неофіційний переклад

NIPP 2013

Партнерство для безпеки та стійкості критичної інфраструктури

Цей текст є неофіційним перекладом документу розміщеного на відкритому інформаційному ресурсі Департаменту національної безпеки Сполучених Штатів Америки та може використовуватись лише з інформаційною та науковою метою
Посилання на офіційний оригінал документа
https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf

Зміст

Перелік малюнків та таблиць

Малюнки

Таблиці

Короткий зміст

Наш національний добробут залежить від безпечної та стійкої критичної інфраструктури — тих активів, систем і мереж, які є основою американського суспільства. Щоб досягти такої безпеки та стійкості, партнери з критичної інфраструктури повинні колективно визначати пріоритети, формулювати чіткі цілі, зменшувати ризики, вимірювати прогрес і адаптуватися на основі зворотного зв'язку та мінливого середовища. NIPP 2013: Партнерство для забезпечення безпеки та стійкості критичної інфраструктури (далі – Національний план) керує національними зусиллями з управління ризиками критичній інфраструктурі країни.

Спільнота, яка бере участь в управлінні ризиками критичній інфраструктурі, є широкою, складається з партнерства між власниками та операторами; Федеральних, державних, місцевих, племінних та територіальних органів влади; регіональних утворень; некомерційних організацій; та наукових кіл. Управління ризиками від значних загроз і небезпек фізичній та кібер- безпеці критичної інфраструктури вимагає комплексного підходу, щоб:

- ідентифікувати, стримувати, виявляти, попереджувати та готуватися до загроз і небезпек критичній інфраструктурі країни;
- зменшити вразливість критично важливих активів, систем і мереж; та
- пом'якшити потенційні наслідки інцидентів або несприятливих подій для критичної інфраструктури.

Успіх цього інтегрованого підходу залежить від використання повного спектру можливостей, знань і досвіду спільноти критичної інфраструктури та відповідних зацікавлених сторін. Це вимагає ефективного обміну корисною та актуальною інформацією між партнерами, щоб розвинути обізнаність про ситуацію та забезпечити ефективне прийняття рішень з урахуванням ризиків.

У лютому 2013 року Президент видав Президентську політичну директиву 21 (PPD-21) «Безпека та стійкість критичної інфраструктури», яка прямо вимагає оновлення Національного плану захисту інфраструктури (NIPP). Це оновлення ґрунтується на суттєвих змінах у ризиках, політиці та операційних середовищах критичної інфраструктури, а також набутому досвіді та уроках з часу останньої публікації NIPP у 2009 році. Національний план спирається на попередні NIPP, наголошуючи на додаткових цілях безпеки і стійкості критичної інфраструктури. Для досягнення цих цілей кібернетична та фізична безпека, а також стійкість критично важливих інфраструктурних активів, систем і мереж інтегровані в корпоративний підхід до управління ризиками.

Інтеграція планування фізичної та кібербезпеки узгоджується з виконавчим наказом 13636 «Покращення кібербезпеки критичної інфраструктури», який наказує федеральному уряду координувати дії з власниками та операторами критичної інфраструктури для покращення обміну інформацією та спільної розробки та впровадження підходів до кібербезпеки, що ґрунтуються на оцінці ризиків. В описі діяльності з управління ризиками в п'яти національних місіях готовності із запобігання, захисту, пом'якшення наслідків, реагування та відновлення, Національний план також узгоджується з національною системою готовності, передбаченою Президентською політичною директивою 8 (PPD-8) «Національна готовність».

У контексті ризиків, політики та операційного середовища сектор критичної інфраструктури та міжсекторальні партнерські структури забезпечують основу для спрямування колективних зусиль партнерів. Національні зусилля щодо посилення безпеки та стійкості критичної інфраструктури залежать від здатності державних і приватних власників і операторів критичної інфраструктури приймати рішення з урахуванням ризиків під час розподілу обмежених ресурсів як у стабільному, так і в кризовому режимі.

Цінність партнерства в рамках Національного плану починається з прямих переваг, пов'язаних із чіткою спільною зацікавленістю в забезпеченні безпеки та стійкості критичної інфраструктури країни. Це базове значення поширюється через мережу національних, регіональних, державних і місцевих партнерств між урядом, власниками та операторами, які відповідають за управління ризиками для підвищення безпеки та стійкості. Щоб будь-яке партнерство було ефективним, воно повинно приносити цінність своїм учасникам. Ціннісна пропозиція для уряду зрозуміла: координація із

зацікавленими сторонами інфраструктури має важливе значення для виконання урядового мандату щодо збереження громадської безпеки та забезпечення національної безпеки. Промисловість робить багато для забезпечення власної інфраструктури та добробуту громад, які вона обслуговує. Уряд може досягти успіху в заохоченні промисловості вийти за рамки того, що відповідає її комерційним інтересам, і інвестувати в національні інтереси шляхом активної участі в партнерських зусиллях.

Наприклад, уряд може надати приватному сектору доступ до своєчасної та дієвої інформації у відповідь на загрози та кризи, що розвиваються. Крім того, уряд може допомогти партнерам з приватного сектору отримати більш повне розуміння всього ландшафту ризиків, підвищуючи їхню здатність робити обґрунтовані та ефективні інвестиції в безпеку та стійкість. Нарешті, учасники індустрії отримують можливість допомагати державним планувальникам приймати кращі рішення щодо урядових ініціатив щодо безпеки та стійкості, що приносить переваги для критичних галузей промисловості та для країни в цілому. Оскільки критична інфраструктура країни в основному належить приватному сектору, управління ризиками для підвищення безпеки та стійкості є спільним пріоритетом для промисловості та уряду.

Національний план визначає бачення, місію та цілі, які підтримуються набором основних принципів, спрямованих на управління ризиками та партнерство для впливу на майбутнє планування безпеки та стійкості критичної інфраструктури на міжнародному, національному, регіональному рівнях, рівні штатів, місцевих, племінних, територіальних урядів, а також на рівні власника та оператора. Національний план базується на структурі управління ризиками критичній інфраструктурі, запровадженій у NIPP 2006 року. Ефективне управління ризиками вимагає розуміння критичності активів, систем і мереж, а також відповідних залежностей і взаємозалежностей критичної інфраструктури. З цією метою Національний план заохочує партнерів визначати критичні функції та ресурси, які впливають на їхні підприємства та спільноти, для підтримки планування готовності та розвитку можливостей.

Основою Національного плану є Заклик до дії, який спрямовує спільні зусилля спільноти критичної інфраструктури для підвищення безпеки та стійкості за трьома широкими категоріями діяльності: розвиток партнерських зусиль; інновації в управлінні ризиками; зосередження на результатах. Заклик до дії забезпечує стратегічне спрямування національних зусиль у найближчі роки шляхом скоординованої та гнучкої реалізації федеральними департаментами та відомствами — у співпраці з урядами штатів, місцевими, племінними та територіальними урядами, регіональними партнерами та партнерами з приватного сектора, якщо це доцільно. Цей Національний план, орієнтований на результати, полегшує оцінку прогресу на шляху до безпеки та стійкості критичної інфраструктури через його цілі та пріоритети та пов’язані з ними результати та результати.

Підсумовуючи, Національний план описує національну єдність зусиль для досягнення безпеки та стійкості критичної інфраструктури. Враховуючи різноманітність повноважень, ролей і обов’язків партнерів з критичної інфраструктури, для забезпечення оптимальної безпеки та стійкості критичної інфраструктури необхідне проактивне та інклюзивне партнерство між усіма рівнями влади, приватним і некомерційним секторами. Ґрунтуючись на вказівках у Національному плані, партнерство встановлюватиме та переслідуватиме ряд спільних цілей і національних пріоритетів, а також використовуватиме спільні структури та механізми, які сприятимуть обміну інформацією та спільному вирішенню проблем.

1. Вступ

Наше національне благополуччя залежить від безпечної та стійкої критичної інфраструктури — тих активів, систем і мереж, які є опорою американського суспільства. Метою NIPP 2013: Партнерство для забезпечення безпеки та стійкості критичної інфраструктури (далі – Національний план) є керівництво національними зусиллями з управління ризиками критичній інфраструктурі країни. Для досягнення цієї мети партнери з критичної інфраструктури повинні колективно визначити національні пріоритети; формулювати чіткі цілі; зменшити ризик; виміряти прогрес; і адаптуватися на основі зворотного зв'язку та мінливого середовища. Успіх у цій складній справі дає змогу використовувати повний спектр можливостей, знань і досвіду міцного партнерства.

Цей Національний план базується на та замінює Національний план захисту інфраструктури 2009 року та визнає цінний прогрес, досягнутий на сьогодні у захисті критичної інфраструктури країни. Він відображає зміни в ризиках, політиці та операційному середовищі критичної інфраструктури та ґрунтується на необхідності інтегрувати кібернетичні, фізичні та людські елементи критичної інфраструктури в управління ризиками. Національний план керує національними зусиллями, стимулює прогрес і залучає ширшу спільноту до важливості безпеки та стійкості критичної інфраструктури.

Аудиторія цього плану включає широку спільноту критичної інфраструктури, що складається з державних і приватних власників і операторів критичної інфраструктури; Федеральні департаменти та агентства, включно з секторальними агентствами (SSA); уряди в штатах, місцеві, племінні та територіальні уряди (SLTT); регіональні утворення; та інші приватні та некомерційні організації, відповідальні за забезпечення та посилення стійкості критичної інфраструктури.

Управління ризиками критичній інфраструктурі вимагає інтегрованого підходу в цій широкій спільноті, щоб:

- ідентифікувати, стримувати, виявляти, попереджувати та готуватися до загроз і небезпек критичній інфраструктурі країни;
- зменшити вразливість критично важливих активів, систем і мереж; та
- пом'якшити потенційні наслідки інцидентів або несприятливих подій для критичної інфраструктури.

Враховуючи різноманітність повноважень, ролей і обов'язків партнерів з критичної інфраструктури, для підвищення безпеки та стійкості критичної інфраструктури потрібні гнучкі, проактивні та інклюзивні партнерства. Президентська політична директива 21 (PPD-21) зазначає: «Власники та оператори критичної інфраструктури мають унікальні можливості керувати ризиками для своїх окремих операцій та активів, а також визначати ефективні стратегії, щоб зробити їх більш безпечними та стійкими». Індивідуальні зусилля з управління ризиками посилюються спільним державно-приватним партнерством, яке функціонує як єдине національне зусилля, на відміну від ієрархічної командно-контрольної структури. PPD-21 наголошує на розподіленому характері критичної інфраструктури, а також на різноманітних повноваженнях і обов'язках партнерів, зазначаючи, що критична інфраструктура включає «розподілені мережі, різноманітні організаційні структури та операційні моделі (включаючи багатонаціональну та міжнародну власність), взаємозалежні функції та системи як в фізичному просторі, так і в кіберпросторі, а також конструкції управління, які включають багаторівневі органи влади, обов'язки та правила»[1]. Національний план визнає, що державно-приватна співпраця будується на надійному середовищі, де процеси обміну інформацією покращують обізнаність про ситуацію та залишаються відкритими та прозорими, захищаючи приватне життя та громадянські свободи.

Національний план враховує різні перспективи управління ризиками державного та приватного секторів, де держава та приватний сектор мають узгоджені, але не ідентичні інтереси щодо забезпечення критичної інфраструктури та підвищення її стійкості. Він використовує порівняльні переваги як приватного, так і державного секторів для взаємної вигоди. Національний план організовано таким чином:

- **Розіл 2 – Бачення, місія та цілі** – Викладає бачення, місію та цілі спільноти критичної інфраструктури.
- **Розділ 3 – Середовище критичної інфраструктури** – Описує політику, ризики та робоче середовище, а також структуру партнерства, в рамках якої спільнота докладає зусиль для досягнення цілей, спрямованих на посилення

[1] Білий дім, Президентська політична директива 21 – Безпека та стійкість критичної інфраструктури, http://www.whitehouse.gov/the-press-office/2013/02/12/ Presidential-policy-directive-critical-infrastructure-security-and -resil, доступ надано 24 вересня 2013 р.

безпеки та стійкості.

