МЕТОДОЛОГІЇ ОЦІНКИ РИЗИКІВ

Оцінка ризиків передбачає оцінку ризиків з урахуванням потенційних прямих і непрямих **наслідків** інциденту, відомі **вразливості** до різних потенційних загроз абонебезпеки, а також загальна або конкретна інформація про **загрози/небезпеки**.
Цей ресурсний документ представляє різні методології, які можуть використовуватися громадами для проведення інфраструктурно-орієнтованої оцінки ризику, як зазначено в кроці 3 IRPF. Якщо Громада вже завершила оцінку ризиків в рамках іншого процесу планування, такого як планування зменшення небезпеки FEMA, результати цієї оцінки можуть бути об'єднані та посилені шляхом проведення критичної оцінки ризиків, специфічних для КІ.
Яку б методологію оцінки ризиків спільнота не вирішила використовувати, метод повинен бути задокументований, відтворюваний та захищений для забезпечення прозорості та практичності для зацікавлених сторін та осіб, які приймають рішення.

Методи аналізу загроз і небезпек

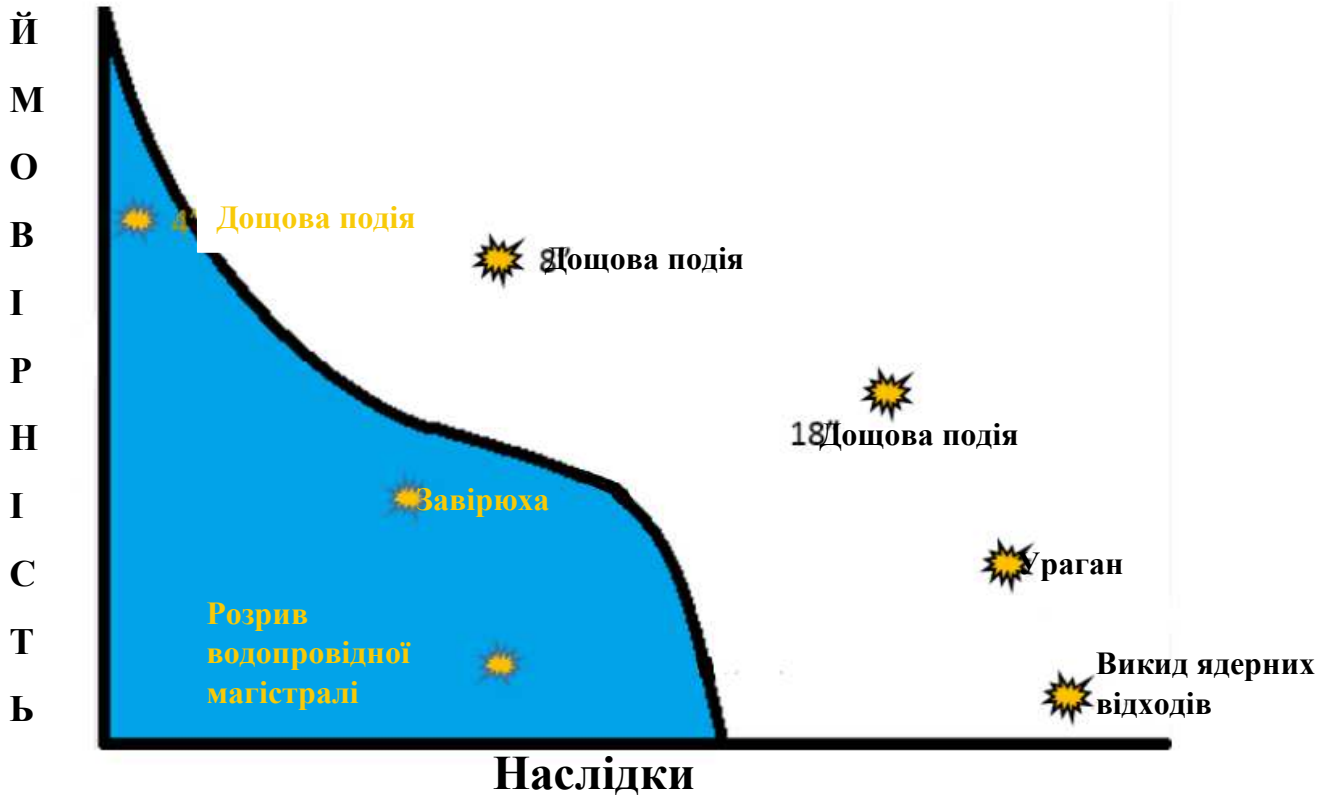
Аналіз впливу небезпек
Цей аналіз визначає існуючі та майбутні системи та активи ОКІ, розташованих в зонах, схильних до небезпек. Цей підхід часто використовує такі інструменти картографування, Географічні інформаційні системи для аналізу та візуалізації. Аналіз може кількісно визначити кількість, тип та вартість КІ громади, розташованої в межах визначеної небезпечні зони, а також показати, які системи та активи піддаються небезпеці M. Ultiple.
Кількість інструментів для підтримки небезпечного впливу, включаючи:

