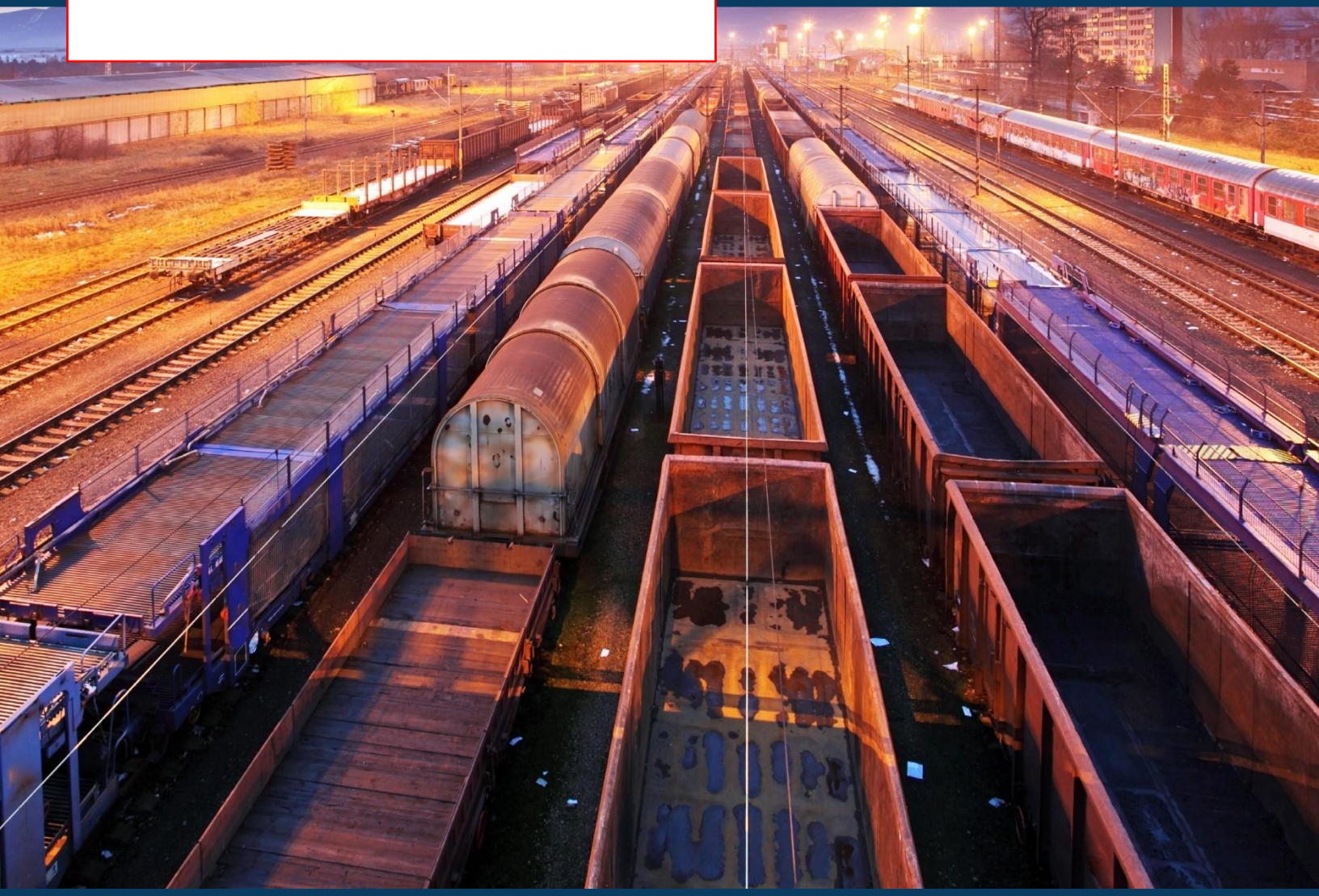


Посібник

Безпека та стійкість критичної інфраструктури

Листопад 2019

Зміст

Передмова

У Сполучених Штатах Америки (США) Патріотичний акт 2001 року визначив критичну інфраструктуру як
"системи та активи, фізичні чи віртуальні, настільки життєвоважливі для Сполучених Штатів, що непрацездатність або знищення таких систем та активів матиме виснажливий вплив на безпеку, національну економічну безпеку, здоров'я та безпеку населення, або будь-яку комбінацію цих питань".

Як зазначено в Національному плані захисту інфраструктури (NIPP) *NIPP 2013: Партнерство зарадибезпеки та стійкості критичної інфраструктури*, бачення США таке:

> *Держава, в якій фізична і кібернетична критична інфраструктура залишається безпечною і стійкою, вразливості зменшуються, наслідки мінімізуються, загрози виявляються і знешкоджуються, а реагування і відновлення прискорюються.* Це бачення лежить в основі базового підходу до безпеки і стійкості критичної інфраструктури в Сполучених Штатах: Посилити *безпеку і стійкість критично важливоїінфраструктури країни шляхом управління фізичними і кібер-ризиками за допомогою спільних і інтегрованих зусиль спільноти критично важливої інфраструктури.*

Міністерство внутрішньої безпеки США у співпраці з Державним департаментом США підготувало цей посібник, щоб надати огляд підходів до безпеки та стійкості критичної інфраструктури, прийнятих у Сполучених Штатах. Оскільки атаки на "м'які" цілі та місця масового скупчення людей тривають по всьому світу, потреба у вирішенні поточних та нових викликів зростає. Тому Міністерство внутрішньої безпеки і Державний департаментСША спільно працюють над зміцненням внутрішньої і глобальної безпеки, реалізуючи поточні програми і визнаючи, що для вирішення цих нових проблем можуть знадобитися нові підходи.

Мета цього посібника - поділитися базовою інформацією та уроками, отриманими США заостанні 15 років, а не просувати конкретні підходи. Ця інформація може бути корисною для інших країн, особливо тих, які розглядають можливість розробки або вдосконалення власних добровільних і нормативних програм безпеки та стійкості інфраструктури.

Кожен розділ цього посібника містить додаткові джерела для отримання більш детальної інформації з конкретних тем, що розглядаються. Веб-сайти, на які є посилання, також містятьбагато інших корисних ресурсів. Ми рекомендуємо читачам також ознайомитися з цією інформацією.

Брайан Харрел

Заступник директора з питань безпеки інфраструктури Агентства з кібербезпеки тазахисту інфраструктури
Міністерство внутрішньої безпеки США

Посол Натан Сейлз

Координатор зпитань боротьби з тероризмом Бюро з питань боротьби з тероризмом
Державний департамент США

Що таке критична інфраструктура?

Критична інфраструктура включає в себе активи, системи, об'єкти, мережі та інші елементи, від яких залежить національна безпека, економічнажиттєздатність, здоров'я та безпека суспільства.Ми знаємо, що критична інфраструктура - це електроенергія, яка використовується в наших будинках, вода, яку ми п'ємо, транспорт, який нас переміщує, магазини, в яких ми робимо покупки, а також Інтернет і комунікації, від яких ми залежимо, щоб підтримувати зв'язок з друзями, родиною та колегами. У США ця фізична та кіберінфраструктура, як правило, перебуває у власності та управлінні приватного сектору, хоча деякі об'єкти належать федеральному уряду, уряду штату або місцевим органам влади. Не вся інфраструктура в межах галузі є критично важливою для країни чи регіону. Необхідно визначити, яка інфраструктура є одночасно критично важливою для підтримки безперервного надання послуг або виконання функцій і вразливою до певних видів загроз або небезпек.
Пріоритетний розподіл наявних ресурсів на цю підгрупу інфраструктури може посилити безпеку країни, підвищити стійкість і знизити ризики.