- **Розділ 4 – Основні принципи** – Описує принципи та припущення, які лежать в основі цього національного плану.
- **Розділ 5 – Співпраця для управління ризиками** – Описує загальну структуру діяльності з управління ризиками, яку проводить спільнота критичної інфраструктури в контексті національної готовності.
- **Розділ 6 – Заклик до дії** – Закликає спільноту критичної інфраструктури (відповідно до повноважень, обов'язків і бізнес-середовища) вживати наскрізних, активних і скоординованих дій, які підтримують колективні зусилля для посилення безпеки та стійкості критичної інфраструктури в найближчі роки.
- **Глосарій**
- **Скорочення**

Кілька додаткових ресурсів будуть запропоновані для надання вказівок і допомоги спільноті критичної інфраструктури в рамках виконання Національного плану. Ці додатки будуть окремими ресурсами та включатимуть, серед інших тем, виконання підходу до управління ризиками критичної інфраструктури; підключення до Національного центру інтеграції кібербезпеки та комунікацій (NCCIC) та Національного координаційного центру інфраструктури (NICC); ресурси для оцінки вразливості; і включення стійкості до критичних інфраструктурних проєктів. Вони будуть доступні онлайн і регулярно оновлюватимуться для легкого доступу спільноти критичної інфраструктури.

Вдосконалення NIPP 2013 порівняно з NIPP 2009

Національний план продовжує зосереджуватися на управлінні ризиками як основі безпеки та стійкості критичної інфраструктури та сприяє партнерству як ключовому механізму управління ризиками. Таким чином, він підтверджує роль різних координаційних структур, включаючи секторальні координаційні ради, урядові координаційні ради та міжсекторальні ради. Спираючись на прогрес, досягнутий цими радами та іншими органами за останні 10 років у напрямку безпеки та стійкості критичної інфраструктури, NIPP 2013:

- посилює безпеку та стійкість як головну мету планування внутрішньої безпеки критичної інфраструктури;
- оновлює структуру управління ризиками критичної інфраструктури та вирішує питання узгодження з національною системою готовності у сферах запобігання, захисту, пом'якшення, реагування та відновлення;
- зосереджується на створенні процесу визначення національних пріоритетів критичної інфраструктури, визначених спільно державним і приватним секторами;
- інтегрує зусилля з кібер- та фізичної безпеки та стійкості в корпоративний підхід до управління ризиками;
- підтверджує, що заходи безпеки та стійкості критичної інфраструктури вимагають міжнародної співпраці;
- підтримує виконання Національного плану та досягнення Національної цілі готовності як на національному рівні, так і на рівні громади, зосереджуючись на залученні регіональних спільних зусиль; і
- представляє детальний Заклик до дії з кроками, які будуть здійснені відповідно до пріоритетів кожного сектору та у співпраці з партнерами з критичної інфраструктури, щоб досягти прогресу на шляху до безпеки та стійкості.

2. Бачення, місія та цілі

Стратегічний напрямок зусиль із створення та підтримки безпеки та стійкості критичної інфраструктури визначається спільним баченням і місією.

Бачення

Країна, в якій постійно забезпечується фізична та кібер-безпека критичної інфраструктури, а сама критична інфраструктура залишається стійкою, зі зниженою вразливістю, мінімізованими наслідками, виявленням і попередженням загроз, прискореним реагуванням і відновленням.

Місія

Зміцнити безпеку та стійкість критичної інфраструктури країни, керуючи фізичними та кібер- ризиками за допомогою спільних та інтегрованих зусиль спільноти критичної інфраструктури.

Бачення та місія залежать від досягнення цілей, які представляють стратегічний напрям, на якому має бути зосереджена діяльність критичної інфраструктури протягом наступних кількох років.

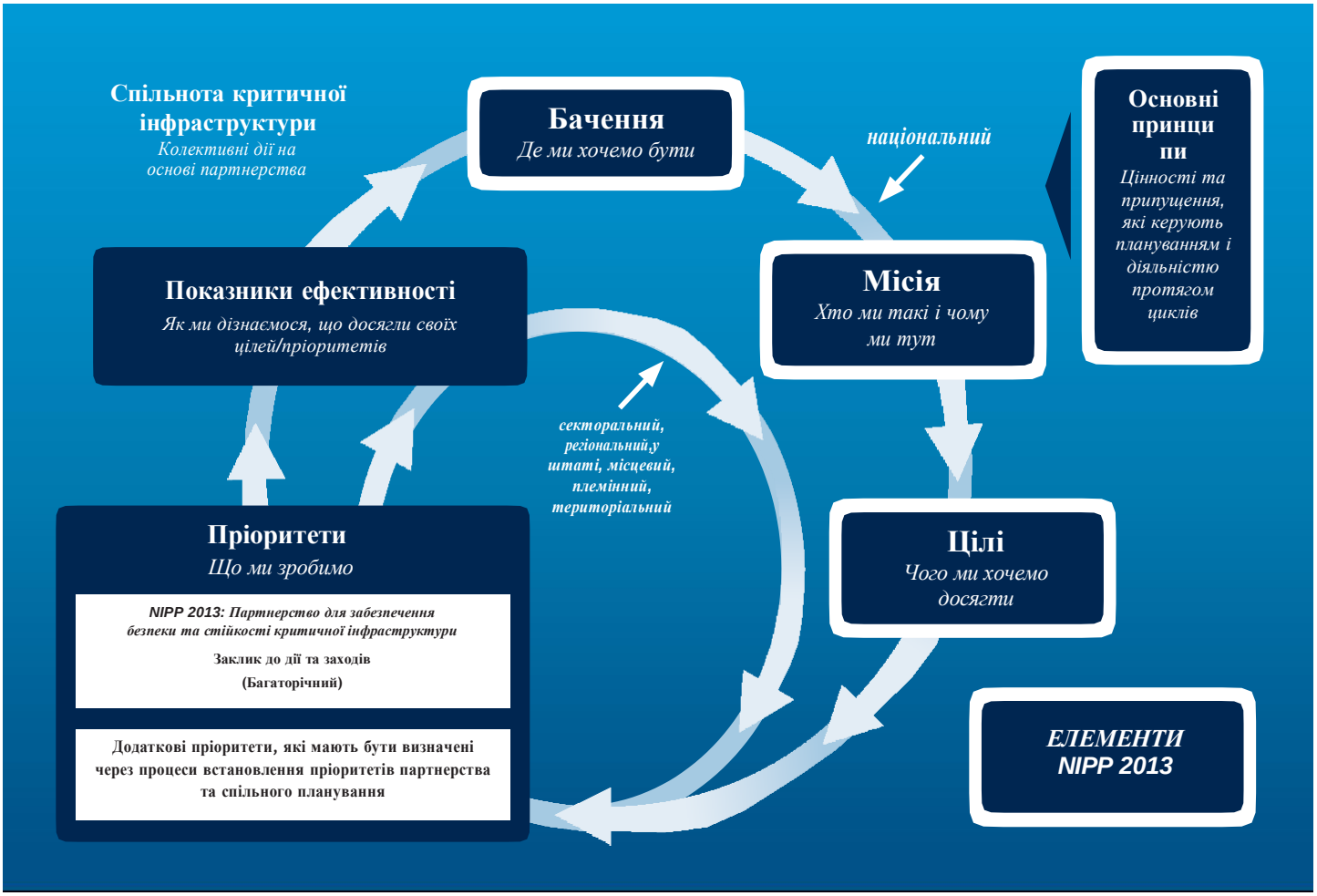
Цілі

- Оцінювати та аналізувати загрози, вразливі місця та наслідки для критичної інфраструктури для інформування про заходи з управління ризиками;
- Забезпечувати безпеку критично важливої інфраструктури від людських, фізичних і кіберзагроз за допомогою постійних зусиль, спрямованих на зниження ризиків, враховуючи при цьому витрати та переваги інвестицій у безпеку;
- Посилювати стійкість критичної інфраструктури шляхом мінімізації несприятливих наслідків інцидентів шляхом попереднього планування та заходів із пом'якшення наслідків, а також застосування ефективних заходів для порятунку життів і забезпечення швидкого відновлення основних послуг;
- Обмінюватися корисною та актуальною інформацією між спільнотою критичної інфраструктури для підвищення обізнаності та прийняття рішень з урахуванням ризиків; та
- Сприяти засвоєнню інформації та адаптації під час і після навчань та інцидентів.

Ці цілі будуть доповнені регулярною розробкою більш конкретних пріоритетів партнерством у сфері критичної інфраструктури, пов'язаних з управлінням ризиками та підвищенням можливостей.

На основі бачення, місії та цілей спільнота критичної інфраструктури працюватиме спільно, щоб визначити конкретні національні пріоритети, враховуючи при цьому доступність ресурсів, уже досягнутий прогрес, відомі прогалини в можливостях і нові ризики. Такі пріоритети повинні стимулювати дії на національному рівні та будуть доповнені галузевими, регіональними та SLTT пріоритетами. Показники ефективності будуть встановлені на основі цілей і пріоритетів. Національний щорічний звіт і Національний звіт про готовність включають вимірювання прогресу, що допоможе створити загальне розуміння стану безпеки критичної інфраструктури та заходів щодо стійкості. Взаємозв'язок цих елементів зображено на малюнку 1.

Малюнок 1 – Підхід Національного плану до побудови та підтримки єдності зусиль



3. Середовище критичної інфраструктури

Цей Національний план спирається на кілька ключових концепцій, які залишаються узгодженими з NIPP 2009 року. У той же час План базується на інформації та оновлюється, щоб відобразити мінливі ризики критичної інфраструктури, політику та робоче середовище. У цьому розділі описано зміни в середовищі критичної інфраструктури з моменту публікації останнього NIPP, водночас підтверджуючи важливість успішної співпраці між основною партнерською структурою для управління ризиками.

Ключові концепції

Ключові концепції, описані нижче, надають контекст для цього середовища критичної інфраструктури. Розуміння цих ключових концепцій впливає на стан критичної інфраструктури та формує підхід спільноти до забезпечення безпеки та стійкості.

- **Критична інфраструктура** представляє собою системи та активи, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що порушення функціонування або знищення таких систем і активів матиме виснажливий вплив на безпеку, національну економічну безпеку, охорону здоров'я чи громадську безпеку або будь-яке їх поєднання. Національний план визнає, що критично важлива інфраструктура країни в основному належить і керується приватним сектором, однак федеральний уряд і уряд SLTT також володіють і керують критичною інфраструктурою, як і іноземні організації та компанії.
- Президентська політична директива 21 (PPD-21) визначає **безпеку** як «зменшення ризику для критичної інфраструктури за допомогою фізичних засобів або захисних кіберзаходів від вторгнень, атак або наслідків природних чи техногенних катастроф». Існує кілька елементів захисту систем критичної інфраструктури, зокрема усунення загроз і вразливостей, а також обмін точною інформацією та аналіз поточних і майбутніх ризиків. Діяльність із запобігання та захисту сприяє посиленню безпеки критичної інфраструктури.
- PPD-21 визначає **стійкість** як «здатність готуватися до мінливих умов і адаптуватися до них, протистояти збоям і швидко відновлюватися після них... [вона] включає здатність протистояти навмисним нападам, нещасним випадкам, стихійним лихам або природним інцидентам». Наявність точної інформації та аналізу ризиків має важливе значення для досягнення стійкості. Стійкі активи, системи та мережі інфраструктури також мають бути надійними, гнучкими та адаптованими. Діяльність із пом'якшення, реагування та відновлення сприяє посиленню стійкості критичної інфраструктури.
- Безпека та стійкість зміцнюються завдяки управлінню ризиками. **Ризик** стосується «потенціалу небажаного результату через інцидент чи події, який визначається його ймовірністю [функцією загроз і вразливостей] і пов'язаними наслідками;» **управління ризиками** – це «процес виявлення, аналізу та передачі інформації про ризик, а також прийняття, уникнення, перенесення або контролю за ним до прийнятного рівня за прийнятну вартість».
- **Партнерські відносини** дозволяють ефективніше та результативніше управляти ризиками. У контексті цього Національного плану партнерство визначається як тісна співпраця між сторонами, які мають спільні інтереси в досягненні спільного бачення. Для спільноти критичної інфраструктури залучення керівництва, відкрите спілкування та довірчі стосунки є важливими елементами партнерства.
-

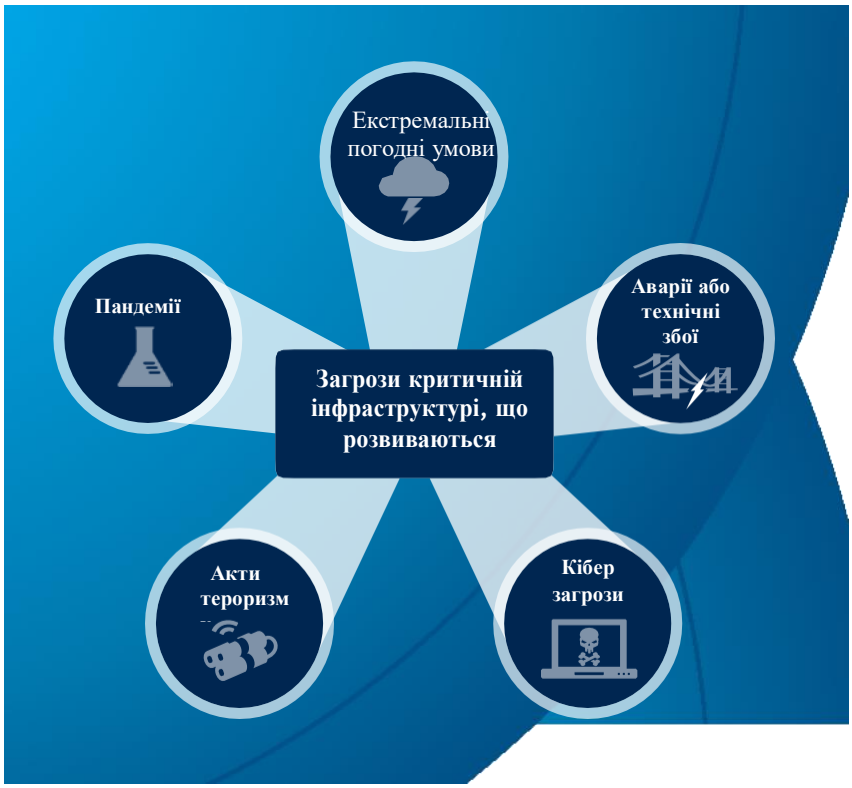
Середовище ризику

Середовище ризику, що впливає на критичну інфраструктуру, є складним і невизначеним; загрози, вразливості та наслідки змінилися протягом останніх 10 років. Наприклад, критична інфраструктура, яка протягом тривалого часу наражалася на ризики, пов'язані з фізичними загрозами та стихійними лихами, тепер все більше піддається кіберризикам, що пов'язано з дедалі більшою інтеграцією інформаційних та комунікаційних технологій у роботу критичної інфраструктури, а також з тим, що противник зосереджується на використанні потенційних кібервразливостей. На малюнку 2 показано загрози критичній інфраструктурі, що розвиваються.

