТЕРМІН	ВИЗНАЧЕННЯ
Спільнота	Одна або більше місцевих юрисдикцій або спеціальних районів, що представляють регіон або спільний інфраструктурний коридор.
Наслідок	Наслідки події, інциденту чи явища, які зазвичай вимірюються чотирма способами: Людські, економічні, місійні та психологічні.
Критична інфраструктура	Активи, системи та мережі, як фізичні, так і віртуальні, настільки життєво важливі на регіональному чи національному рівні, що їхня недієздатність або руйнування матиме виснажливий вплив на безпеку, економіку, громадське здоров'я чи безпеку, або будь-яку їх комбінацію.
Критичність	Міра важливості, пов'язана з втратою або деградацією інфраструктури.
Кіберінфраструктура	Електронні інформаційно-комунікаційні системи та послуги.
Залежність	Відносини довіри всередині та між інфраструктурними системами, які необхідно підтримувати для того, щоб ці системи могли функціонувати або надавати послуги. Залежності можуть бути двосторонніми за своєю природою.
Оцінка	Оцінка ефективності планування з точки зору досягнення поставлених цілей, завдань і показників ефективності.
Фасилітатор	Фізична або юридична особа, відповідальна за скликання зацікавлених сторін та управління діалогом з метою вироблення планів і зобов'язань до дій. Може також виконувати функції керівника групи планування.
Мета	Широке формулювання, яке описує бажаний кінцевий стан, те, чого прагне досягти спільнота, впроваджуючи рішення зі стійкості критично важливої інфраструктури.
Техногенна небезпека	Злочинна або терористична атака, наприклад, вибуховий, біологічний, кібернетичний або хімічний агент, який може порушити або використати інфраструктуру громади.
Пом'якшення наслідків	Потенціал, необхідний для зменшення людських жертв і матеріальних збитків шляхом послаблення впливу катастроф.
Моніторинг	Відстеження впровадження пріоритетних стійких рішень.
Природна небезпека	Погодні та геологічні явища, такі як повінь, ураган, торнадо або землетрус, які можуть порушити або вивести з ладу інфраструктуру громади.

ТЕРМІН	ВИЗНАЧЕННЯ
Мета	Конкретне, вимірюване твердження, яке підтримує досягнення мети.
Фізична інфраструктура	Матеріальні структури або об'єкти та компоненти, які надають послуги інфраструктурного сектору громадам або регіонам, що надають послуги.
Рамки планування	Кроки, яких можуть дотримуватися громади, щоб розробити стратегію або перелік пріоритетних дій, які підвищують безпеку та стійкість критичної інфраструктури.
Група планування	Група осіб у громаді з різних секторів, установ та організацій, які роблять внесок у процес планування стійкості та залишаються відданими своїй справі протягом усього процесу.
Керівник групи планування	Ключовий персонал, який бере участь у процесі планування стійкості інфраструктури та керує ним на всіх етапах, має практичні знання та розуміння місцевих загроз, небезпек та інфраструктури. Може виконувати подвійну роль "фасилітатора".
Стійкість	Здатність готуватися та адаптуватися до мінливих умов, протистояти та швидко відновлюватися після збоїв; включає здатність протистояти та відновлюватися після навмисних атак, нещасних випадків або природних загроз чи інцидентів.
Ризик	Потенціал несприятливого результату, що оцінюється як функція загроз, вразливостей і наслідків, пов'язаних з інцидентом, подією або явищем, часто вимірюється і використовується для порівняння різних майбутніх ситуацій.
Оцінка ризиків	Оцінка, яка враховує типи загроз і небезпек, що загрожують системам інфраструктури громади, та зважає на вразливу інфраструктуру громади.
Зацікавлена сторона	Зацікавлена сторона - це сторона або організація, яка надає послуги інфраструктури, залежить від них або зазнає впливу від діяльності, планів або рішень, що розглядаються.
Техногенна небезпека	Випадкові дії людини, такі як будівництво дамб і гребель або виробництво, транспортування, зберігання і використання небезпечних матеріалів, які можуть порушити або вивести з ладу інфраструктуру громади.
Загроза	Будь-який об'єкт, дія або подія, природна чи створена людиною, що має або вказує на потенційну загрозу життю, інформації, діяльності та/або майну.
Вразливість	Характеристика дизайну, розташування, стану безпеки, функціонування або будь-якої їх комбінації, що робить об'єкт, актив, систему, мережу або географічну територію вразливими до підриву, знищення або використання.