- **Сейсмічні небезпеки:** карти небезпек USGS та дані щодо конкретних місць, http://earthquake.usgs.gov/hazards/hazmaps/
- підвищення рівня моря та затоплення прибережних територій: підвищення рівня моря та вплив затоплення прибережних територій; перегляд і розробка даних, NOAA https://coast.noaa.gov/digitalcoast/tools/slr.html
- **Повені:** продукти FEMA для картографування повеней, https://www.fema.gov/flood-mapping-products
- **Зсувні процеси:** Програма небезпеки зсувів, USGS http://landslides.usgs.gov

Аналіз ризиків "що-якщо"
Аналіз ризиків "що-якщо" - це структурований метод мозкового штурму для розробки сценаріїв загроз і небезпек, а також оцінки їхньої ймовірності та наслідків. Це можна використовувати для розробки стратегії управління ризиком на основі визначених сценаріїв. Додаткову інформацію про аналіз небезпек «Що, якщо» можна знайти за адресою:
http://web.mit.edu/course/10/10.27/www/1027CourseManual/1027CourseManual-AppVI.html

Аналіз сценаріїв загроз і небезпек

Ідентифікація загроз і небезпек, а також оцінка ризиків (THIRA) і огляд готовності зацікавлених сторін (SPR) FEMA. Посібник з комплексної готовності (CPG) 201 містить вказівки щодо проведення THIRA, що включає процес розробки сценаріїв ризику, які можна використовувати для виконання оцінки ризику. Розробляючи сценарії, громади повинні вибирати загрози та небезпеки на основі двох факторів: 1) ймовірності виникнення загрози чи небезпеки 2) наслідків цієї події, якщо вона відбудеться.



Сценарії мають відображати серйозні події, які можуть вплинути на вашу спільноту

Розробляючи сценарії, планувальники повинні враховувати не лише загрози та небезпеки, з якими зазвичай стикається та які розглядає громада, а й ті, які є незвичними, малоймовірними або потенційно можуть виникнути в найближчі роки.

Зрештою, група планування повинна визначити вірогідні сценарії та представляти низку загроз і небезпек, які можуть вплинути на громаду. Важливо, що хороший набір сценаріїв охоплюватиме три рівні ймовірності:

- *Порядок проведення: один раз на 5 років.* На цьому рівні системи критичної інфраструктури повинні залишатися функціональними і не зазнавати значних пошкоджень або збоїв[1]
- *Дизайн: раз на 50 років тип заходу.* На цьому рівні системи інфраструктури повинні зазнавати мінімальних пошкоджень або збоїв, як це визначено проектними рівнями продуктивності[2].
- *Екстремальний: раз на 200+ років тип події.* На цьому рівні можна очікувати серйозних пошкоджень або збоїв, але КІ повинна працювати на мінімальному рівні[3].

Після розробки набору сценаріїв ризику кожен сценарій слід описати та надати контекст. Це означає визначення факторів, таких як час, місце та умови небезпеки. Для цілей оцінки ризику надання деталей щодо цих аспектів допоможе визначити наслідки небезпеки для систем КІ.