Стратегічна національна оцінка ризиків (SNRA) визначає чисельні загрози та небезпеки національній безпеці в широких категоріях спричинених людиною, природних і технологічних/випадкових загроз. Критично важливі активи, системи та мережі стикаються з багатьма загрозами, класифікованими SNRA, включаючи терористів та інших суб'єктів, які прагнуть завдати шкоди та перервати надання основних послуг через фізичні та кібер-атаки, суворі погодні явища, пандемію грипу чи інші кризові ситуації зі здоров'ям, а також потенційні аварії та збої через те, що інфраструктура працює понад запланований термін служби. Можливість виникнення взаємопов'язаних подій із невідомими наслідками додає невизначеності на додаток до відомих ризиків, які аналізуються в рамках SNRA.

Зростаюча взаємозалежність між системами критичної інфраструктури, зокрема залежність від інформаційних і комунікаційних технологій, збільшила потенційну вразливість до фізичних і кібер-загроз і потенційні наслідки в результаті компрометації базових систем або мереж.

Малюнок 2 – Загрози критичній інфраструктурі, що розвиваються



У все більш взаємопов'язаному світі, де критична інфраструктура перетинає національні кордони та глобальні ланцюги поставок, потенційні наслідки зростають із цими взаємозалежностями та здатністю різноманітних загроз використовувати їх.

Крім того, наслідки екстремальних погодних умов становлять значний ризик для критично важливої інфраструктури — підвищення рівня моря, сильніші шторми, екстремальні та тривалі умови посухи та сильні повені разом загрожують інфраструктурі, яка надає основні послуги американському населенню. Поточні та майбутні зміни клімату можуть посилити ці ризики та мати серйозний вплив на роботу інфраструктури.

Нарешті, вразливість також може існувати в результаті виходу на пенсію робочої сили або нестачі кваліфікованої робочої сили. Кваліфіковані оператори необхідні для обслуговування інфраструктури, а отже, безпеки та стійкості. Такі фактори впливають на середовище ризику та разом із політичним та операційним середовищами створюють основу для прийняття рішень щодо безпеки та стійкості критичної інфраструктури.

Політичне середовище

У розділі II Акту про внутрішню безпеку 2002 року (зі змінами) детально визначено обов'язки Департаменту внутрішньої безпеки (DHS) щодо безпеки та стійкості критичної інфраструктури. Згідно з Актом на DHS покладено повноваження щодо розробки комплексного плану захисту критичної інфраструктури країни. DHS завершив першу версію NIPP у 2006 році та випустив оновлення у 2009 році. З 2009
формувати спосіб, у який нація вирішує питання безпеки та ст
готовності.

- Хімічний
- Комерційні об'єкти
- Комунікаційний
- Критичне виробництво
- Дамби
- Оборонно-промисл. база
- Служби екстреної доп.
- Енергетичний
- Фінансові послуги
- Харчування та с/г
- Державні установи
- Охорона здоров'я
- Інформаційні технології
- Ядерні реактори, матеріали та відходи
- Транспортні системи
- Системи водопостачання та водовідведення

12 лютого 2013 року Президент видав PPD-21 (Президентську політичну директиву) «Безпека та стійкість критичної інфраструктури», яка передбачає розробку оновленого національного плану. Директива описує національні зусилля щодо обміну інформацією про загрози, зменшення вразливостей, мінімізації наслідків і прискорення реагування на загрози та відновлення критичної інфраструктури. PPD-21 також визначає 16 секторів критичної інфраструктури, наведені в блоці праворуч.

У лютому 2013 року Президент прийняв Указ 13636 «Покращення кібербезпеки критичної інфраструктури», який закликає федеральний уряд тісно координувати роботу з власниками та операторами критичної інфраструктури для покращення обміну інформацією про кібербезпеку та для спільної розробки та впровадження підходів до забезпечення кібербезпеки, заснованих на оцінці ризиків.
Указ покладає на федеральний уряд обов'язки розробити технологічно нейтральну структуру кібербезпеки для зменшення кіберризику критичній інфраструктурі; заохочувати впровадження надійних практик з кібербезпеки; збільшити обсяг, забезпечувати своєчасність та якість інформації щодо кіберзагроз, якою обмінюються; і включити захист конфіденційності та свобод громадян в ініціативи безпеки та стійкості критичної інфраструктури.

Національний план узгоджується з ціллю PPD-8 «Національна готовність» щодо «безпечної та стійкої нації з можливостями, необхідними для всієї спільноти, щоб запобігати, захищати від, пом'якшувати, реагувати на загрози та небезпеки та відновлюватися після них». Ці п'ять напрямів діяльності, зазначені в PPD-8, є центральними для комплексного підходу до підвищення національної готовності, а заходи з управління ризиками критичній інфраструктурі в усіх п'яти напрямах сприяють досягненню цілі національної готовності. Крім того, Національний план узгоджується з національними рамками планування та міжвідомчими оперативними планами, розробленими відповідно до PPD-8. Сфера застосування Національного плану не спрямована на впровадження та виконання попереджувальних заходів, як описано у Федеральному міжвідомчому оперативному плані з попередження, і не змінює їх. Проте сфера застосування Національного плану включає заходи, які часто пов'язані з та підтримують попереджувальні заходи, спрямовані на уникнення, запобігання або припинення неминучої загрози чи фактичних атак.

Два додаткові політичні документи, які узгоджуються з цим Національним планом, включають Президентський план дій щодо

клімату, прийнятий у червні 2013 року, та Національну стратегію обміну інформацією та збереження інформації (NSISS), прийняту в грудні 2013 року. План дій щодо клімату встановлює низку стратегічних цілей і зобов'язує федеральні агентства вжити подальших заходів для кращої підготовки Америки до наслідків зміни клімату, включаючи посилення стійкості інфраструктури. NSISS визначає як один із 16 національних пріоритетів необхідність створення «процесів обміну інформацією та протоколів для окремих секторів з партнерами з приватного сектору, щоб покращити якість і своєчасність інформації та захистити інфраструктуру країни».

Операційне середовище

Ступінь взаємозалежності інфраструктури формує середовище для безпеки та стійкості критичної інфраструктури, вимагаючи співпраці як у плануванні, так і в діях. Критична інфраструктура країни стала набагато більш взаємозалежною, продовжуючи перехід від операційного середовища, яке характеризується розрізненими активами, системами та мережами, до середовища, в якому хмарні обчислення, мобільні пристрої та бездротове підключення різко змінили спосіб роботи інфраструктури. Взаємозалежності можуть бути операційними (наприклад, потужність, необхідна для роботи водонасосної станції) або фізичними (наприклад, розміщена інфраструктура, така як водопровідні та електричні лінії, що проходять під прольотом мосту). Взаємозалежності можуть обмежуватися невеликими міськими чи сільськими районами або охоплювати великі регіони, перетинаючи юрисдикційні та національні кордони, включаючи інфраструктуру, яка вимагає точного позиціонування, навігації та часу (PNT). Послуги PNT мають вирішальне значення для роботи багатьох секторів критичної інфраструктури та життєво важливі для реагування на інциденти.

Країна отримала вигоду від інвестицій в посилення безпеки та стійкості власниками та операторами як державного, так і приватного секторів. Значна частина спільноти критичної інфраструктури продовжує інтегрувати кібербезпеку в основні бізнес-практики, роблячи значні інвестиції для посилення безпеки та стійкості. Однак в інших сферах, незважаючи на витрати державного та приватного секторів на експлуатацію та підтримку систем критичної інфраструктури, рівень інвестицій був недостатнім, про що свідчить погіршення стану багатьох систем інфраструктури. Національна академія наук повідомила, що попередні значні інвестиції країни в проєктування, будівництво та експлуатацію систем критичної інфраструктури — водопостачання, водовідведення, енергетики, транспорту та телекомунікацій — не були забезпечені коштами, необхідними для збереження цих систем у хорошому стані або їх модернізації, щоб задовольнити потреби зростаючого та мінливого населення.

Активи, системи та мережі критичної інфраструктури, а також інші ключові ресурси знаходяться в певних юрисдикціях, але отримана ними інформація, продукти, послуги та функції можуть надаватися по всьому світу. Природа володіння та експлуатації критичної інфраструктури також розподілена, а потреба у спільному плануванні та інвестиціях стає все більш поширеною та необхідною на міжнародному рівні. Такі глобальні зв'язки визначають спосіб, яким спільнота критичної інфраструктури має планувати спільну роботу всередині та між секторами, а також через юрисдикції та національні кордони, щоб підвищити безпеку та стійкість критичної інфраструктури. Інформаційна безпека та конфіденційність також визначають операційне середовище. Зростаюча доступність даних та інформації, необхідних для експлуатації та підтримки інфраструктури та пов'язаних технологій, забезпечує доцільніші та ефективніші практики. Ця інформація вразлива до несанкціонованого доступу, який може вплинути на її конфіденційність, цілісність або доступність. Розповсюдження такої інформації серед тих організацій, які можуть використовувати її для доцільного та ефективного управління ризиками, залишається проблемою. Важливо підтримувати доступність інформації та розповсюджувати її тим, хто може використовувати та захищати її належним чином. Це передбачає прозорість практики обміну інформацією; захист джерел і методів; а також забезпечення конфіденційності та захисту громадянських свобод, а також можливість проведення розслідувань правоохоронними органами.

Це комплексне середовище підкреслює складність забезпечення та посилення стійкості критичної інфраструктури країни. Через динамічний характер цього середовища здатність постійно співпрацювати, щоб скористатися перевагами унікальних навичок і здібностей у спільноті, залишається основою для зусиль із забезпечення безпеки та стійкості критичної інфраструктури.

Структура партнерства

Добровільна співпраця між власниками та операторами приватного сектору (включно з їхніми партнерськими асоціаціями, постачальниками та іншими) та їхніми державними партнерами була і залишатиметься основним механізмом для просування колективних дій щодо безпеки та стійкості національної критичної інфраструктури. Під

час реалізації своєї ролі у національній і внутрішній безпеці Федеральний уряд повинен робити економічні розрахунки ризику, враховуючи при цьому багато неекономічних значень, наприклад, проблеми конфіденційності. У результаті держава може мати нижчу толерантність до ризику безпеки, ніж комерційна організація. Обидва варіанта є виправданими, але в світі, в якому промисловість і уряд покладаються на критичну інфраструктуру і де промисловість може перебувати на передовій національної оборони, наприклад, під час кібератаки, необхідно розвинути стійке партнерство для розгляду обох варіантів.