Існує чотири функції життєзабезпечення - транспорт, водопостачання, енергетика та зв'язок, а це означає, що їхня надійна робота є настільки важливою, що порушення або втрата однієї з цих функцій безпосередньо вплине на безпеку та стійкість критично важливої інфраструктури в багатьох секторах та між ними. Наприклад, зацікавлені сторони в енергетичному секторі забезпечують в секторах зв'язку, транспорту і водопостачання, а енергетичний сектор, у свою чергу, покладається на них у постачанні палива (транспортування), виробництві електроенергії (води для виробництва і охолодження), а також в управлінні і експлуатації інфраструктури (зв'язок) Ці зв'язки і взаємозалежності між елементами інфраструктури і секторами означають, що втрата однієї або декількох життєво важливих функцій, як правило, має негайний вплив на операцію або місію в декількох секторах. Як наслідок, з часом може виникнути додаткова втрата інших функцій. Крім того, визначення та офіційне визнання галузей, які є життєво важливими та/або мають міжгалузеву взаємозалежність, полегшує співпрацю та обмін інформацією, що сприяє забезпеченню безперервності операцій та послуг. Вибір секторів, які є пріоритетними в інформаційно-роз'яснювальній роботі, повинен відображати розуміння взаємозв'язку та взаємозалежності інфраструктури, визнавати існуючі галузеві асоціації та узгоджуватися з функціями та наглядовими обов'язками урядових установ.

Критична інфраструктура охоплює не лише функції життєзабезпечення. Наприклад, у 2017 році виборча інфраструктура була виокремлена в підсектор "Урядові об'єкти" через важливість вільних і чесних демократичних виборів як основи американського способу життя. Робота над зменшенням ризиків у партнерстві з державними та приватними структурами, відповідальними за виконання таких важливих функцій, є ключовим елементом підтримки довіри громадськості до критично важливої інфраструктури країни

Поточні сектори критичної інфраструктури США

- Хімічна
- Комерційні об'єкти
- Комунікації
- Критичне виробництво
- Дамби
- Оборонно-промислова база
- Служби екстреної допомоги
- Енергія
- Фінансові послуги
- Продовольство та сільське господарство
- Державні установи
- Охорона здоров'я та громадське здоров'я
- Інформаційні технології
- Ядерні реактори, матеріали та відходи
- Транспортні системи
- Системи водопостачання та водовідведення

Вибрані ресурси

1. *Акт про об'єднання та зміцнення Америки шляхом надання відповідних інструментів, необхідних дляперехоплення та перешкоджання тероризму (USA PATRIOT ACT) від 2001 року* (https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf)
2. Веб-сторінка Агентства кібербезпеки та інфраструктури Міністерства внутрішньої безпеки США. (https://www.cisa.gov/)
3. NIPP 2013: *Партнерство* заради *безпеки та стійкості критичної інфраструктури* (https://www.cisa.gov/national-infrastructure-protection-plan)
4. План розвитку енергетичного сектору США окреслює загальні міжгалузеві взаємозалежності в Розділі 4.2 "Взаємозалежність такоординація", а також надає загальний огляд взаємозалежностей між функціями життєзабезпечення. (https://www.cisa.gov/infrastructure-security)
5. Додаткову інформацію можна знайти на веб-сторінці DHS Critical Infrastructure Security. (https://www.dhs.gov/topic/critical-infrastructure- security)

Що таке "загрози та небезпеки" для критичної інфраструктури?

Як природні, так і антропогенні (навмисні або випадкові) інциденти можуть завдати шкоди, пошкодити, вивести з ладу або знищити критично важливу інфраструктуру. Замість того, щоб зосереджуватися на одному типі загроз чи небезпек, таких як урагани або тероризм, державам слід визначити всі загрози і небезпеки, які становлять найбільші ризики для критичної інфраструктури, що дозволить більш ефективно і раціонально планувати і розподілятиресурси.

Критична інфраструктура вже давно піддається ризикам, пов'язаним з фізичними загрозами та стихійними лихами, а зараз все частіше зазнає впливу кібер-ризиків. Ці ризики виникають через зростаючу інтеграцію інформаційно- комунікаційних технологій з критичною інфраструктурою та зловмисниками, які зосереджуються на використанні потенційних кібервразливостей. Оскільки фізична інфраструктура стає все більш залежною від складних кіберсистем, критично важлива інфраструктура може стати більш вразливою до певних кіберзагроз, в тому числі транснаціональних.

Зв'язки та взаємозалежності між елементамиінфраструктури та секторами означають, що пошкодження, порушення або руйнування одного елемента інфраструктури може спричинити каскадний ефект, що вплине на безперервну роботу інших.
Виявлення та розуміння взаємозалежностей (двосторонніх) або залежностей (односторонніх)між елементами та секторами інфраструктури є важливими для оцінки ризиків та вразливостей, а також для визначення кроків, які можуть бути зроблені для підвищення безпеки та стійкості.

Наприклад, функціонування електромережі залежить від інтегрованих інформаційно-комунікаційних систем інших секторів критичної інфраструктури. Одним із прикладів негайної потреби в енергії є відновлювальні роботи після стихійного лиха. До відновлення енергосистеми системи водопостачання та водовідведення не можуть забезпечувати чисту воду, природний газ не може постачати тепло, а системи генерації та телекомунікації швидко виходять з ладу, як тільки починають виходити з ладу резервні джерела живлення. Енергетика настільки важлива для зусиль з реконструкції та відновлення США, що компанія Florida Power and Light (FPL) за останні кілька років інвестувала близько 3 мільярдів доларів у відновлення та зміцнення інфраструктури виробництва та постачання електроенергії у Флориді. Ці гроші пішли на зміцнення 700 ліній електропередач до критично важливих об'єктів, таких як поліцейські дільниці, лікарні та заправки; закопування 60 ліній електропередач під землю; розчищення від рослинності 150 000 миль ліній; перевірку 150 000 опор щороку; встановлення 4,9 мільйона "розумних" лічильників, які допомагають прогнозувати та запобігати перебоям в електропостачанні. Після ураганів, що спустошили весь штат у 2017 році, компанія FPL змогла відновити електропостачання всім клієнтам, здатним безпечно отримувати електроенергію протягом декількох днів, включаючи аварійні служби, лікарні та інші життєво важливі об'єкти інфраструктури.

М'які цілі та місця скупчення людей

Від кіберзагроз до загроз фізичній безпеці, ми живемо у світі, де терористична активність зростає і стає все більш дифузною, де атаки можуть бути як простими і опортуністичними за своєю природою,

так і складними і організованими. Зростаюча кількість атак на "м'які" цілі/місця масового скупчення людей у різних містах світу - від Орландо до Нової Зеландії, від Сан-Бернардіно до Шрі-Ланки - демонструє, що характер загрози змінюється, і посилює потребу в глобальній пильності, готовності та співпраці. Національні та міжнародні зусилля спрямовані на подолання тенденції до атак на "м'які" цілі та місця масового скупчення людей.

Наприклад, Сполучені Штати працюють на національному рівні з усіма рівнями влади, щоб забезпечити навчання, ресурси і матеріали для посилення і просування безпеки "м'яких цілей" і місць скупчення людей.

На міжнародному рівні країни працюють разом, обмінюючись передовою практикою, отриманими уроками і досвідом протидії атакам на м'які цілі і місця масового скупчення людей, щоб допомогти створити і розвивати глобальну культуру безпеки. Ініціатива Глобального антитерористичного форуму (GCTF) із захисту м'яких цілей, яку спільно очолюють США і Туреччина, передбачала проведення у 2017 році серії регіональних семінарів за участю представників уряду і приватного сектору, спрямованих на підвищення обізнаності, готовності і створення першого набору необов'язкових міжнародних стандартів захисту м'яких цілей в антитерористичному контексті.