1 НІСТ, 74
2 Там же, 74
3 Там же, 74

Методології оцінки ризиків

Сценарій	Опис контенту
Ураган 4 категорії	Ураган із постійною швидкістю вітру 135 миль на годину та поривами до 160 миль на годину досягає чотирьох миль на схід від центру міста, викликаючи 15-футовий штормовий нагін уздовж прибережних районів і випадаючи 12 дюймів опадів на більшу частину регіону в 24-годинний період.

Після розробки ці сценарії можуть бути використані для інших програм оцінки ризиків, таких як оцінка вразливостей та аналіз наслідків.

Методи аналізу вразливостей

Галузеві плани Методології оцінки вразливості

Багато галузевих планів (SSP) описують методології оцінки вразливості, які використовуються в окремих секторах КІ. SSP також надають інформацію про виконання оцінки вразливості. SSP можна знайти за адресою: https://www.cisa.gov/critical-infrastructure-sectors

Інструмент обстеження інфраструктури (IST)

IST — це добровільне веб-дослідження вразливостей, яке проводить Агентство з кібербезпеки та безпеки інфраструктури (CISA) для визначення та документування загальної безпеки та стійкості об'єкта. Дані опитування, що складаються зі зважених балів за різними факторами для конкретної КІ, графічно відображаються на інформаційній панелі IST, яка порівнює дані з подібними об'єктами та інформує про заходи захисту, планування стійкості та розподіл ресурсів. IST наразі не доступний як інструмент самооцінки. Власники та оператори КІ повинні зв'язатися з місцевим консультантом з безпеки CISA (PSA), щоб запланувати візит для ~~проведення оцінки I~~IST. Більше інформації про IST можна знайти за адресою: https://www.dhs.gov/sites/default/files/publications/ecip-ist-fact-sheet-508.pdf

Інтегрований швидкий візуальний екран (IRVS)

IRVS був розроблений Управлінням науки та технологій DHS, щоб забезпечити оцінку ризику на рівні об'єкта проти ряду загроз і небезпек. Частина оцінки вразливості IRVS включає аналіз ділянки, архітектури, огороджувальних конструкцій, структурних компонентів, механічних систем і безпеки для оцінки ризику. Додаткову інформацію про IRVS і версію інструменту, яку можна завантажити, можна знайти за адресою: https://www.dhs.gov/bips-04-integrated-rapid-visual-screening-series-irvs-buildings

Метод аналізу наслідків

HAZUS-MH

HAZUS — це загальнонаціональна стандартизована методологія, яка містить моделі для оцінки потенційних збитків від землетрусів, повеней і ураганів. HAZUS використовує технологію GIS для оцінки фізичних, економічних і соціальних наслідків катастроф. Він графічно ілюструє межі визначених місць високого ризику через землетрус, ураган і повінь. Потім користувачі можуть візуалізувати просторові відносини між населенням та іншими більш постійно фіксованими географічними активами або ресурсами для конкретної небезпеки, що моделюється. Додаткову інформацію про HAZUS можна знайти за адресою: http://www.fema.gov/hazus

Метод оцінки ефективності для виявлення ризику

Підхід NIST Community Resilience Planning Guide (CRPG) можна використовувати для оцінки операційних можливостей систем і активів критичної інфраструктури щодо встановлених цілей ефективності за різних сценаріїв загрози/небезпеки. CRPG наголошує на розумінні того, як довго спільнота може продовжувати працювати, якщо різні служби та
системи інфраструктури скомпрометовані. Залежно від катастрофи громада повинна мати очікуваний графік оперативних можливостей на основі короткострокових (години), проміжних (тижні) і довгострокових (місяців) цілей.

На малюнку нижче показано зразок періоду відновлення працездатності. Для кожного активу або системи КІ планувальники повинні визначити відповідні контрольні показники ефективності після події. Громади повинні визначити, як швидко необхідно відновити кожен ідентифікований актив чи систему, щоб забезпечити швидке реагування та відновлення та уникнути довгострокової економічної чи соціальної шкоди для громади. Деякі активи або системи можуть бути настільки критичними, що будь-яке зменшення потужності може завдати довгострокової шкоди, тоді як іншим активам необхідно підтримувати лише невелику частину своєї робочої здатності одразу після інциденту.