Оскільки природа середовища ризику критичної інфраструктури не дозволяє будь-якій одній організації самостійно управляти ризиками, партнери отримують вигоду від доступу до знань і можливостей, які інакше були б для них недоступні. Багато секторів критичної інфраструктури працюють над встановленням стабільних і представницьких партнерств, керуючи змінами в керівництві та розширюючи коло членів і набір навичок, необхідних для досягнення спільних цілей. Крім того, через довірчі відносини і обмін інформацією, федеральні агентства краще розуміють ризики та стан готовності, пов'язані з критичною інфраструктурою. Це дозволяє організаціям приймати більш обґрунтовані рішення під час визначення та вирішення пріоритетів національної критичної інфраструктури. Участь у цих зусиллях ґрунтується на чіткій та спільній зацікавленості в забезпеченні безпеки та стійкості критичної інфраструктури країни та розумінні порівняльних переваг, які кожен елемент партнерства може принести для досягнення цих спільних інтересів.

Національний план організовує критичну інфраструктуру в 16 секторів і призначає федеральний департамент або агентство як головного координатора — секторальне агентство (SSA) — для кожного сектора (ролі та обов'язки SSA див. у Додатку B). Структури галузевих і міжгалузевих партнерських рад, описані в попередніх NIPP, залишаються основою для цього Національного плану та зображені в таблиці 1.

Таблиця 1 – Секторальні та міжсекторальні координаційні структури ***(оригінал знизу)***

		Консультативна рада партнерства з критичної інфраструктури		
Сектор критичної інфраструктури	**Секторальні агентства**	**Секторальні координаційні ради**	**Урядові координаційні ради**	**Регіональний консорціум**
Хімічний	Департамент внутрішньої безпеки	Міжсекторальна рада критичної інфраструктури	Координаційна рада штату, місцевого, племінного та територіального урядів, Федеральна рада вищого керівництва	Регіональна координаційна рада консорціуму
Комерційні об'єкти*				
Комунікаційний*				
Критичне виробництво				
Дамби				
Служби екстреної допомоги*				
Інформаційні технології*				
Ядерні реактори, матеріали та відходи				
Харчування та сільське господарство	Департамент сільського господарства, Департамент охорони здоров'я та соціальних служб			
Оборонно-промислова база*	Департамент оборони			
Енергетичний*	Департамент енергетики			

Охорона здоров’я*	Департамент охорони здоров'я та соціальних служб			
Фінансові послуги*	Департамент казначейства	Використовує окрему координаційну установу		
Системи водопостачання та водовідведення*	Агентство охорони навколишнього середовища	Міжсекторальна рада критичної інфраструктури		
Державні установи	Департамент внутрішньої безпеки, Адміністрація загального обслуговування	Секторальні координаційні ради відсутні		
Транспортні системи*	Департамент внутрішньої безпеки, Департамент транспорту	Різні секторальні координаційні ради, розподілені за видами транспорту або підсекторами.		
* - вказує на те, що сектор має призначену організацію для обміну інформацією.				

Таблиця 1 – Секторальні та міжсекторальні координаційні структури *(переклад зверху)*

		Консультативна рада партнерства з КІ		
Critical Infrastructure Sector	**Sector Specific Agency**	**Sector Coordinating Councils (SCCs)**	**Government Coordinating Councils (GCCs)**	**Regional Consortia**
Chemical	Department of Homeland Security	3	3	
Commercial Facilities ⓘ		3	3	
Communications ⓘ		3	3	
Critical Manufacturing		3	3	
Dams		3	3	
Emergency Services ⓘ		3	3	
Information Technology ⓘ		3	3	
Nuclear Reactors, Materials & Waste		3	3	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	3	3	
Defense Industrial Base ⓘ	Department of Defense	3	3	
Energy ⓘ	Department of Energy	3	3	
Healthcare & Public Health ⓘ	Department of Health and Human Services	3	3	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	3	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	3	3	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	3	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	3	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Структура секторальних та міжсекторальних рад:

- **Секторальні координаційні ради (SCCs)** – Самоорганізовані, самокеровані та самоврядні ради приватного сектора, що складаються з власників, операторів та їхніх представників, які взаємодіють у широкому діапазоні секторальних стратегій, політики, діяльності та питань. SCC служать основними точками співпраці між урядом і власниками та операторами приватного сектору для координації та планування політики безпеки критичної інфраструктури та стійкості, а також низки пов'язаних секторальних заходів.
- **Міжсекторальна рада критичної інфраструктури** – Ця рада приватного сектору, що складається з голів і заступників голів SCC, координує міжгалузеві питання, ініціативи та взаємозалежності для підтримки безпеки та стійкості критичної інфраструктури.
- **Урядові координаційні ради (GCCs)** – Ці ради, що складаються з представників різних рівнів влади (включно з федеральним і SLTT), залежно від умов діяльності кожного окремого сектора, забезпечують міжвідомчу, міжурядову та міжюрисдикційну координацію всередині та між секторами та співпрацюють із SCC з питань державно-приватних засад.
- **Федеральна рада вищого керівництва (FSLC)** – FSLC, до складу якої входять високопосадовці з SSA та інших федеральних департаментів і відомств, які відповідають за безпеку та стійкість критичної інфраструктури, сприяє комунікації та координації питань з безпеки та стійкості критичної інфраструктури в межах федерального уряду.
- **Координаційна рада штату, місцевого, племінного та територіального урядів (SLTTGCC)** – SLTTGCC, що складається з представників усіх державних установ SLTT, сприяє залученню партнерів SLTT до національної безпеки критичної інфраструктури та зусиль із забезпечення стійкості та забезпечує організаційну структуру для координації вказівок, стратегій і програм державних і місцевих органів влади між юрисдикціями.
- **Регіональна координаційна рада консорціуму (RC3)** – Включає регіональні групи та коаліції по всій країні, які беруть участь у різноманітних ініціативах для покращення безпеки та стійкості критичної інфраструктури в державному та приватному секторах.
- **Організації обміну інформацією** – Організації, включаючи Центри обміну та аналізу інформації (ISAC), виконують операційні функції та функції розповсюдження для багатьох секторів, підсекторів та інших груп, а також сприяють обміну інформацією між урядом і приватним сектором. ISAC також співпрацюють на міжгалузевій основі через національну раду.

Примітка: Додаток А далі описує функції вищезазначених партнерських структур, а також додаткових структур, які підтримують безпеку та стійкість національної критичної інфраструктури.

Описаний вище секторальний і міжсекторальний партнерський підхід розроблений таким чином, щоб бути масштабованим і дозволяти окремим власникам і операторам критичної інфраструктури та іншим зацікавленим сторонам по всій країні брати участь. Він призначений для сприяння узгодженості процесу для забезпечення ефективної співпраці між розрізненими частинами співтовариства критичної інфраструктури, одночасно дозволяючи використовувати інші життєздатні структури партнерства та процеси планування. Ця концепція виявилася успішною та може бути використана на рівні штату, місцевому, племінному та територіальному рівнях, а також усередині та між регіонами для побудови, формування або розширення існуючих мереж; визначити перевірені практики; адаптуватися до отриманих уроків або перейняти їх; і за потреби використовуйте практики, процеси чи плани.

Багато з перерахованих структур використовують переваги Консультативної ради партнерства з критичної інфраструктури (CIPAC). Секретар внутрішньої безпеки заснував CIPAC у 2006 році як механізм для прямої підтримки інтересів секторів брати участь у публічно-приватних обговореннях критичної інфраструктури та брати участь у широкому спектрі заходів. CIPAC виключає зустрічі партнерів із Закону про Федеральний консультативний комітет (FACA), що дозволяє державно-приватній спільноті критичної інфраструктури брати участь у відвертому або делікатному діалозі для пом'якшення вразливості критичної інфраструктури та зменшення впливу загроз, що розвиваються або виникають. Зокрема, форуми CIPAC підтримують обговорення федеральним урядом критичних питань інфраструктури, які необхідні для досягнення консенсусу або під час надання офіційних рекомендацій. CIPAC також може використовуватися на рівні сектору, міжсектору або робочої групи, залежно від теми та мети обговорення. Інші федеральні агентства також можуть мати та використовувати комітети та консультативні ради, звільнені від FACA, для взаємодії з приватним сектором; однак модель CIPAC забезпечує правову основу для міжсекторальної співпраці.

4. Основні принципи

Національний план визначає сім основних принципів, що представляють цінності та припущення, які спільнота критичної інфраструктури має враховувати (на національному, регіональному, SLTT, а також на рівнях власника та оператора) під час планування безпеки та стійкості критичної інфраструктури.

1. Ризики необхідно визначати та керувати ними скоординованим і комплексним способом у межах спільноти критичної інфраструктури, щоб забезпечити ефективний розподіл ресурсів безпеки та стійкості.

   Спільне управління ризиками вимагає обміну інформацією (включаючи розумні практики), сприяння більш ефективному та результативному використанню ресурсів і мінімізації дублювання зусиль. Це дає змогу розробляти та впроваджувати більш комплексні заходи для захисту від загроз, знищення та підготовки до них; зменшення вразливості; і зменшення наслідків по всій країні. Щоб забезпечити комплексний підхід до управління ризиками, спільнота критичної інфраструктури розглядає стратегії досягнення пом'якшення ризиків, а також інші способи розгляду ризиків, включаючи прийняття, уникнення або передачу.

2. Розуміння та усунення ризиків, пов'язаних із міжсекторальними залежностями та взаємозалежностями, має важливе значення для посилення безпеки та стійкості критичної інфраструктури.

   Те, як сектори інфраструктури взаємодіють, у тому числі через використання спільних інформаційних і комунікаційних технологій (наприклад, хмарних сервісів), визначає те, як національні партнери критичної інфраструктури повинні спільно керувати ризиками. Наприклад, усі сектори критичної інфраструктури покладаються на функції, які забезпечують, зокрема, енергетичні, комунікаційні, транспортні та водні системи. Крім того, взаємозалежності протікають в обох напрямах, як і залежність енергетичних і комунікаційних систем одна від одної та від інших функцій. Для спільноти критичної інфраструктури важливо розуміти та належним чином враховувати залежності та взаємозалежності під час управління ризиками.

3. Отримання знань про ризики інфраструктури та взаємозалежності вимагає обміну інформацією у межах спільноти критичної інфраструктури.

   Завдяки своїй діяльності та перспективам зацікавлені сторони в спільноті критичної інфраструктури володіють і виробляють різноманітну інформацію, корисну для підвищення безпеки та стійкості критичної інфраструктури. Обмін і спільне планування на основі цієї інформації є обов'язковим для комплексного вирішення питань безпеки та стійкості критичної інфраструктури в середовищі зростаючої взаємопов'язаності. Щоб це відбулося, мають бути встановлені належний правовий захист, довірчі відносини, сприятливі технології та послідовні процеси.

4. Партнерський підхід до безпеки та стійкості критичної інфраструктури визнає унікальні перспективи та порівняльні переваги різноманітної спільноти критичної інфраструктури.

   Державно-приватне партнерство є ключовим для підтримки безпеки та стійкості критичної інфраструктури. Добре функціонуюче партнерство залежить від ряду атрибутів, включаючи довіру; визначену мету діяльності; чітко сформульовані цілі; вимірний прогрес і результати для спрямування спільної діяльності; залучення керівництва; чітке і часте спілкування; гнучкість і адаптивність. Усі рівні уряду, а також приватний і некомерційний сектори привносять унікальний досвід, можливості та ключові компетенції в національні зусилля. Визнання цінності різних точок зору допомагає партнерству більш чітко розуміти проблеми та рішення, пов'язані з безпекою та стійкістю критичної інфраструктури.

5. Регіональні партнерства та партнерства **SLTT** мають вирішальне значення для розробки спільних точок зору на прогалини та дії для покращення безпеки та стійкості критичної інфраструктури.

   Національний план наголошує на партнерстві між установами та в межах географічних кордонів для досягнення безпеки та стійкості. Ризики часто мають локальні наслідки, що робить важливим виконання ініціатив у регіональному масштабі таким чином, щоб доповнювати та реалізовувати національні зусилля. Це вимагає, щоб місцеві державні, приватні та некомерційні організації надавали свої погляди на оцінку ризиків і стратегії

пом'якшення. Місцеві партнерства по всій країні збільшують зусилля існуючих партнерств на національному рівні та мають важливе значення для справжніх національних зусиль щодо зміцнення безпеки та стійкості.

6. Інфраструктура, яка має важливе значення для Сполучених Штатів, виходить за рамки національних кордонів, вимагаючи транскордонного співробітництва, взаємодопомоги та інших угод про співпрацю.