Абревіатури та скорочення

АБРЕВІАТУРА	ВИЗНАЧЕННЯ
ASCE	Американське товариство інженерів-будівельників
CIP	План капітального ремонту
CISA	Агентство з кібербезпеки та безпеки інфраструктури
CRPG	Посібник з планування стійкості громад
CTEP	Комплекс настільних вправ CISA
DDoS	Розподілена відмова в наданні послуг
DHS	Департамент внутрішньої безпеки
DOE	Департамент енергетики
DOT	Департамент транспорту
DoS	Відмова в наданні послуг
EDGe\$	Програмне забезпечення-посібник для прийняття економічних рішень
EPA	Агентство охорони навколишнього середовища
FEMA	Федеральне агентство з надзвичайних ситуацій
FIRM	Мапа тарифів страхування від повеней
HUD	Житлове будівництво та міський розвиток
ICS-CERT	Команда кібер реагування на надзвичайні ситуації в промислових системах управління
IDR	Розвиток та відновлення інфраструктури
IRPF	Структура планування стійкості інфраструктури

АБРЕВІАТУРА	ВИЗНАЧЕННЯ
IRVS	Інтегрований швидкий візуальний скринінг
IST	Інструмент дослідження інфраструктури
LCAT	Інструмент оцінки логістичного потенціалу
NIFC	Національний міжвідомчий протипожежний центр
NIPP	Національний план захисту інфраструктури
NIST	Національний інститут стандартів і технологій
NOAA	Національне управління океанічних і атмосферних досліджень
PPD	Президентська політична директива
PSA	Радник з питань захисту та безпеки
SCADA	Наглядний контроль та збір даних
SHELDUS	База даних подій та збитків від просторових небезпек
SLTT	В штатах, місцеві, племенні та територіальні
SME	Експерт з предметної області
SRMA	Агентство з управління секторальними ризиками
SSP	Секторальний план
THIRA	Оцінка ризику визначення загрози та небезпеки
US-CERT	Команда комп'ютерної готовності до надзвичайних ситуацій США
USGS	Геологічна служба США

Сектори критичної інфраструктури

СЕКТОР	СЕКТОРАЛЬНЕ АГЕНТСТВО З УПРАВЛІННЯ РИЗИКАМИ(SRMA)
Хімічний	Агентство з кібербезпеки та безпеки інфраструктури
Комерційні об'єкти	Агентство з кібербезпеки та безпеки інфраструктури
Комунікаційний	Агентство з кібербезпеки та безпеки інфраструктури
Критичне виробництво	Агентство з кібербезпеки та безпеки інфраструктури
Дамби	Агентство з кібербезпеки та безпеки інфраструктури
Оборонно-промислова база	Департамент оборони
Служби екстреної допомоги	Агентство з кібербезпеки та безпеки інфраструктури
Енергетичний	Департамент енергетики
Фінансові послуги	Департамент казначейства
Харчування та сільське господарство	Департамент сільського господарства та Департамент охорони здоров'я та соціальних служб
Державні установи	Адміністрація загального обслуговування
Охорона здоров'я	Департамент охорони здоров'я та соціальних служб
Інформаційні технології	Агентство з кібербезпеки та безпеки інфраструктури
Ядерні реактори, матеріали та відходи	Агентство з кібербезпеки та безпеки інфраструктури
Транспортні системи	Департамент транспорту
Системи водопостачання та водовідведення	Агентство охорони навколишнього середовища



Структура планування **стійкості інфраструктури** (IRPF)

Березень 2023 | Версія 1.1

Програма розвитку та відновлення інфраструктури -

IRF@csa.dhs.gov