Пріоритет інфраструктури	**Необхідна підтримка**	**Етап 1 Короткостроковий (години) 0-24 24-48 48-72**			**Етап 2 Середній рівень (тижні) 1-4 4-8 8-12**			**Етап 3 Довгостроковий (місяці) 3+ 4-24 24+**		
Інфраструктурна система/актив 1	R, S, MS C	90%								
Інфраструктурна система/актив 2	R	30%	90%							
Інфраструктурна система/актив 3	MS	30%			60% 90%					
Інфраструктурна система/актив 4	C		30%			60%		90%		
Інфраструктурна система/актив 5		60%	90%							

Наступні визначення цільових показників продуктивності адаптовані з NIST CRPG. Планувальники можуть використовувати ці визначення для встановлення цільових показників ефективності або створювати власні, які більше відповідають їхнім потребам.

- 30% представляє операційну потужність активу або частини інфраструктурної системи, які повинні бути функціональними для ініціювання заходів реагування та відновлення
- 60% означає робочу здатність активу або частини інфраструктурної системи, необхідну для відновлення звичайних (тобто щоденних) операцій у зменшеному масштабі.

- 90% являє собою частку, необхідну для декларування активів або інфраструктурних систем у нормальній робочій потужності.

Окрім цільових показників ефективності, спільноти можуть визначати, які зовнішні системи підтримки
(наприклад, взаємодопомога), необхідні для виконання запланованих критеріїв. Вони типові у:

- *(R) Регіональні: сусідні громади, уряд округу*
- *(s) Держава: Державні органи*
- *(MS) Багатодержавність: Рада урядів/губернаторів, міждержавна підтримка*
- *(c) корпоративні/громадські організації: наприклад, Червоний Хрест, основні галузі промисловості в громаді або регіоні*

Зі встановленими цільовими показниками ефективності планувальники можуть використовувати сценарії ризиків, створені за допомогою процесу THIRA (або будь-якого іншого методу розробки сценаріїв), щоб встановити очікувані рівні ефективності. Для кожного сценарію планувальники повинні переоцінити цілі ефективності та оцінити очікувану ефективність. Це повинно включати огляд і аналіз:

- **Інформація про минулі інциденти**, які продемонструють, як подібні загрози та небезпеки вплинули на системи КІ в минулому, і спрогнозує, як вони впораються зі сценаріями ризику
- **Експертний досвід учасників планування,** особливо власників і операторів критичної інфраструктури, а також тих, хто володіє знаннями про вразливість активів і систем до конкретних загроз і небезпек, буде особливо актуальним для визначення очікуваної продуктивності
- **Попередній аналіз**, проведені в громаді або сусідніми громадами, можуть надати оцінки очікуваної ефективності.

Використовуючи таблицю цілей продуктивності, вкажіть очікуваний рівень продуктивності для інфраструктурних активів і систем, як показано на малюнку нижче. Ця робота допоможе виявити ключові розбіжності між цілями продуктивності та очікуваними рівнями продуктивності, які становлять ризики для вашої спільноти, і повинні стати основою для планування стійкості. Ці ризики мають бути задокументовані та використані як основа для визначення рішень щодо стійкості.

Очікувані показники: ураган 4 категорії

Пріоритет інфраструктури	**Необхідна підтримка**	**Етап 1 Короткостроковий (години)**			**Етап 2 Середній рівень (тижні)**			**Етап 3 Довгостроковий (місяці)**		
		0-24	**24-48**	**48-72**	**1-4**	**4-8**	**8-12**	**3+**	**4-24**	**24+**
Пріоритет інфраструктури 1	R, S, MS C	90% 30%	60%		90%					
Пріоритет інфраструктури 2	R	30%	90% 30%		60%	90%				
Пріоритет інфраструктури 3	MS	30% 30%			60% 90% 60% 90%					
Пріоритет інфраструктури 4	C		30% 30%			60% 60%		90% 90%		
Пріоритет інфраструктури 5		60%	90% 30%		60%	90%				