Сполучені Штати отримують переваги та залежать від глобальної мережі інфраструктури, яка забезпечує безпеку та спосіб життя країни. Розподілений характер і взаємозв'язок цих активів, систем і мереж створюють складне середовище, в якому ризики, з якими стикається країна, не виділяються чітко в межах її кордонів. Це стається дедалі частіше, оскільки послуги, що надаються критичною інфраструктурою, часто залежать від інформації, яка збирається, зберігається або обробляється в розподілених місцях. Вкрай важливо, щоб уряд, приватний сектор і міжнародні партнери працювали разом. Це включає співпрацю для повного розуміння вразливостей ланцюга постачання та впровадження скоординованих, а не конкуруючих, глобальних заходів безпеки та стійкості. Національний план є зосередженим на внутрішніх зусиллях щодо безпеки та стійкості критичної інфраструктури, при цьому визнаючи міжнародні аспекти національного підходу.

7. Під час проєктування активів, систем і мереж слід враховувати безпеку та стійкість.

Оскільки критична інфраструктура будується та оновлюється, ті, хто бере участь у прийнятті проєктних рішень, у тому числі тих, що стосуються систем керування, повинні розглядати найбільш ефективні та результативні способи виявлення, стримування, зриву та підготовки до загроз і небезпек; усунення вразливостей; і мінімізації наслідків. Сюди ж входить розгляд принципів стійкості інфраструктури.

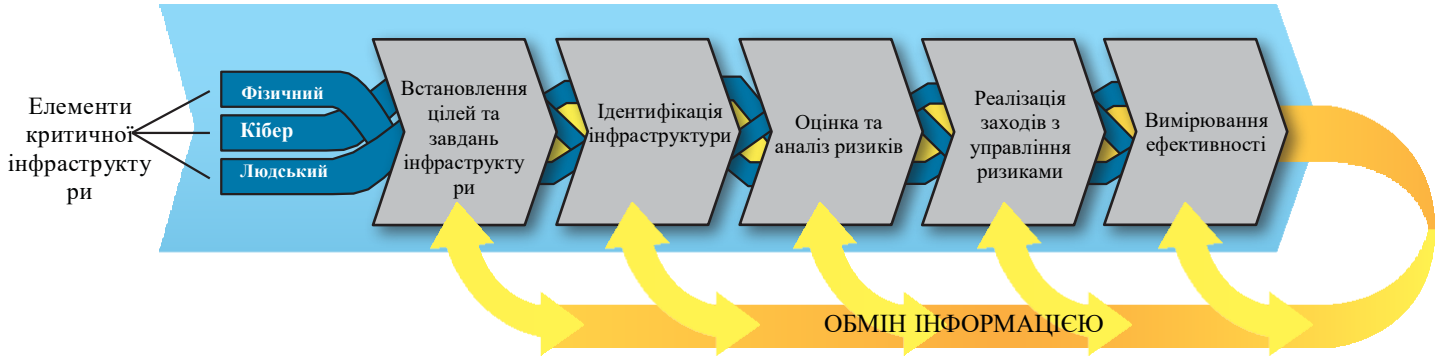
5. Співпраця для управління ризиками

Національні зусилля щодо зміцнення безпеки та стійкості критичної інфраструктури залежать від здатності державних і приватних власників і операторів критичної інфраструктури приймати рішення з урахуванням ризиків щодо найбільш ефективних доступних способів вирішення при розподілі обмежених ресурсів як у стабільному, так і в кризовому режимах. Таким чином, управління ризиками є наріжним каменем Національного плану та є актуальним на національному, регіональному місцевому рівнях та рівні штатів. Національна, регіональна та місцева стійкість залежить від створення та підтримки сталого надійного партнерства між державним і приватним секторами. У той час як окремі організації несуть відповідальність за управління ризиками для своєї організації, партнерства покращують розуміння загроз, вразливостей і наслідків, а також способів управління ними за допомогою обміну індикаторами та практиками та координації політики, заходів реагування та відновлення.

Партнери з критичної інфраструктури керують ризиками на основі різноманітних зобов'язань перед суспільством, зосередженості на добробуті клієнтів і структур корпоративного управління. Допуски до ризику відрізнятимуться від організації до організації, а також від сектора до сектору, залежно від бізнес-планів, ресурсів, операційної структури та нормативного середовища. Вони також відрізняються між приватним сектором і урядом через основні обмеження. Різні організації, ймовірно, матимуть різні пріоритети щодо інвестицій у безпеку, а також потенційно різні судження щодо того, якою може бути відповідна точка толерантності до ризику. Організації приватного сектору, як правило, можуть збільшити інвестиції, щоб відповідати своїм допустимим ризикам і забезпечувати свою спільноту зацікавлених сторін, але інвестиції в безпеку та стійкість мають законні межі. Уряд повинен забезпечувати національну та громадську безпеку, і при цьому діяти з різними обмеженнями. Пошук відповідної ціннісної пропозиції серед партнерів вимагає розуміння цих різних точок зору та того, як вони можуть вплинути на зусилля щодо встановлення спільних пріоритетів. У межах цих параметрів безпека та стійкість критичної інфраструктури залежать від застосування практик управління ризиками як у промисловості, так і в уряді, у поєднанні з наявними ресурсами та стимулами для спрямування та підтримки зусиль.

Цей розділ створено на основі структури управління ризиками критичної інфраструктури, представленої в NIPP 2006 року та оновленої в цьому Національному плані. Оновлення допомагають уточнити компоненти та оптимізувати етапи інфраструктури, зображені на малюнку 3 нижче. А саме три елементи критичної інфраструктури (фізичний, кібернетичний та людський) є чітко визначеними та повинні бути інтегровані на всіх етапах структури управління ризиками критичній інфраструктурі, якщо це доцільно. Крім того, оновлена структура консолідує кількість кроків або «шевронів», включаючи визначення пріоритетів із запровадженням діяльності з управління ризиками. Пріоритезація варіантів зменшення ризиків є невід'ємною частиною процесу прийняття рішень щодо вибору заходів з управління ризиками, які мають бути впроваджені. Нарешті, посилання на цикл зворотного зв'язку видалено, а замість цього структура тепер описує важливість обміну інформацією протягом усього процесу управління ризиками. Інформація передається на кожному етапі структури, включаючи етап «вимірювання ефективності», що сприяє зворотному зв'язку та забезпечує безперервне вдосконалення безпеки критичної інфраструктури та заходів щодо стійкості.

Малюнок 3 – Структура управління ризиками критичній інфраструктурі



Структура управління ризиками критичної інфраструктури підтримує процес прийняття рішень, який партнери критичної інфраструктури спільно здійснюють для інформування щодо вибору дій з управління ризиками. Ця структура не є обов'язковою, і багато організацій мають моделі управління ризиками, які довели свою ефективність і повинні підтримуватися. Однак це забезпечує організаційну конструкцію для цих моделей. У цьому розділі представлено вибір заходів з управління ризиками, які реалізуються спільнотою критичної інфраструктури, але там, де це можливо, описано конкретні внески різних партнерів. Крім того, виноски в цьому розділі визначають зв'язки між кроками в структурі управління ризиками та конкретними діями, визначеними в Заклику до дії в розділі 6 цього Національного плану.

Структура управління ризиками критичній інфраструктурі розроблена для забезпечення гнучкості під час її використання в усіх секторах, у різних географічних регіонах і різними партнерами. Її можна адаптувати до різних операційних середовищ і застосовувати до всіх загроз і небезпек. Структура управління ризиками призначена для доповнення та підтримки завершення процесу ідентифікації загроз і небезпек та оцінки ризиків (THIRA), який проводиться регіональними, SLTT і міськими юрисдикціями для встановлення пріоритетів можливостей. Посібник із комплексної готовності 201: Виявлення загроз і небезпек, а також оцінка ризиків, друге видання згадує власників і операторів інфраструктури як джерела інформації про загрози та небезпеки та як цінних партнерів під час завершення процесу THIRA. *Посібник із комплексної готовності 201: Виявлення загроз і небезпек, а також оцінка ризиків, друге видання* зазначає власників і операторів інфраструктури як джерела інформації про загрози та небезпеки та як цінних партнерів під час завершення процесу THIRA.

Спільнота критичної інфраструктури ділиться інформацією на всіх етапах структури управління ризиками, щоб задокументувати та використати найкращі практики та отримані уроки, а також допомогти виявити та заповнити прогалини в зусиллях щодо безпеки та стійкості. Спільноті важливо ділитися інформацією про ризики, також відомою як комунікація щодо ризиків, яка визначається як обмін інформацією з метою покращення розуміння ризику, впливу на сприйняття ризику та/або підготовки людей чи груп до відповідних дій у відповідь на ідентифікований ризик.

Управління ризиками дозволяє спільноті критичної інфраструктури зосередитися на тих загрозах і небезпеках, які можуть завдати шкоди, і застосовувати підходи, розроблені для запобігання або пом'якшення наслідків таких інцидентів. Це також підвищує безпеку та зміцнює стійкість шляхом визначення пріоритетів дій для забезпечення безперервності основних функцій та послуг, а також підтримки покращеного реагування та відновлення.

Set Infrastructure Goals and Objectives

Національний план визначає низку головних національних цілей щодо безпеки та стійкості критичної інфраструктури. Такі національні цілі підкріплюються завданнями та пріоритетами, розробленими на секторальному рівні, які можуть бути сформульовані в рамках секторальних планів і слугувати об'єктом спільного планування між секторальними агентствами та їхніми секторальними партнерами в уряді та приватному секторі.

Як зазначалося в розділі 2, набір національних багаторічних пріоритетів, розроблений за участю всіх рівнів партнерства, доповнить ці цілі. Такі пріоритети можуть бути зосереджені на конкретних цілях або міжгалузевих питаннях, де увага та ресурси можуть бути використані в рамках спільноти критичної інфраструктури з найбільш значним впливом.

Пов'язані Заклики до дії:

- Встановіть національну спрямованість шляхом спільного визначення пріоритетів.
- Визначте колективні дії шляхом спільного планування.

Власники та оператори критичної інфраструктури, а також SLTT і регіональні організації можуть визначати завдання та пріоритети для критичної інфраструктури, які відповідають національним пріоритетам, розробленим за участю всіх рівнів партнерства, національним цілям і секторальним завданням, але при цьому є пристосованими та масштабованими відповідно до їхнього операційного середовища та середовища ризику, а також наявних ресурсів.

Ідентифікація інфраструктури

Для ефективного управління ризиками критичній інфраструктурі партнери повинні ідентифікувати активи, системи та мережі, які є важливими для їх подальшої роботи, враховуючи відповідні залежності та взаємозалежності. Такий аспект процесу управління ризиками також має ідентифікувати інформаційні та комунікаційні технології, які сприяють наданню основних послуг.

Партнери з критичної інфраструктури дивляться на критичність по-різному, виходячи зі своїх унікальних ситуацій, операційних моделей і пов'язаних з ними ризиків. Федеральний уряд ідентифікує та пріоритезує критичну інфраструктуру національного значення на основі законодавчого визначення та національних міркувань. Уряди SLTT ідентифікують і пріоритезують критичну інфраструктуру відповідно до свого ділового та операційного середовища та пов'язаних із цим ризиків. Власники та оператори інфраструктури ідентифікують активи, системи та мережі, які є важливими для безперервної роботи та надання продуктів і послуг клієнтам. На секторальному рівні багато секторальних агентств співпрацюють з власниками та операторами, а також організаціями SLTT для розробки переліку інфраструктури, яка є важливою на національному, регіональному та місцевому рівнях.

Пов'язаний Заклик до дії:

- Аналізуйте залежності та взаємозалежності.

Ефективне управління ризиками вимагає розуміння критичності, а також пов'язаних взаємозалежностей інфраструктури. Цей Національний план визначає певні життєво важливі функції, які є важливими для роботи найбільш критичних секторів інфраструктури. До цих життєво важливих функцій належать комунікації, енергетика, транспорт і вода. Партнери з критичної інфраструктури повинні визначити основні функції та ресурси, які впливають на їхній бізнес і спільноти. Визначення цих життєво важливих функцій може підтримувати планування готовності та розвиток можливостей.

Оцінка та аналіз ризиків

Ризики критичній інфраструктурі можна оцінити з точки зору:

- **Загрози** – природне або спричинене людиною явище, особа, організація або дія, яка має або вказує на потенційну шкоду життю, інформації, діяльності, навколишньому середовищу та/або власності.
- **Вразливості** – фізична особливість або робочий атрибут, який робить об'єкт відкритим для експлуатації або чутливим до певної небезпеки.
- **Наслідку** – вплив інциденту чи події.

Оцінки ризиків проводяться багатьма партнерами з критичної інфраструктури, щоб отримати інформацію для прийняття власних рішень, використовуючи широкий спектр методологій. Такі оцінки дозволяють керівникам спільнот критичної інфраструктури зрозуміти найбільш вірогідні та серйозні інциденти, які можуть вплинути на їхні операції та громади, і використовувати цю інформацію для підтримки планування та скоординованого розподілу ресурсів.