Передовий досвід має на меті інформувати та спрямовувати уряди та приватний сектор у їхній спільній роботі над розробкою політики, практики,керівних принципів, програм та підходів до захисту своїх громадян від терористичних атак на "м'які" цілі та місця масового скупчення людей. Під час дискусій було визнано, що держави несуть головну відповідальність за забезпечення безпеки на своїй території та захист свого цивільного населення відповідно до Статуту Організації Об'єднаних Націй (ООН). Резолюція Ради Безпеки ООН 2341 (2017) окреслює роль держав у захисті критичної інфраструктури та особливо вразливих об'єктів, таких як громадські місця, від терористичних атак,у тому числі за допомогою державно-приватного партнерства у відповідних випадках.

Загрози та небезпеки

Загрози та небезпеки можуть бути специфічними для географічних регіонів або всієї країни, інавіть мати глобальні наслідки, наприклад, такі як

- **Кліматологічні події** (екстремальні температури, посуха, лісові пожежі)
- **Гідрологічні події** (повені)
- **Метеорологічні події** (тропічні циклони, сильні конвективні шторми, сильні зимові бурі)
- **Геофізичні події** (землетруси, цунамі, виверження вулканів)
- **Пандемії** (глобальні спалахи захворювань)
- **Події космічної погоди** (геомагнітні бурі)
- **Технологічні та промислові аварії** (руйнування конструкцій, промислові пожежі, викиди небезпечних речовин, розливи хімічних речовин)
- **Незаплановані збої** (старіння інфраструктури, несправність обладнання,масштабні відключення електроенергії)
- **Кримінальні інциденти та терористичні атаки** (вандалізм, крадіжки, пошкодження майна, інциденти з активними стрільцями, кінетичні атаки)
- **Кіберінциденти** (атаки на відмову в обслуговуванні, шкідливе програмне забезпечення, фішинг)
- **Атаки на ланцюги поставок** (використання вразливостей для спричинення збою в роботі системи або мережі)
- **Операції іноземного впливу** (з метою поширення дезінформації або підриву демократичних процесів)
- **Ненадійні інвестиції** (потенційно можуть надати іноземним державам надмірний вплив на американську критичну інфраструктуру)

Ці загрози та небезпеки необхідно проаналізувати, щоб визначити їхній потенційний вплив на інфраструктуру та ймовірність їхньої реалізації.

Управління міжгалузевими ризиками для критичної інфраструктури

У квітні 2019 року Агентство кібербезпеки та інфраструктурної безпеки (CISA) вперше в історії оприлюднило перелік з 55 національних критично важливих функцій для більш ефективного управління найбільш стратегічними ризиками для нації. Національні критичні функції - це функції уряду та приватного сектору, які є настільки важливими для Сполучених Штатів, що їх порушення, корупція або дисфункція матимуть виснажливий вплив на безпеку, національну економічну безпеку, національну охорону здоров'я або безпеку, або будь-яку їх комбінацію. Ці функції були розроблені в координації з галузевими і державними, місцевими, племінними і територіальними партнерами і дозволяють спільноті критичної інфраструктури аналізувати складні виклики, які нелегко ідентифікувати, зрозуміти або дослідити в рамках існуючих структур управління ризиками для кібер- і фізичної інфраструктури.

Ефективне управління ризиками залежить від здатності спільноти критичної інфраструктури взаємодіяти з різними секторами для сприяння спільному розумінню ризиків та інтеграції широкого спектру заходів з управління ризиками. Як основа, Національні критичні функції охоплюють наскрізні, міжгалузеві ризики та пов'язані з ними залежності, які можуть мати каскадний вплив у межах секторів та між ними. Визначаючи, що є дійсно критично важливим на функціональному рівні і де лежать ключові залежності та взаємозалежності, CISA може виявити осередки ризику, які вважаються неприйнятними для нації. Такий підхід дозволить CISA більш ефективно фіксувати ризики для безпекита стійкості ланцюга поставок, такі як поява підроблених деталей та компонентів або унікальні виклики, пов'язані з ощадливими процесами та практикою "точно в строк". Система національних критичних функцій також дозволяє CISA більш ефективно оцінювати основні проблеми кібербезпеки, такі як атаки з метою крадіжки інтелектуальної власності або зловживання системами управління, які можуть призвести до фізичної шкоди, небезпеки для персоналу та переривання операцій.
Функціональний підхід також висвітлює системні виклики, пов'язані з розвитком робочої сили в умовах стрімкого розвитку технологій. Національні критичні функції сигналізують про визнання того, що технології зумовлюють потребу в координації та співпраці, яка ґрунтується на традиційних успіхах секторального підходу, що дозволяє залучати представників різних галузей для вирішення складних проблем, таких як вразливість, пов'язана з системами визначення місцезнаходження, навігації та синхронізації часу.

Більше інформації на сайті: www.cisa.gov/national-critical-functions.

Вибрані ресурси

1. Департамент критичної інфраструктури Міністерства внутрішньої безпеки США (https://www.cisa.gov/critical-infrastructure-sectors)
2. "Критична інфраструктура, взаємозалежності та стійкість", Т.Д. О'Рурк, *The Bridge* (https://www.nae.edu/7655/ CriticalInfrastructureInterdependenciesandResilience)
3. Комісія з питань державної служби штату Флорида (http://www.psc.state.fl.us/ElectricNaturalGas/EnergyInfrastructure)
4. Домашня сторінка Департаменту внутрішньої безпеки США "Безпека м'яких цілей та місць масового скупчення людей" (https://www.cisa.gov/securing-soft-targets- and-crowded-places)
5. *Стратегічна національна оцінка ризиків на підтримку* ППР *8: Комплексний підхід, заснований на оцінці ризиків, на шляху до безпечної та стійкої нації* містить огляд багатьох видів загроз і небезпек (https://www.dhs.gov/xlibrary/assets/rma-strategic- national-risk-assessment- ppd8.pdf).
6. Внутрішня *загроза для критичної інфраструктури* (https://www.dhs.gov/cisa/insider-threat-mitigation)
7. *Посібник Міністерства внутрішньої безпеки США "М'які цілі та місця масового скупчення людей" та "Огляд планів безпеки":* Багато матеріалів у цьому посібнику були створені у співпраці з галузевими партнерами, щоб гарантувати їхню корисність і відповідність динамічному середовищу, в якому ми живемо. (https://www.cisa.gov/publication/securing-soft-targets-and-crowded-places-resources)
8. Резолюція Ради Безпеки ООН 2341 про захист критичної інфраструктури (http://www.un.org/en/ga/search/view_doc.asp?symbol=S/ RES/2341%282017%29&referer=/english/&Lang=E)
9. Ініціатива GCTF із захисту м'яких цілей Анталійський меморандум про захист м'яких цілей в умовах боротьби з тероризмом (http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2341%282017%29&referer=/english/&Lang=E)
10. Організація Об'єднаних Націй: рекомендовані практики захисту критичної інфраструктури (https://www.thegctf.org/Portals/1/Documents/Links/ Meetings/2017/Twelveth GCTF Coordinating Committee Meeting/GCTF - Анталійський меморандум про захист м'яких цілей в умовах боротьби з тероризмом)
11. Компендіум Організації Об'єднаних Націй: Захист КІ від терористичних атак: https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP- final-version-120618_new_fonts_18_june_2018_optimized.pdf.

Хто відповідає за критичну інфраструктуру?

Посилення безпеки та стійкості критичної інфраструктури є спільною відповідальністю зацікавлених сторін - власників та операторів об'єктів критичної інфраструктури, а також різних державних установ та неурядових організацій (в тому числі галузевих асоціацій).