Пов'язаний Заклик до дії:

- Покращуйте обмін інформацією та застосовуйте знання для прийняття рішень з урахуванням ризиків.

Для ефективної оцінки ризиків партнерам з критичної інфраструктури, включаючи власників і операторів, секторальні ради та державні установи, потрібна своєчасна, надійна та дієва інформація щодо загроз, вразливостей і наслідків. Неурядові організації повинні брати участь у розробці та розповсюдженні продуктів щодо загроз, вразливостей і потенційних наслідків і надавати інформацію про ризики в надійному середовищі. Партнери повинні проводити спільний аналіз інформації, якщо це необхідно. Партнерство у сфері критичної інфраструктури може дуже посприяти покращенню розуміння ризиків як для кібер-, так і для фізичних систем і активів. Ні державний, ні приватний сектори не можуть повністю зрозуміти ризик без цієї інтеграції широких знань і аналізу.

Ініціативи підтримки обміну інформацією існують як на національному, так і на регіональному рівнях. Діяльність з обміну інформацією може захистити конфіденційність, застосовуючи FIPP, і захистити громадянські свободи, дотримуючись відповідних законів і політик. Не менш важливо забезпечити належний захист конфіденційної бізнес-інформації та інформації про безпеку, яка може спричинити серйозний негативний вплив на приватний бізнес, економіку та безпеку державних або приватних підприємств через несанкціоноване розкриття, доступ або використання. Федеральний уряд несе законну відповідальність за захист інформації критичної інфраструктури. DHS та інші агенції використовують програму захисту інформації критичної інфраструктури (PCII) та інші протоколи, такі як Таємна інформація щодо національної безпеки, Конфіденційна інформація правоохоронних органів і Федеральні рекомендації щодо класифікації безпеки. Програма PCII, затверджена Актом про інформацію щодо критичної інфраструктури (CII) 2002 року та його виконавчими положеннями (розділ 6 Кодексу федеральних нормативних актів, частина 29), визначає вимоги подання Акту, а також вимоги до державних установ, які вони мають дотримуватися для доступу та охорони Акту.

Реалізація заходів з управління ризиками

Особи, які приймають рішення, встановлюють пріоритетність діяльності з управління ризиком критичної інфраструктури на основі критичності ураженої інфраструктури, вартості такої діяльності та потенціалу зниження ризику. Деякі види діяльності з управління ризиками стосуються кількох аспектів ризику, тоді як інші спрямовані на вирішення конкретних загроз, вразливостей або потенційних наслідків. Ці види діяльності можна розділити на такі підходи:

Ідентифікація, стримання, виявлення, попередження та підготовка до загроз і небезпек

- Створити та впровадити спільні плани та процеси для оцінки необхідних посилень безпеки та заходів стійкості на основі попереджень про небезпеку та звітів про загрози.
- Здійснювати постійний моніторинг кіберсистем.
- Використовувати системи безпеки, щоб виявити або затримати атаку або вторгнення.
- Виявляти зловмисну діяльність, яка загрожує критичній інфраструктурі та відповідній операційній діяльності в секторах.
- Впровадити систему виявлення або захисту від вторгнень у конфіденційних або критично важливих мережах і об'єктах для виявлення та запобігання несанкціонованому доступу та використанню.
- Відстежувати об'єкти та системи критичної інфраструктури, які є потенційною мішенню для атак (наприклад, через місцеві правоохоронні та комунальні служби).

Зменшення вразливостей

- Додати безпеку та стійкість до проєктування та експлуатації активів, систем і мереж.
- При розміщенні нової інфраструктури враховувати особливості розміщення, наприклад, уникати сейсмічні зони та інші місця, схильні до ризику.
- Розробити та провести навчальні програми та тренування для підвищення обізнаності та розуміння загальних вразливостей і можливих стратегій пом'якшення.
- Використовувати отримані уроки та застосовувати коригувальні дії в результаті інцидентів і навчань для посилення захисних заходів.
- Розробляти та виконувати плани дій у надзвичайних ситуаціях та плани забезпечення безперервності для бізнесу та уряду на місцевому та регіональному рівнях, щоб сприяти безперервному виконанню критично важливих функцій під час надзвичайної ситуації.
- Усувати кібервразливості шляхом постійної діагностики та визначення пріоритетів вразливостей із високим ризиком.
- Проводити дослідження та розробки, щоб зменшити відомі кібер- та фізичні вразливості, усунення яких виявилося складним або дорогим.

Пом'якшення наслідків

- Обмінюватися інформацією для підтримки ситуаційної обізнаності та оцінки кібер- і фізичної шкоди критичній інфраструктурі під час і після інциденту, включаючи характер і масштаб загрози, каскадні ефекти та статус реагування.
- Працювати для відновлення роботи критичної інфраструктури після інциденту.
- Підтримувати надання основних послуг, таких як: аварійне живлення критичних об'єктів; запаси палива для рятувальників; а також питна вода, мобільний зв'язок, продукти харчування та фармацевтичні препарати для постраждалої громади.

- Перевіряти, що на віддалених серверах створено резервні копії важливої інформації та що для ключових функцій реалізовано резервні процеси, що зменшить потенційні наслідки інциденту кібербезпеки.
- Видалити ключові операційні функції з підключеної до Інтернету бізнес-мережі, зменшивши ймовірність того, що інцидент кібербезпеки призведе до компрометації основних служб.

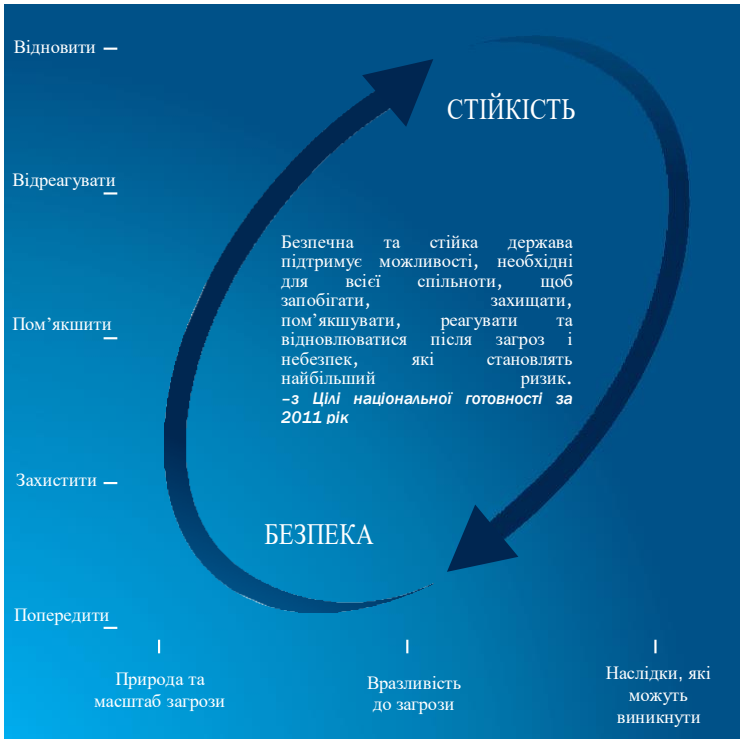
Пов'язані Заклики до дії:

- Швидко визначайте, оцінюйте та реагуйте на каскадні ефекти під час і після інцидентів.
- Сприяйте відновленню інфраструктури, спільноти та регіону після інцидентів.

- Переконатися, що інциденти, що впливають на кіберсистеми, повністю обмежені; функціональність активу, системи або мережі відновлено до стану до інциденту; і що уражена інформація доступна в безкомпромісному та безпечному стані.
- Визнавати та враховувати взаємозалежності у реагуванні та планах відновлення.
- Відремонтувати або замінити пошкоджену інфраструктуру економічно ефективними конструкціями, які є більш безпечними та стійкими.
- Використовувати та забезпечувати надійність можливостей екстреного зв'язку.
- Сприяти розвитку та виконанню приватного сектору, SLTT та регіональних пріоритетів як для найближчого, так і для довгострокового відновлення.

Вищезазначені дії є прикладами заходів з управління ризиками, які здійснюються для підтримки загального досягнення безпеки та стійкості на організаційному, громадському, секторальному чи національному рівні. Діяльність із запобігання найбільш тісно пов'язана із зусиллями щодо усунення загроз; заходи захисту, як правило, спрямовані на вразливості; а заходи з реагування та відновлення допомагають мінімізувати наслідки. Зусилля щодо пом'якшення виходять за межі всього спектру загроз, уразливостей і наслідків. Ці п'ять сфер, як описано в Цілі та системі національної готовності, забезпечують корисну основу для розгляду інвестицій в управління ризиками. Малюнок 4 ілюструє взаємозв'язок сфер національної готовності та елементів ризику.

Малюнок 4 – Ризик критичної інфраструктури в контексті національної готовності



Ціль національної готовності також встановлює 31 основну можливість, які підтримують п'ять сфер національної готовності. Розвиток багатьох із цих основних можливостей сприяє досягненню безпеки та стійкості критичної інфраструктури, а громади, власники та оператори можуть застосовувати ці можливості для визначених заходів для управління ризиками. Такі зусилля посилюються, коли ризики критичної інфраструктури розглядаються як частина встановлення цільових можливостей.

Щоб підтримати зусилля перед або під час інциденту, спільнота критичної інфраструктури співпрацює на основі структур, закріплених у Національній структурі запобігання, Національній структурі захисту, Національній структурі пом'якшення наслідків, Національній структурі реагування (NRF), Національній структурі відновлення після стихійних лих, а також у тимчасовому Національному плані реагування на кіберінциденти або його наступнику. Одним із

прикладів того, як ці структури підтримують спільні зусилля, є NRF. Організаційні структури NRF координують заходи, пов'язані з критичною інфраструктурою, які проводяться у відповідь на національно оголошене лихо або серйозний інцидент, що потребує федеральної допомоги. Додаток підтримки критичної інфраструктури NRF пояснює, як заходи безпеки та стійкості критичної інфраструктури інтегровані в NRF, і описує політику, ролі та обов'язки, дії, пов'язані з інцидентами, і координаційні структури, які використовуються для оцінки, визначення пріоритетів, безпеки та відновлення критичної інфраструктури під час фактичних чи потенційних побутових випадків. Додаток використовує структури партнерства та процеси обміну інформацією та управління ризиками, описані в цьому Національному плані. Подібні зв'язки існують і будуть продовжувати вдосконалюватися через інші структури та плани реагування на інциденти.

На додаток до ідентифікованих заходів щодо зменшення загроз, уразливостей і наслідків, зниження ризику можна досягти за допомогою розробки критичної інфраструктури та системи контролю. Завчасне врахування заходів безпеки та стійкості в проєктних рішеннях може полегшити інтеграцію заходів для пом'якшення фізичної та кібервразливості, а також природних і технологічних небезпек за менших витрат. Уряди та компанії можуть краще інвестувати в заходи, які підвищують безпеку та стійкість як критичної інфраструктури, так і суспільства в цілому за допомогою аналізу ризиків, методів проєктування, заснованих на фактичних даних, і врахування витрат і вигод. Це також корисно під час зусиль з відновлення інфраструктури, у тих випадках, коли федеральний уряд працює з громадами та промисловістю для відновлення інфраструктури.

Вимірювання ефективності

Спільнота критичної інфраструктури оцінює ефективність зусиль з управління ризиками в секторах та на національному, місцевому та регіональному рівнях та рівні штатів шляхом розробки метрики для прямого та непрямого вимірювання показників. Секторальні агентства співпрацюють із Секторальною координуючою радою через процес планування для окремих секторів, щоб розробити атрибути, які підтримують національні цілі та пріоритети, а також інші пріоритети для окремих секторів. Такі заходи інформують про зусилля партнерів з управління ризиками в межах спільноти критичної інфраструктури та допомагають побудувати національну картину прогресу на шляху до бачення цього Національного плану, а також Цілі національної готовності.

На національному рівні в Національному плані сформульовані широкі територіальні цілі для досягнення бачення Плану, які будуть доповнені набором багаторічних національних пріоритетів. Спільнота критичної інфраструктури згодом оцінить свій колективний прогрес у досягненні цілей і пріоритетів.

Цей процес оцінювання функціонує як інтегрований безперервний цикл:

- сформулювати бачення та національні цілі;
- визначити національні пріоритети;
- визначити результати високого рівня або такі, що пов'язані з національними цілями та національними пріоритетами;
- зібрати дані про ефективність для оцінки прогресу в досягненні визначених результатів;
- оцінити прогрес у досягненні національних пріоритетів, національних цілей і бачення;
- оновити національні пріоритети та відповідно адаптувати діяльність з управління ризиками; та
- періодично переглядати національні цілі та бачення.

Related Calls to Action

- **Evaluate Achievement of Goals**
- **Learn and Adapt During and After Exercises and Incidents**

Подібно до того, як регулярна оцінка прогресу в досягненні національних цілей інформує про постійну еволюцію практик безпеки та стійкості, заплановані навчання та реальні інциденти також надають можливості для навчання та адаптації. Наприклад, нестача палива після урагану «Сенді» продемонструвала взаємозалежність і складність інфраструктурних систем, труднощі в досягненні спільної обізнаності про ситуацію під час великих подій, а також потребу в покращенні збору інформації та обміну інформацією між партнерами з уряду та приватного сектору для підтримки відновлювальних заходів. Співтовариства критичної інфраструктури та національної готовності також проводять навчання на постійній основі в рамках Національної програми навчань та інших механізмів для оцінки та підтвердження спроможності організацій, установ та юрисдикцій. Під час і після таких запланованих і незапланованих операцій партнери виявляють індивідуальні та групові слабкі місця, впроваджують і оцінюють коригувальні дії, а також діляться найкращими практиками з більш широкими спільнотами критичної інфраструктури та управління надзвичайними ситуаціями. Таке навчання та адаптація визначають майбутні плани, діяльність, технічну допомогу, навчання та освіту.

6. Заклик до дії: Етапи просування національних зусиль

Заклик до дії скеровує зусилля для досягнення національних цілей, спрямованих на підвищення безпеки та стійкості національної критичної інфраструктури. Такі заходи виконуються спільнотою критичної інфраструктури у співпраці.

Федеральні департаменти та агентства, співпрацюючи з SLTT, регіональними партнерами та партнерами з приватного сектору, беручи до уваги унікальні перспективи управління ризиками, пріоритети та обмеження ресурсів кожного сектора, працюватимуть разом, щоб сприяти безперервному вдосконаленню заходів безпеки та стійкості для виконання завдань нижче. Дії, перелічені в цьому розділі, не є вичерпними, і не передбачається, що кожен сектор виконуватиме всі дії. Замість цього цей розділ призначений як дорожня карта для спрямування національного прогресу, враховуючи при цьому різні пріоритети в різних секторах. Таким чином, перелічені нижче дії забезпечують стратегічний напрям для національних зусиль у найближчі роки. Виноски в цьому розділі вказують на зв'язки між діяльністю «Заклик до дії» та національними цілями, представленими в розділі 2.

Розвиток партнерських зусиль:

1. Встановіть національну спрямованість шляхом спільного визначення пріоритетів.
2. Визначте колективні дії шляхом спільного планування.
3. Розширюйте можливості місцевого та регіонального партнерства для розбудови спроможності на національному рівні.
4. Використовуйте стимули для підвищення безпеки та стійкості.

Інновації в управлінні ризиками:

5. Забезпечте ухвалення рішень з урахуванням ризиків завдяки розширеній ситуаційній обізнаності.
6. Аналізуйте залежності, взаємозалежності та пов'язані каскадні ефекти інфраструктури.
7. Виявляйте, оцінюйте та реагуйте на непередбачені каскадні ефекти інфраструктури під час та після інцидентів.
8. Сприяйте відновленню інфраструктури, спільноти та регіону після інцидентів.
9. Посилюйте скоординований розвиток та забезпечуйте надання технічної допомоги, проведення навчань.
10. Посилюйте безпеку та стійкість критичної інфраструктури за допомогою вдосконалення рішень щодо досліджень і розробок.

Зосередження на результатах:

11. Оцініть прогрес у досягненні цілей.
12. Навчайтеся та адаптуйтеся під час і після вправ та інцидентів.

Ці дії інформуватимуть і спрямовуватимуть зусилля, визначені за допомогою процесів встановлення пріоритетів і спільного планування, описаних нижче, залежно від ресурсів.

Розвиток партнерських зусиль

Заклик до дії #1: Встановіть національну спрямованість шляхом спільного визначення пріоритетів

Пов'язаний з усіма національними цілями

Щоб керувати національними зусиллями та приймати рішення, структури національної ради спільно встановлюватимуть багаторічні пріоритети та переглядатимуть їх щорічно за участю всіх рівнів спільноти критичної інфраструктури.

Ці пріоритети враховуватимуть ризики, з якими стикається країна, на основі SNRA, оцінки ризиків партнерами з критичної інфраструктури, а також державних і регіональних THIRA. Щорічне звітування про критичну інфраструктуру та готовність також інформуватиме про національні пріоритети через оцінку прогалин у можливостях.

- Спільно встановіть набір пріоритетів безпеки та стійкості національної критичної інфраструктури для підтримки федерального розподілу ресурсів, а також планування та оцінки на всіх рівнях національного партнерства.
- Переглядайте та перевіряйте національні пріоритети щорічно та оновлюйте їх у регулярному циклі, призначеному для інформування щодо розробки федерального бюджету та програм грантів SLTT.

Заклик до дії #2: Визначте колективні дії шляхом спільного планування

Пов'язаний з усіма національними цілями

Діяльність з планування в межах спільноти критичної інфраструктури має відображати цей Національний план і спільні пріоритети, визначені в Заклику до дії №1.
Зокрема, діяльність має бути зосереджена на розбудові потенціалу SCC, SLTT та регіонального потенціалу та посиленні координації зі спільнотою управління надзвичайними ситуаціями.

- Усі сектори оновлюватимуть свої Секторальні плани (SSP) для підтримки цього Національного плану, а потім кожні чотири роки на основі вказівок, розроблених DHS у співпраці з SSA та міжсекторальними радами. Секторальні плани будуть:
  - відображати спільні пріоритети.
  - звертати увагу на залежність сектора від життєво важливих функцій і включати стратегії пом'якшення наслідків втрати цих функцій, в тому числі потенційні каскадні ефекти.
  - описувати підходи до інтеграції критичної інфраструктури та національних заходів щодо готовності, зокрема, перехід від стабільного стану до реагування на інциденти та відновлення за допомогою функцій підтримки надзвичайних ситуацій (ESF) Національної рамкової системи реагування та функцій підтримки відновлення (RSF) Національної рамкової системи відновлення після аварій.
  - описувати поточні та заплановані зусилля з кібербезпеки, включаючи, але не обмежуючись цим, використання Структури кібербезпеки, ініціативи з обміну інформацією з кібербезпеки, програмні заходи, оцінки ризиків, навчання, заходи з реагування на інциденти та відновлення, а також будь-які показники.
  - керувати розробкою відповідних показників і цілей для вимірювання прогресу в досягненні національних цілей і пріоритетів, а також інших галузевих пріоритетів.
- Якщо доцільно, SLTT та регіональні організації можуть розробити допоміжні плани до цього Національного плану та оновлених SSP, як міжгалузевих, так і окремих секторів, які формулюють спільні пріоритети та заходи на таких рівнях. SLTTGCC співпрацюватиме з партнерами для надання вказівок щодо таких планів.
- Федеральний уряд співпрацюватиме зі спільнотою критичної інфраструктури, щоб надати оновлені рекомендації щодо реагування на кіберінциденти.

Заклик до дії #3: Розширюйте можливості місцевого та регіонального партнерства для розбудови спроможності на національному рівні

Пов'язана національна ціль:

- Посилення стійкості критичної інфраструктури шляхом мінімізації негативних наслідків...

Оскільки більшість інцидентів мають локальний характер, місцева та регіональна співпраця має важливе значення для інтеграції безпеки критичної інфраструктури, стійкості та заходів щодо готовності на національному рівні. Місцеві та регіональні партнерства роблять значний внесок у національні зусилля, збільшуючи охоплення національного партнерства, демонструючи його цінність і просуваючи національні цілі.

- Визначте існуючі місцеві та регіональні партнерства, що стосуються безпеки та стійкості критичної інфраструктури, їхню спрямованість та узгодженість із національними партнерськими структурами та способи взаємодії з ними. Використовуйте ті, що в штатах, та великі міські центри злиття для взаємодії з місцевими та регіональними партнерами.
- Розширте національну мережу критичної інфраструктури та партнерства та коаліції SLTT, щоб доповнити та посилити фокус на національному рівні на секторах, зберігаючи при цьому знання про різні правові структури в різних юрисдикціях та організаціях.
- Використовуйте процес THIRA як метод інтеграції людських, фізичних і кібернетичних елементів управління ризиками критичної інфраструктури. Використання існуючого процесу сприятиме кращій координації планування, розподілу ресурсів та оцінки прогресу державними та місцевими органами влади, а також власниками та операторами місцевої інфраструктури.
- Розробіть та вдосконалюйте спільний набір регіональних проєктів готовності, що демонструють комплексне застосування управління ризиками та планування критичної інфраструктури. Це залучатиме федеральні агентства, відповідальні за впровадження PPD-8 і PPD-21, які співпрацюватимуть із штатами, мегаполісами, сільськими громадами та регіональними коаліціями.

Заклик до дії #4: Використовуйте стимули для підвищення безпеки та стійкості

Пов'язані національні цілі:

- Захист критичної інфраструктури від загроз...
- Посилення стійкості критичної інфраструктури шляхом мінімізації негативних наслідків...

Уряд і приватний сектор спільно зацікавлені в забезпеченні життєздатності критичної інфраструктури та наданні основних послуг за будь-яких умов. Власники та оператори критичної інфраструктури часто отримують найбільшу вигоду від інвестицій у власну безпеку та стійкість, і під впливом соціальної відповідальності застосовують такі практики. Однак приватний сектор може бути виправдано стурбований поверненням інвестицій у безпеку та стійкість, які можуть не принести миттєвої вимірної вигоди. Ефективні стимули можуть допомогти виправдати витрати на покращену безпеку та стійкість, збалансувавши короткострокові витрати на додаткові інвестиції з такими ж короткостроковими вигодами.

Ринкові стимули можуть сприяти суттєвим змінам у бізнес-практиці та заохочувати розвиток ринків, таких як страхування кібернетичних, хімічних, біологічних або радіологічних ризиків. Крім того, штати та місцеві органи влади можуть вивчити можливість запропонувати власні стимули для заохочення інвестицій у заходи безпеки та стійкості.

- Продовжуйте визначати, аналізувати та, де необхідно, впроваджувати стимули.
- Підтримуйте дослідження та збір даних для кількісної оцінки потенційних витрат, спричинених відсутністю безпеки та стійкості критичної інфраструктури та недостатньою готовністю до кібернетичного середовища.
- Створіть програми інноваційних викликів, щоб стимулювати нові рішення для посилення безпеки та стійкості інфраструктури на етапах планування, проєктування та редизайну інфраструктури, включаючи технологічні, інженерні та операційні вдосконалення.

Заклик до дії #5 Забезпечте ухвалення рішень з урахуванням ризиків завдяки розширеній ситуаційній обізнаності

Пов'язана національна ціль:
- Обмін корисною та актуальною інформацією...

Щоб гарантувати, що можливості ситуаційної обізнаності не відстають від динамічного середовища ризику, що розвивається, спільнота критичної інфраструктури має продовжувати вдосконалювати методи обміну інформацією та застосування знань, отриманих завдяки змінам у політиці, процесах і культурі.

Спільнота може сприяти розвитку культури «необхідності ділитися» та «відповідальності за надання» на всіх рівнях і в усіх секторах, визнаючи, що власники та оператори критичної інфраструктури та уряди SLTT є ключовими споживачами та постачальниками інформації про ризики. Ця культура побудована на спільному розумінні національних зусиль щодо підвищення безпеки та стійкості критичної інфраструктури.

Відповідно, федеральний уряд буде консультуватися з урядами SLTT, власниками та операторами, щоб переконатися, що аналіз розвідувальних даних відповідає їхнім потребам, і використовувати послідовні засоби для розповсюдження розвідувальних даних та продуктів інформаційної безпеки. Уряд також продовжуватиме покращувати здатність NICC, NCCIC та інших федеральних ресурсів для обміну інформацією створювати та ділитися міжгалузевою ситуаційною обізнаністю майже в реальному часі, захищаючи конфіденційну інформацію. Крім того, федеральний уряд використовуватиме політику та процедури «розривної лінії» та «обмежуваної лінії», щоб полегшити обмін дієвими частинами таємних звітів або нетаємних звітів з обмеженим доступом із приватним сектором та партнерами SLTT. Так само державні та місцеві органи влади можуть покращити обмін інформацією між службовцями SLTT, відповідальними за безпеку та стійкість критичної інфраструктури. Державні та місцеві органи влади та регіональні партнерства можуть сприяти більш широкому використанню державних і великих міських центрів синтезу в межах своїх відповідних юрисдикцій і регіонів для визначення загроз, оцінки ризиків і пріоритетного розвитку. Власники та оператори можуть підтримувати покращення, надаючи аналітикам урядової розвідки постійний зворотний зв'язок щодо інформаційних потреб, розповсюдження та застосування їхніх інформаційних продуктів, а також обмінюючись інформацією з федеральними урядами та урядами SLTT.