Ролі та обов'язки щодо підтримання або підвищення безпеки та стійкості інфраструктури широко варіюються і залежатьвід багатьох факторів, таких як

- Державна чи приватна власність;
- Регулювання в межах сектору;
- Очікувані загрози та небезпеки для конкретного сектору;
- Рішення про те, що сектор або регіон обирає - зосередитися на заходах із захисту інфраструктури, зменшенні наслідків або швидкому реагуванні та відновленні після несприятливих подій.

Галузеві асоціації часто відіграють ключову роль наданні рекомендацій, тоді як в інших секторах можуть існувати нормативні акти, що вимагають певних дій, або ж можуть застосовуватися і ті, й інші. У деяких секторах діють державні або національні стандарти проектування, які допомагають захистити від пошкоджень, спричинених такими подіями, як пожежі, повені та землетруси. Страхові компаніїтакож можуть встановлювати вимоги безпеки для своїх страхувальників у деяких секторах.
Наприклад, хімічна промисловість США сприяє підвищенню готовності через добровільну угоду між промисловістю та урядом, а також частково підпадає під дію регуляторних програм.

Заходи з ліквідації можуть здійснюватися силами служб швидкого реагування, власників/операторів, регіональних і федеральних ресурсів, але відповідальність за відновлення в переважно добровільній системі, як, наприклад, у США, зазвичай покладається на власників і операторів, які найкраще знають інфраструктуру.

Взаємодія на всіх рівнях уряду і промисловості сприяє взаєморозумінню і довірі, а також обміну інформацією та практичним досвідом. Взаємодія, яка сприяє плануванню, визначенню пріоритетів у використанні ресурсів, проведенню навчань і тренувань, значною мірою сприяє успіху національних зусиль із забезпечення готовності і, особливо, ефективному і своєчасному реагуванню. Такі заходи також стимулюють підтримку спільних державно-приватних зусиль.

Тематичне дослідження - Центри обміну та аналізу інформації

Центри обміну та аналізу інформації (ISAC) допомагають власникам та операторам об'єктів критичної інфраструктури захистити свої об'єкти, персонал та клієнтів від кібер- та фізичної загрози та інших небезпек. ISAC збирають, аналізують та поширюють інформацію про загрози серед своїх членів, а також надають їм інструменти для зменшення ризиків та підвищення стійкості. ISAC - це довірені організації, створені власниками та операторами об'єктів критичної інфраструктури для сприяння обміну інформацією та найкращими практиками щодо фізичних і кіберзагроз та їх пом'якшення. Концепція ISACs була запроваджена та оприлюднена відповідно до Директиви Президента України №63 (PDD-63), підписаної у 1998 році. Деякі БНКІ були створені ще в 1999 році, а більшість з них існують вже щонайменше десять років. Як правило, будучи неприбутковими організаціями, МНКР працюють у своїх галузях, поширюючи критично важливу інформацію та підтримуючи обізнаність щодо ситуації в секторі вцілому.

Центр обміну та аналізу інформації про нерухомість (RE-ISAC) є чудовим прикладом такої структури обміну інформацією. RE-ISAC - це державно-приватне партнерство з обміну інформацією між Сектором комерційних об'єктів США та федеральними службовцями внутрішньої безпеки, організоване та кероване "Круглим столом з питань нерухомості" (некомерційною організацією, що базується у Вашингтоні, округ Колумбія). Сектор комерційних об'єктів є невід'ємною частиною критичної інфраструктури США і включає в себе широкий спектр об'єктів, де люди живуть, працюють, роблять покупки і розважаються. RE-ISAC - це спеціальний галузевий канал для обміну інформацією про потенційні загрози та вразливості фізичної та кібербезпеки, що допомагає захистити комерційні об'єкти та людей, які ними користуються.
Завдяки об'єднанню представників галузі для агрегування, обміну та оцінки інформації, якість, актуальність та загальна цінність отриманої інформації зростає в геометричній прогресії. Як результат, RE-ISAC та її члени можуть досягти цілей, яких жодна галузева організація не змогла б досягти самотужки. Це приносить користь галузі, уряду та нації в цілому.

Добровільний та регуляторний підходи

Програми з безпеки та стійкості інфраструктури можуть бути добровільними, нормативними або комбінованими. У Сполучених Штатах найпоширенішими є добровільні програми.

- Добровільні програми найкраще працюють для просування нових програм або там, де розмаїття в галузі занадто велике, щоб застосовувати єдині стандарти.
- Волонтерські програми повинні мати сильні ціннісні пропозиції або бізнес-кейси, щоб продемонструвати переваги участі в них, щоб в кінцевому підсумку бути успішними.
- Регуляторні підходи можуть бути бажаними для забезпечення єдиного стандарту, необхідного для всіх, заохочення певних галузевих практик, де це доречно, і забезпечення того, щоб дотримання стандартів не було конкурентною перевагою.

Вибрані ресурси

1. Див. веб-сайт FEMA "Підхід всієї громади до управління надзвичайними ситуаціями: Принципи, теми та шляхидій" (http://www.fema.gov/whole-community)
2. Веб-сторінка Партнерства Міністерства безпеки США у сфері критичної інфраструктури (https://www.cisa.gov/critical-infrastructure-sector- partnerships)

Що визначає безпеку та стійкість критичної інфраструктури?

Безпека може бути визначена як зменшення ризику для критичної інфраструктури від вторгнень, атак або наслідків природних чи техногенних катастроф шляхом застосування фізичних засобів або оборонних кіберзаходів.

Стійкість можна визначити як здатність готуватися та адаптуватися до мінливих умов.Це означає здатність протистояти і швидко відновлюватися після збоїв, навмисних атак, аварій або природних загроз чи інцидентів.
Відмовостійка інфраструктура також повинна бути надійною, гнучкою та адаптивною.

Ефективна програма безпеки та стійкості критичної інфраструктури ґрунтується на співпраці та обміні інформацією.

Співпраці сприяє створення структур і процесів,необхідних для того, щоб уряд(и) і приватний сектор могли вільно спілкуватися, не розголошуючи службову інформацію і не надаючи несправедливих переваг; підтримувати довірливе середовище обміну інформацією, в якому зацікавлені сторони обмінюються інформацією для зміцнення безпеки і стійкості; забезпечувати справедливе представництво і залучення відповідних зацікавлених сторін на всіх рівнях влади, промисловості, управління в надзвичайних ситуаціях і безпеки.

Успішний обмін інформацією вимагає налагоджених механізмів або каналів для регулярного зв'язку із зацікавленими сторонами, а також до, під час і після інциденту. Обмін інформацією може відбуватися в різних формах, включаючи навчальні заходи, брифінги, сповіщення електронною поштою, конференц-дзвінки абозустрічі в безпечних місцях для обговорення секретних матеріалів про конкретні загрози та небезпеки, а також документи та форуми, які заохочують до обміну набутим досвідом.

Остання категорія покращує планування реагування на майбутні події.

Для сприяння добровільній співпраці та обміну інформацією між секторами критичної інфраструктури та державними установами (федеральними, штатними, місцевими, племінними та територіальними), а також між ними, США створили офіційну структуру партнерства, що складається з координаційних рад державного та приватного секторів, які проводять окремі та спільні засідання з метою підвищення безпеки та стійкості критичної інфраструктури. Обмін інформацією з приватним сектором здійснюється через Центри обміну та аналізу інформації (ISAC).

ISACs переважно працюють за галузевою моделлю, що означає, що організації певного сектору критичної інфраструктури (або певного сегменту в межах сектору) об'єднуються для обміну інформацією.

Хоча багато з цих груп вже є важливими рушіями ефективного обміну інформацією, деякі організації не вписуються в усталений сектор або мають унікальні потреби. У США також існують галузеві організації з обміну та аналізу інформації (ISAO).

Створені для збору, аналізу та поширення інформації про кіберзагрози, ISAO пропонують більш гнучкий підхід до самоорганізованого обміну інформацією між певними спільнотами за інтересами (наприклад, малий бізнес у різних секторах, таких як юридичні, бухгалтерські та консалтингові фірми, які підтримують міжгалузевих клієнтів).

Обмін інформацією

Нижче наведені рекомендації можуть допомогти полегшити та підтримати зусилля з обміну інформацією:

- Визначити зацікавлені сторони, які мають інтерес та/або зацікавленість у безпеці та стійкості критичної інфраструктури.
- Надавати дієву інформацію про загрози, щоб власники/оператори могли впроваджувати плани та вживати відповідних заходів.
- Визначити, що обмін інформацією має бути взаємним - адже власники та оператори можуть спостерігати підозрілу активність, яка допомагає виявити та підтвердити загрози.
- Створити та підтримувати зручні системи обміну інформацією для зацікавленихсторін, які сприятимуть як рутинному, так і швидкому спілкуванню під час подій/надзвичайних ситуацій.
- Інформація про загрози повинна оброблятися таким чином, щоб усунути специфіку джерел і методів збору даних, щоб нею можна було ширше ділитися, особливо з відповідними зацікавленими сторонами.
- Інформація про власника та оператора повинна бути захищена відповідно до національного законодавства.

Вибрані ресурси

1. Система *обміну інформацією про загрози для критичної інфраструктури: Ресурсний посібник* описує, як відбувається обмін інформацією про загрози між федеральним урядом, власниками та операторами. Ця система включає опис і контактну інформаціюключових суб'єктів обміну інформацією про загрози, а також тематичні дослідження, які показують, як обмін інформацією про загрози працює на практиці. (https://www.cisa.gov/publication/ci- threat-info-sharing-framework)
2. Організації з обміну інформацією та аналізу (https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos)
3. Обидва американські механізми обміну інформацією - Шлюз захисту інфраструктури (Infrastructure Protection Gateway) та Інформаційна мережа національної безпеки (Homeland Security Information Network, HSIN) - використовуються для зв'язку з партнерами у сфері критичної інфраструктури; подібні мережі можуть бути корисними і в інших країнах для забезпечення спільної платформи для збору, аналізу та надання інформації про потенційні загрози і небезпеки, а також для підтримання обізнаності про обстановку в країні.

Початок роботи

Розвиток безпеки критичної інфраструктури та Програма стійкості починається з визначення цілей і завдань; вони можуть бути на національному, регіональному, місцевому, галузевому чи організаційному рівнях. Бачення та місія також можуть бути корисними, щоб поділитися думкою про те, чого прагне досягти програма. Кроки, визначені на наступній сторінці, зазвичай задокументовані в плані безпеки та стійкості критичної інфраструктури. Для того, щоб не зупинятися на досягнутому і не відсунути плани на другий план через інші пріоритети, важливо встановити конкретні терміни та етапи виконання.

У деяких країнах для спрямування та об'єднання зусиль, у тому числі між урядом і промисловістю, може бути корисною низхідна або національна структура, що працює за принципом "зверху-вниз". Однак в інших країнах, можливо, більш поширеною є практика, коли штати, провінції, регіони або подібні структури організовують і контролюють заходи з безпеки, управління надзвичайними ситуаціями та забезпечення готовності до них.

Програма безпеки та стійкості критичної інфраструктури повинна відображати існуюче операційне середовище, культурні цінності/переконання та спиратися на існуючі відносини, зусилля та політику. Вона повинна узгоджуватися з іншими програмами і підтримувати їх, щоб забезпечити ефективне використання ресурсів, залучення наявних можливостей і спільнот, а також розуміння ролей і обов'язків.

Визначення обсягу зусиль також є важливим на початковому етапі. Серед питань, на які слід відповісти, є такі: визначити кілька секторів життєзабезпечення чи більшу групу секторів інфраструктури? Державна і приватна інфраструктура, чи тільки одна з них для початку? Чи буде фінансування для створення програми, чи буде урядова директива для початку роботи? Чи всі загрози і небезпеки мають бути включені (рекомендовані), чи лише вибрані? Чим повніший та інтегрованіший обсяг, тим більші переваги готовності, які можна реалізувати на постійній основі.

Інші початкові питання стосуються визначення зацікавлених сторін - які установи, асоціації, власники та оператори інфраструктури та інші зацікавлені сторони повинні бути залучені? Досвід у сфері США вказує, що широка участь є ключем до успішної розробки та впровадження комплексної програми сприяння постійному підвищенню безпеки та стійкості.

Визначення ролей та обов'язків різних зацікавлених сторін на початковому етапі може допомогти узгодити і навіть об'єднати відповідні знання/дисципліни, зосередити зусилля, забезпечити дотримання термінів і надати бажані ресурси для ефективної програми.

Аналогічно, виявлення існуючих програм або зусиль, пов'язаних з безпекою та стійкістю інфраструктури, може допомогти закріпити розробку загальної програми і слугувати орієнтиром для інших секторів.
Подумайте, чи існують проекти з перевірки в аеропортах, а також заходи з водної та енергетичної безпеки, які вже впроваджуються або можуть слугувати прикладом для наслідування.

Співпраця та обмін інформацією в рамках спільноти критичної інфраструктури мають фундаментальне значення для загального процесу. Створення механізмів, які сприятимуть відкритій співпраці та забезпечать обмін своєчасною та дієвою інформацією, а також найкращими практиками, допоможе отримати участь у

програмі як під час проектування та розробки програми, так і під час її реалізації. Партнерство уможливлює більш ефективне та результативне управління ризиками. Розгляньте потребу в таких механізмах і партнерствах на кожному рівні організації або управління, наприклад, всередині і між секторами, всередині і між урядами, всередині і між приватним сектором.

Основні кроки для створення Плану безпеки та стійкості критичної інфраструктури

- Визначити цілі та завдання
- Визначити існуючі приклади відповідних планів або програм з безпеки та стійкості критичної інфраструктури
- Визначити сферу застосування
- Визначити зацікавлені сторони
- Задокументувати ролі та обов'язки
- Створити механізми координації та обміну інформацією
- Встановити часові рамки
- Побудувати систему управління ризиками
- Розробка та проведення оцінювання
- Проводити тренінги та навчання, в тому числі практичні вправи
- Встановити метрики
- Просувати програму через інформаційно-просвітницьку роботу та підвищення обізнаності

Після того, як ви склали план, обов'язково регулярно виконуйте його. Це гарантує, що в разі реального інциденту кожен буде знати свою роль і що робити.

Вибрані ресурси

1. На додаток до моделі, наведеної в НПІП 2013 року та його попередників, прикладом програми стійкості містає Чарльстонська мережа стійкості. (http://www.charlestonresilience.net/)

Система управління ризиками

Ризик - це потенційна можливість небажаного результату в результаті інциденту, події або явища, що визначається його ймовірністю - функцією загроз і вразливостей - і пов'язаними з ним наслідками. Управління ризиками - це процес виявлення, аналізу та інформування про ризик, а також прийняття, уникнення, передачі або контролю ризику до прийнятного рівня за прийнятну ціну.

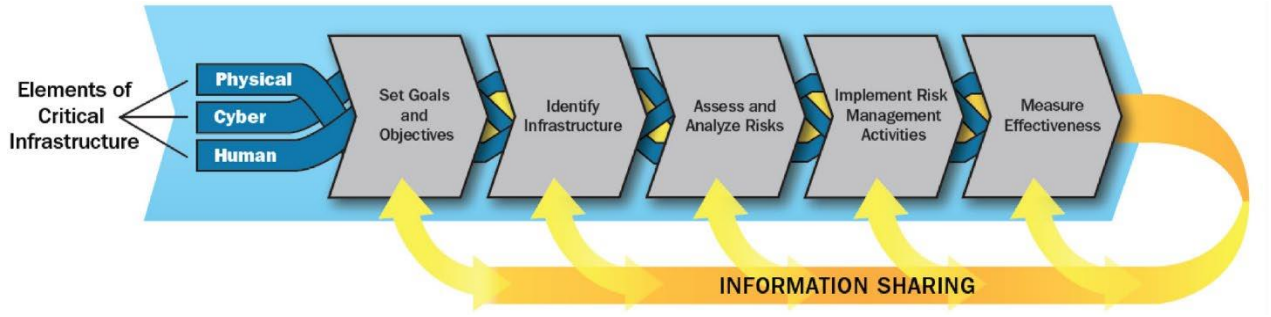
Управління ризиками зосереджує ресурси на тих загрозах і небезпеках, які з найбільшою ймовірністю можуть спричинити значні небажані наслідки для конкретної інфраструктури чи сектору, і визначає дії, спрямовані на запобігання або пом'якшення наслідків цих інцидентів. Воно також підвищує безпеку і зміцнює стійкість шляхом визначення і пріоритизації дій, спрямованих на забезпечення безперервності основних функцій і послуг, а також на підтримку посиленого реагування і відновлення. Управління ризиками полегшує прийняття рішень і визначення пріоритетів для всіх зацікавлених сторін.

Система управління ризиками визначає підхід до послідовного:

- Ідентифікувати, аналізувати та розподіляти ресурси для стримування, виявлення, підриву та підготовки до загроз і небезпек для критичної інфраструктури;
- Визначити пріоритетність зусиль зі зниження вразливості, звернути увагу на фізичні особливості або експлуатаційні характеристики, які роблять елемент інфраструктури відкритим для експлуатації або вразливим до певної загрози;
- Пом'якшувати потенційні наслідки інцидентів на випередження або готуватися до їх ефективного подолання,якщо вони все ж таки трапляться.

Система управління ризиками може застосовуватися на всіх рівнях державного управління та в організаціях приватного сектору. Вона повинна охоплювати всі загрози і небезпеки, а також різноманітні фактори в усіх секторах критичної інфраструктури, на додаток до окремих активів і систем.

Нинішня система управління ризиками для критичної інфраструктури США представлена нижче і описана в Національному плані захисту інфраструктури (NIPP) 2013 року.



U. Рамкова основа управління ризиками критичної інфраструктури США

Основні принципи управління ризиками в США

1. Для ефективного розподілу ресурсів необхідно скоординовано виявляти ризики та управляти ними в рамках спільноти критичної інфраструктури.

2. Партнерства у сфері критичної інфраструктури можуть значно покращити розуміння еволюції ризиків як для кібер-, так і для фізичних систем та активів, а також надавати дані та перспективи від різних зацікавлених сторін.

3. Розуміння та усунення ризиків, пов'язаних з міжсекторальними залежностями та взаємозалежностями, є важливим для підвищення загальної безпеки та стійкості критично важливої інфраструктури.

4. Здобуття знань та зменшення інфраструктурних ризиків вимагає обміну інформацієюна всіх рівнях спільноти критичної інфраструктури.

5. Партнерський підхід, що передбачає залучення державних і приватних зацікавлених сторін, визнає унікальні перспективи та порівняльні переваги різноманітної спільноти об'єктів критичної інфраструктури. Наприклад, Функція 14 "Підтримка в надзвичайних ситуаціях" Національної системи реагування підтримує координацію міжсекторальних операцій, включаючи стабілізацію ключових ланцюгів постачання та систем життєзабезпечення громади, між власниками та операторами інфраструктури, бізнесом та їхніми державними партнерами.

6. Регіональні, державні та місцеві партнерства мають вирішальне значення для вироблення спільних поглядів на прогалини та заходи з покращення ситуації.

7. Критична інфраструктура виходить за межі національних кордонів, вимагаючи двосторонньої, регіональної та міжнародної співпраці, розбудови потенціалу, взаємодопомоги та інших угод про співпрацю. Наприклад, "Канадсько-американський план дій щодо критичної інфраструктури" закладає основу для транскордонних зусиль двох країн у сфері безпеки та стійкості критичної інфраструктури.

8. Безпека та стійкість повинні бути враховані під час проектування елементів інфраструктури.

Вибрані ресурси

1. Інструменти та ресурси, які допоможуть бізнесу спланувати, підготуватися та захиститися від атаки (https://www.cisa.gov/hometown-security)
2. *Посібник із захисту критичної інфраструктури та ключових ресурсів на державному, регіональному, місцевому, племінному та територіальному рівнях* використовується на державному, місцевому та регіональному рівнях для адаптації національного підходу до відповідних потреб. (https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf).
3. Огляд ESF та Додатків до нього, що координують федеральну допомогу на підтримку Національної системиреагування. (https://www.fema.gov/media-library-data/20130726-1825-25045-8535/overview_esf support_annexes_2008.pdf).

Роль оцінки ризиків

Існує цілий ряд методологій для оцінки загроз і небезпек та розробки програм управління ризиками. Оцінки допомагають урядовцям, власникам і операторам розуміти потенційні інциденти і те, як вони можуть вплинути на інфраструктуру та громади.

Оцінка ризиків дає особам, які приймають рішення, кращу інформацію для визначення того, які заходи з пом'якшення наслідків та управління ризиками є найбільш важливими, а також для розуміння того, де різні типи дій є найбільш прийнятними. Спектр доступних заходів включає: координацію з іншими зацікавленими сторонами; надання додаткового обладнання для ліквідації наслідків або відновлення; модифікацію дизайну інфраструктури; обмеження на операції; найм і навчання персоналу та інші. Оцінка ризиків також утримує увагу від автоматичного перемикання на рідкісні або найгірші події з екстремальними наслідками, сприяючи розгляду низки більш вірогідних подій, навіть якщо вони мають дещо менші, але все ж таки значні наслідки.

Мета полягає у проведенні точних і всебічних оцінок, які індивідуально або колективно охоплюють загрозу, вразливість і наслідки (також відомі як небезпека, частота і наслідки для ризиків, не пов'язаних із загрозами). Тип оцінки може визначатися міжнародними стандартами, найкращими галузевими практиками або наявними історичними даними. Оскільки кібербезпека є ключовим питанням для забезпечення стійкості критичної інфраструктури, комплексне розуміння безпеки та стійкості передбачає цілісний розгляд як фізичної, так і кібернетичної сфер. Тому до оцінювання слід залучати експертів як з фізичної, так і з кібербезпеки критичної інфраструктури.

Аналіз залежностей і взаємозалежностей в рамках оцінки ризиків (на міжнародному, національному, регіональному та/або місцевому рівнях) може сприяти плануванню та визначенню пріоритетів у розподілі ресурсів для забезпечення безперервності надання критично важливих послуг і пом'якшення каскадних наслідків інцидентів, які все ж таки відбуваються. Моделювання та імітація можуть бути важливою частиною аналізу складних систем і взаємозалежностей. У США неурядові організації (науковці, асоціації тощо) також розробляють і поширюють продукти щодо загроз, вразливостей і потенційних наслідків для широкої аудиторії.

Проведення оцінки ризиків для елемента інфраструктури може вимагати значних витрат ресурсів з боку власників/операторів або інших осіб, які не завжди можуть бути виправданими. Для визначення масштабу оцінки багато методологій оцінки ризиків пропонують спочатку провести певний вид перевірки - як правило, перевірки наслідків, щоб з'ясувати, чи є потенційні впливи значними чи ні. Це допомагає мінімізувати ресурси, виділені на повну оцінку ризиків. У США уряд пропонує експертні рекомендації та допомогу через радників з питань безпеки, розгорнутих по всій країні, а також надає інструменти, які допомагають власникам і операторам у проведенні оцінок і допомагають управляти витратами.

Повна оцінка ризиків може бути виправдана для всіх або більшості критично важливих елементів інфраструктури в певних районах, де потенційні наслідки, пов'язані з порушенням роботи, руйнуванням або експлуатацією, є особливо високими. У цих обмежених випадках процес перевірки не є необхідним, оскільки всі

активи "пройдуть відбір". Процес перевірки рекомендується проводити для всіх інших об'єктів інфраструктури, щоб знизити вимоги дотих елементів, які можуть не потребувати повної оцінки. Наприклад, для більшості об'єктів інфраструктури в сільській місцевості може бути достатньо оцінки на рівні перевірки, в той час як у великих мегаполісах може знадобитися повна оцінка ризиків для низки елементів інфраструктури.

Обмін результатами оцінок між зацікавленими сторонами критичної інфраструктури забезпечить краще розуміння ймовірності, впливу та пов'язаних з ними наслідків різних загроз і небезпек.
Інформування про результати оцінки може допомогти відповідним зацікавленим сторонам у плануванні та розподілі ресурсів і витрат. Крім того, інформування про ризик сприятиме забезпеченню готовності, пом'якшенню наслідків і реагуванню з боку власників, операторів і державних службовців.

Інформування про готовність до катастрофічних землетрусів на північному заході Тихого океану

Землетрус магнітудою 9.0 в зоні субдукції Каскадія матиме широку регіональну зону впливу, що простягається на понад 700 миль від Британської Колумбії до Північної Каліфорнії. Прямі сейсмічні поштовхи, руйнування ґрунту та затоплення цунамі завдадуть значних пошкоджень значній частині інфраструктури регіону на системному рівні. У багатьох випадках ці системи, ймовірно, будуть виведені з ладу одразу після першого землетрусу. Такі значні пошкодження інфраструктури західного Вашингтону вимагатимуть від уряду і приватного сектору значних зусиль для забезпечення регіону основними товарами і предметами першої необхідності для підтримки постраждалих від стихійного лиха. Більш чітке розуміння обсягу, масштабу і ступеня впливу землетрусу в ЦСЗ на об'єкти і системи критичної інфраструктури з урахуванням характеристик стійкості на системному рівні є життєво важливим кроком у розробці планів реагування на катастрофи і відновлення, а також планів пом'якшення наслідків катастроф до їх настання. На підтримку таких зусиль щодо забезпечення готовності до ЦСЗ на федеральному рівні, рівні штатів і місцевому рівні, Програма CISA з оцінки регіональної стійкості (RRAP) здійснила три спільні проекти з оцінки регіональної стійкості, зосередившись на регіональних транспортних системах, включаючи автомобільні, залізничні, мостові, морські та авіаційні види транспорту, а також на водопостачанні у штатах Вашингтон і Орегон. На сьогоднішній день ці зусилля принесли такі результати:

- Визначено найбільш життєздатний мультимодальний транспортний маршрут та об'єкти, які можуть бути використані для ліквідації наслідків ЧСЗ.
- Визначено та пріоритезовано транспортні маршрути та об'єкти для потенційних інвестицій у зміцнення/обслуговування, заміну/модернізацію та/або заходи з пом'якшення наслідків стихійних лих.
- Надано відтворювані методології перевірки сейсмічної вразливості для подальшого використання державними та місцевими органами влади.
- Вивчили сейсмічну вразливість та роль аеродромів у забезпеченні доставки життєво важливих ресурсів до постраждалих районів.
- Розпочато визначення ймовірного впливу на систему водопостачання та потенційних альтернативних джерел води і стратегій водопостачання для тих, хто вижив.

Найважливіше те, що спільний характер цих зусиль об'єднав і сприяв ще більшій співпраці між федеральними, державними і місцевими органами влади та приватним сектором у вирішенні цих критично важливих питань, в яких кожен з них відіграє свою окрему, але важливу роль. Ця важлива робота безпосередньо впливає на планування та готовність до катастроф, підвищуючи стійкість критично важливої інфраструктури, а разом з нею і стійкість громад у цих двох штатах.

Вибрані ресурси

1. Шлюз захисту інфраструктури - це сховище для певних інструментів оцінки. Шлюз захисту інфраструктури ілюструє, як уряд може віртуально ділитися інструментами з партнерами, як тільки вони стають доступними. (https://www.cisa.gov/ip-gateway)
2. На веб-сторінці "Оцінки вразливості критичної інфраструктури" описано низку конкретних підходів. (https://www.cisa.gov/critical- infrastructure-vulnerability-assessments)
3. Прикладом міжнародного стандарту для критичної інфраструктури є Директива Ради Європейського Союзу 2008/114/ЄС про ідентифікацію та призначення європейських об'єктів критичної інфраструктури та оцінку необхідності покращення їх захисту. (https:// eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF)

Навчання та освіта

Навчання та освіта мають фундаментальне значення для успіху програми безпеки та стійкості критичної інфраструктури і повинні охоплювати державних службовців, власників та операторів інфраструктури, служби швидкого реагування та громадськість, де це доречно.

Навчання повинно бути доступним у різних формах, щоб забезпечити якнайширше охоплення, включаючи курси під керівництвом інструктора, вебінари, онлайн-курси для самостійного навчання, а також письмові інструкції та робочі посібники. Навчальні програми можуть бути присвячені загальним концепціям, кращим практикам або дуже специфічним темам.
На бічній панелі нижче проілюстровано спектр тем, які наразі пропонуються Міністерством внутрішньої безпеки США та іншими інфраструктурними партнерами.

Практика підкріплює навчання та освіту і допомагає досягти найбільшої користі від витраченого часу та ресурсів. Навчання забезпечують таку практику в практичний спосіб, що включає обговорення або моделювання небажаних подій, які можуть бути пов'язані з критичною інфраструктурою. Існує багато різних типів навчань, зокрема: дискусійні тренінги або семінари; фасилітовані дискусії з кількома установами та операторами інфраструктури щодо конкретного сценарію (так звані "настільні вправи"); відпрацювання конкретних планів або заходів; змодельовані події (функціональні навчання); і реальне реагування на штучні події (відомі як повномасштабні навчання).

Додатковою перевагою тренінгів та освітніх заходів є налагодження відносин між зацікавленими сторонами, особливо під час практичних занять. Розвиток більшої довіри та взаєморозуміння в секторі сприяє більш ефективному реагуванню під час кризи.

Створення культури постійного вдосконалення безпеки та стійкості інфраструктури також вимагає збільшення уваги до фундаментальних концепцій у певних навчальних програмах коледжів та університетів.
Метою академічних програм може бути: навчання студентів використанню методів оцінки; підвищення обізнаності інженерів про способи захисту елементів інфраструктури, зменшення їхньої вразливості або підвищення стійкості шляхом проектування; інформування планувальників про важливість завчасного планування, обміну інформацією та партнерства; допомога керівникам аварійних служб у розумінні потенційних наслідків каскадних збоїв; серед інших факторів.

Потенційні теми тренувань

- Найкращі практики фізичної безпеки
- Active Shooter
- Виявлення та повідомлення про підозрілу діяльність
- Загроза зсередини
- Акредитація
- Перевірка сумок
- Перевірка меценатів
- Найкращі практики сектору (наприклад, хімічна промисловість, енергетика, водопостачання)
- Управління ризиками ланцюга постачання та залежність від третіх осіб
- Управління інцидентами та реагування на них
- Загроза вибуху бомби
- Протидія саморобним вибуховим пристроям
- Загрози від транспортних засобів
- Терористи-смертники
- Кібербезпека
- Вправи
- Загрози, тактика і тенденції тероризму
- ІКС та операційні технології
- Оцінка ризиків (загрози, вразливості та/або наслідків) та їх пом'якшення

Вибрані ресурси

1. На веб-сторінці "Навчання з питань критичної інфраструктури" є посилання на багато різних навчальних пропозицій; інші надаються професійними товариствами, окремими компаніями, торговельними асоціаціями та академічними установами. (https://www.dhs.gov/critical-infrastructure-training)
2. Приклад вправи для електромережі (http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx)
3. Методологія проведення навчань у галузі зв'язку є прикладом, який можна вдосконалити та розвинути для проведення навчань та оцінки конкретних проблемних питань, що виникають у власників та операторів інфраструктури зв'язку. (https://www.dhs.gov/ sites/default/files/publications/CommunicationsSpecificTabletopExerciseMethodology.pdf)
4. CISA Hometown Security. (https://www.cisa.gov/hometown-security)

Оцінювання програми

Після того, як ви розробили програму оцінки та протидії загрозам критичній інфраструктурі, рекомендується періодично оцінювати цю програму. Ключовим викликом в оцінюванні є вимірювання програм безпеки та стійкості критичної інфраструктури через широту та різноманітність інфраструктури програми - у багатьох секторах, на різних рівнях влади, з різними типами власників та операторів.

Є два конкуруючих імперативи:

- Розробка загальних і послідовних вимірювань для порівняння ефективності в різних секторах, видах діяльності та регіонах, а також для визначення пріоритетності прогалин;
- Налаштування вимірювань ефективності,які відповідають унікальним потребам кожної звітної ситуації.

Метрики або показники ефективності повинні бути простими і повторюваними, їх слід використовувати для встановлення підзвітності,документування фактичних результатів діяльності, полегшення виявлення недоліків або прогалин, визначення коригувальних дій, підвищення ефективності управління ризиками,а також для переоцінки цілей, завдань і термінів.

Гібрид показників, спільних для всіх галузей,і показників, адаптованих до кожного елемента в межах галузі, може допомогти вирішити конкуруючі завдання. Показники ефективності повинні враховувати проміжні результати (наприклад, кількість оцінок або заходів) і кінцеві результати (наприклад, зниження ризиків або підвищення стійкості),а також оцінювати прогрес у досягненні поставлених цілей і завдань. Для документування програми безпеки та стійкості критичної інфраструктури, а також для визначення необхідних коригувань має бути передбачена регулярна звітність про результати діяльності.

Аналогічно, необхідно визначити процеси, системи та інструменти збору даних, а також аналітичні підходи. Це може бути складно, якщо загальна програма безпеки та стійкості критичної інфраструктури є добровільною, а дані вважаються власністю власників та операторів інфраструктури. Може бути корисною координація з наглядовими державними установами, особливо тими, які вже збирають інформацію про операційні показники конкретних секторів, оскільки вони, можливо, усунули деякі з бар'єрів для збору даних, принаймні на високому рівні.

Ціннісна пропозиція/Бізнес-кейс

- Вимірювання результативності стисло формулює ціннісну пропозицію або бізнес-кейс. Що компанії або уряди можуть очікувати отримати в результаті своєї участі в цьому процесі?
- Чи дізнаються вони більше про найкращі практики, які можуть зробити їх більш конкурентоспроможними? Чи зменшується їхня відповідальність? Чи є переваги від деяких заходів зі зменшення впливу на зміну клімату для повсякденної діяльності? Чи можуть органи місцевого самоврядування краще планувати витрати своїх ресурсів? Чи роблять вони помітний внесок у безпеку та стійкість своєї компанії та/або країни?
- Фіксація успіхів, досягнутих у результаті програми, та їх просування допоможуть сформувати ціннісну пропозицію або бізнес-кейс.

Вибрані ресурси

1. Сектор екстрених служб - Пакет планування безперервності (https://www.cisa.gov/emergency-services-sector-continuity-planning-suite).
2. Оцінки кібербезпеки. (https://www.cisa.gov/cybersecurity-assessments).
3. Національна консультативна рада з питань інфраструктури Оцінка та вдосконалення обміну та аналізу інформації: Заключний звіт та рекомендації. (https://www.cisa.gov/publication/niac-eval-enhance-info-sharing-final-report).

Популяризація Програми

Безпека та стійкість критичної інфраструктури впливає на кожного. Хоча не всі зацікавлені сторони залучені до більш детальних елементів програми, вони все одно потребують розуміння ризиків на високому рівні, щоб мати адекватну інформацію та більшу впевненість у своїх рішеннях щодо заходів зі зниження та управління ризиками - особливо тих, які можуть вимагати змін у їхній повсякденній діяльності та житті.

Зацікавлені сторони можуть включати окремі компанії, широку громадськість, місцеві органи влади та багато інших. Для охоплення цих різноманітних аудиторій можуть бути корисними маркетингові кампанії, такі як "Побач щось, скажи щось" у Сполучених Штатах. Ці зусилля успішно вийшли за рамки інфраструктурних партнерів, залучивши всю громаду і підвищивши їхню обізнаність про ситуацію. Інші інформаційно-просвітницькі заходи можуть спиратися на існуючі канали комунікації, що використовуються галузевими асоціаціями та торговельними групами.

Повідомлення для різних аудиторій повинні зосереджуватися на певних ключових тезах, які зрозумілою і простою мовою відображають суть проблеми, як вона зачіпає їхні інтереси, а також суть бажаних дій для кожної з цільових аудиторій. Що громадськість повинна розцінювати як підозрілу діяльність і як про неї повідомляти? До кого компаніям слід звертатися за додатковою інформацією про заходи безпеки та стійкості, а також про найкращі практики в конкретних галузях?
Як місцеві та регіональні органи влади можуть бути більш залученими?

Різні аудиторії повинні бути визначені таким чином, щоб наявні ресурси для інформаційно-роз'яснювальної роботи використовувалися ефективно і відображали роль кожної аудиторії в підвищенні безпеки та стійкості інфраструктури.

Канали зв'язку

- Веб-сторінки
- Соціальні мережі
- Навчання за допомогою Інтернету
- Громадські медіа
- Брифінги для керівників
- Технічні презентації та виставки на конференціях
- Семінари, адаптовані до різних аудиторій
- Галузеві публікації
- Електронні новинні організації
- Прес-релізи
- Спеціальні події

Вибрані ресурси

1. Репрезентативні інформаційно-просвітницькі матеріали можна знайти за посиланням: Веб-сторінка "Безпека рідного міста" (https://www.cisa.gov/hometown-security)
2. Веб-сторінка "Готовність активного стрільця" (https://www.cisa.gov/active-shooter-preparedness)
3. Веб-сторінка Управління із запобігання бомбуванню (https://www.cisa.gov/office-bombing-prevention-obp)
4. Веб-сторінка "Якщо ти щось бачиш, скажи щось" (https://www.dhs.gov/see-something-say-something)

Висновки

Критична інфраструктура є основою, від якої залежить щоденна життєдіяльність суспільства та економіки, і порушення або втрата будь-якого елементу критичної інфраструктури може серйозно вплинути на наше життя. Спільна робота та обмін передовими практиками, підходами та досвідом допоможуть зміцнити безпеку та стійкість критичної інфраструктури на національному та глобальному рівнях сьогодні та в майбутньому.