- Проведіть загальнопартнерський огляд перешкод для обміну інформацією, щоб підтримати зусилля з вирішення цих проблем і розробити найкращі практики. Проаналізуйте правові аспекти, класифікацію або конфіденційний характер певної інформації, закони та політику, які регулюють поширення інформації, а також необхідність зміцнення довіри між партнерами.
- Спирайтесь на описи функціональних зв'язків, розроблені в рамках PPD-21, шляхом подальшого аналізу функціональних зв'язків у федеральному уряді та між урядами (зосередженому на безпеці та стійкості критичної інфраструктури), щоб виявити збіги, неефективність і прогалини та рекомендувати зміни для покращення обізнаності про ситуацію та прийняття рішень з урахуванням ризику.
- Розробіть впорядковані, стандартизовані процеси для сприяння інтеграції та координації обміну інформацією за допомогою спільно розробленої доктрини та допоміжних стандартних операційних процедур.
- Розробіть стандарти сумісності, щоб забезпечити більш ефективний обмін інформацією через визначені стандарти та вимоги до даних, щоб включити (1) основу для середовища обміну інформацією, яке має загальні вимоги до даних та потік інформації та обмін між суб'єктами; та (2) вимоги до критичної інформації для конкретного сектору (тобто критичні критерії звітності), щоб забезпечити покращений потік інформації та звітність для отримання більш повної та своєчасної ситуаційної обізнаності для безпеки та стійкості.

Заклик до дії #6: Аналізуйте залежності, взаємозалежності та пов'язані каскадні ефекти інфраструктури

Пов'язана національна ціль:
- Оцінка та аналіз загроз, вразливостей і наслідків...

Поглиблений аналіз залежностей і взаємозалежностей на міжнародному, національному, регіональному та місцевому рівнях може стати основою для планування та сприяти визначенню пріоритетів ресурсів для забезпечення безперервності критичних послуг і пом'якшення каскадного впливу інцидентів, які трапляються.

- Розвивайте здатність визначати та розуміти міжсекторальні фізичні та кіберзалежності та взаємозалежності протягом різних часових меж на міжнародному, національному, регіональному та місцевому рівнях. Зосередьтеся на рятувальних функціях і стійкості глобальних ланцюгів постачання під час потенційно серйозних інцидентів,

враховуючи їх важливість для громадського здоров'я, добробуту та економічної діяльності.

- Продовжуйте розвивати підхід до ідентифікації кіберзалежної інфраструктури відповідно до Указу 13636, щоб врахувати потенційні ризики, пов'язані з залежністю від інформаційно-комунікаційних технологій, і інформувати про планування готовності та розвиток можливостей.

Заклик до дії #7: Виявляйте, оцінюйте та реагуйте на непередбачені каскадні ефекти інфраструктури під час та після інцидентів

Пов'язана національна ціль:

- Посилення стійкості критичної інфраструктури шляхом мінімізації негативних наслідків ...

Планування та навчання критичної інфраструктури та реагування на надзвичайні ситуації, а також події в реальному світі підкреслюють необхідність підготовки до каскадних ефектів під час інцидентів, які потенційно можуть посилити наслідки. Спільнота критичної інфраструктури може значно допомогти країні підготуватися до інцидентів, пов'язаних із усіма ризиками, розвинувши здатність швидко ідентифікувати, оцінювати та реагувати на каскадні наслідки, починаючи з функцій рятувальної лінії, під час і після інцидентів.

- Посилюйте здатність швидко визначати та оцінювати каскадні ефекти, пов'язані з функціями рятувальної лінії, і сприяти визначенню пріоритетів інфраструктури — як відомих, так і нових — під час заходів з реагування та відновлення.

- Посилюйте спроможність партнерів з критичної інфраструктури працювати через структури управління інцидентами, такі як ESF, щоб пом'якшити наслідки збоїв у функціях життєзабезпечення.

Заклик до дії #8: Сприяйте відновленню інфраструктури, спільноти та регіону після інцидентів

Пов'язана національна ціль:

- Посилення стійкості критичної інфраструктури шляхом мінімізації негативних наслідків

Нещодавні інциденти підкреслюють потребу в довгострокових можливостях відновлення для підвищення безпеки та стійкості інфраструктури, громад і регіонів під час відновлення. Щоб розвивати такі можливості, партнери з критичної інфраструктури можуть використовувати існуючі довірчі відносини та залучати цілий спектр партнерів із спільноти, активних у відновленні, включно з громадянами, некомерційними організаціями, бізнес-лідерами та представниками уряду, які зазвичай не залучені до обговорень інфраструктури чи безпеки.

- Залучайте федеральний польовий персонал (включно з радниками з питань безпеки) і заохочуйте штати та місцеві органи сприяти врахуванню проблем критичної інфраструктури при плануванні відновлення стану до інциденту, оцінці шкоди після інциденту та розробці стратегій відновлення.

- Підтримуйте вивчення ініціатив щодо вдосконалення, ремонту або заміни інфраструктури, що забезпечує життєві функції під час відновлення.

Заклик до дії #9: Посилюйте скоординований розвиток та забезпечуйте надання технічної допомоги, проведення навчань

Пов'язана національна ціль:

- **Сприяти навчанню та адаптації під час і після навчань та інцидентів ...**

Щоб продовжувати виконувати та підтримувати заходи з управління ризиками та готувати організації та спеціалістів до вирішення майбутніх викликів, спільнота критичної інфраструктури має продовжувати розробляти та надавати інноваційні програми технічної допомоги, навчання та освіти та оцінювати їх ефективність.

- Збирайте, звітуйте та визначайте пріоритети щодо технічної допомоги, навчання та освітніх потреб різних партнерів у спільноті критичної інфраструктури.

- Вивчіть поточні програми федеральної технічної допомоги, навчання та освіти, щоб переконатися, що вони підтримують національні пріоритети та заходи з управління ризиками, описані в цьому Національному плані, з метою просування прогресу на шляху до національних цілей.

- Поліпшуйте координацію зусиль щодо технічної допомоги, зокрема в рамках DHS і між SSA, і задіюйте ширшу мережу партнерів для реалізації навчальних і освітніх програм, щоб краще обслуговувати одержувачів і охоплювати ширшу аудиторію, зберігаючи ресурси.

- Співпрацюйте з академічними колами, щоб створити та оновити навчальні плани з критичної інфраструктури, які допоможуть навчити фахівців з критичної інфраструктури, включаючи керівників і менеджерів, керувати перевагами та притаманними вразливостями, створеними інформаційно-комунікаційними технологіями в активах, системах і мережах критичної інфраструктури.

Заклик до дії #10: Посилюйте безпеку та стійкість критичної інфраструктури за допомогою вдосконалення рішень щодо досліджень і розробок

> **Пов'язані національні цілі:**
> - Захист критичної інфраструктури від загроз...
> - Посилення стійкості критичної інфраструктури шляхом мінімізації негативних наслідків

PPD-21 зобов'язує федеральний уряд надати план досліджень і розробок (R&D), який враховує мінливий ландшафт загроз, річні показники та іншу відповідну інформацію для визначення пріоритетів і спрямування вимог до досліджень і розробок та інвестицій. Національний план досліджень і розробок безпеки та стійкості критичної інфраструктури буде перевидаватись кожні чотири роки з проміжними оновленнями за потреби. Він буде зосереджуватися на наступному:

- Просувайте дослідження і розробки для забезпечення безпечного та стійкого проєктування та будівництва критичної інфраструктури та більш безпечної супутньої кібертехнології;
- Розширюйте можливості моделювання для визначення потенційного впливу на критичну інфраструктуру сценарію інциденту чи загрози, а також каскадного впливу на інші сектори;
- Сприяйте ініціативам щодо заохочення інвестицій у кібербезпеку та впровадження критично важливих функцій інфраструктури, які посилюють безпеку та стійкість до всіх небезпек; та
- Пріоритезуйте зусилля для підтримки стратегічних вказівок, виданих DHS.

Щоб підвищити безпеку та стійкість інфраструктури, дослідження та розробки потребують координації для усунення прогалин в аналітичних і політичних можливостях, покращення можливостей управління ризиками для власників та операторів, а також виконання та переведення досліджень та розробок в оперативне використання. Дослідження та розробки повинні стосуватися захисту існуючої критичної інфраструктури, а також проєктування та будівництва нової інфраструктури з урахуванням взаємозалежностей. Пріоритети можуть випливати з вимог 16 секторів до досліджень та розробок, як із загальноприйнятих вимог, так і з окремих вимог, які забезпечують найбільшу потенційну віддачу. Національний план досліджень і розробок безпеки та стійкості критичної інфраструктури включатиме документи щодо планування досліджень і розробок, спрямовані на потреби та пріоритети з точки зору секторів.

Зосередження на результатах

Заклик до дії #11: Оцініть прогрес у досягненні цілей

> **Пов'язана національна ціль:**
> - Сприяти навчанню та адаптації під час і після навчань та інцидентів...

Хоча значна частина підґрунтя для інтегрованого циклу оцінювання, описаного в розділі 5, уже існує, партнери з критичної інфраструктури повинні брати участь у ширшому та більш послідовному масштабі, щоб полегшити розуміння прогресу та адаптивне прийняття рішень.

- Спільно визначте кінцеві результати або результати високого рівня, пов'язані з національними цілями та пріоритетами, щоб полегшити оцінку прогресу на шляху до цілей та пріоритетів.
- Щорічно розробляйте Національний звіт про критичну інфраструктуру та Національний звіт про готовність за допомогою стандартизованих запитів даних до SSA та галузевих партнерів, щоб створити національну картину прогресу на шляху до бачення та цілей Національного плану та Цілі національної готовності. Включайте дані про продуктивність від сектору, SLTT і регіональних організацій, щоб відобразити прогрес у спільноті критичної інфраструктури на всіх рівнях.

Заклик до дії #12: Навчайтеся та адаптуйтеся під час і після вправ та інцидентів

Враховуючи мінливий характер загроз і небезпек, національне прагнення до безпечної та стійкої критичної інфраструктури можливе лише завдяки колективним зусиллям численних партнерів, заснованих на постійному навчанні та адаптації до мінливого середовища. Спільнота критичної інфраструктури може краще реалізувати можливості для навчання та адаптації під час і після навчань та інцидентів завдяки більш спільному плануванню навчань, скоординованому отриманню уроків і процесам коригувальних дій, а також спрощеному обміну передовим досвідом.

- Розробляйте та проводьте вправи за допомогою процесів участі відповідно до різноманітних потреб і цілей.
  - Сприяти участі та координації між урядом і зацікавленими партнерами з приватного сектору, включно зі спільнотою досліджень та розробок, у плануванні, проведенні та оцінці вправ, щоб відобразити перспективи всіх партнерів і максимізувати цінність майбутнього планування та операцій.
  - Розробка вправ на багатьох рівнях і в різних форматах відповідно до національних, регіональних і SLTT потреб.

Пов'язана національна ціль:

- Сприяти навчанню та адаптації під час і після навчань та інцидентів...

- Розробіть вправи для відображення отриманих уроків і тестування коригувальних дій у результаті попередніх навчань та інцидентів, усунення як фізичних, так і кібернетичних загроз і вразливостей, а також оцінки переходу від стабільного стану до реагування на інцидент і зусиль з відновлення.
- Діліться отриманими уроками та коригуючими діями під час навчань та інцидентів і швидко включайте їх у програми технічної допомоги та навчання для покращення майбутніх зусиль щодо безпеки та стійкості.

Дії, перелічені в цьому розділі, не мають на меті бути вичерпними, а радше допомагають зосередити спільноту критичної інфраструктури для просування національних зусиль у напрямку безпеки та стійкості. Завдяки скоординованому та гнучкому впровадженню федеральними департаментами та агентствами, а також SLTT, регіональними партнерами та партнерами з приватного сектору, якщо це доцільно, враховуючи їхні унікальні перспективи управління ризиками, ці дії дозволять постійно вдосконалювати зусилля щодо безпеки та стійкості для вирішення як вже відомих, так і нових проблем.

Більше інформації про **NIPP** доступно в Інтернеті за посиланням:
www.dhs.gov/nipp

Скорочення

CDII	Ідентифікація кіберзалежної інфраструктури
CII	Інформація про критичну інфраструктуру
CIPAC	Консультативна рада партнерства з критичної інфраструктури
DHS	Департамент внутрішньої безпеки
EO	Указ
ESF	Функція екстреної підтримки
FACA	Акт про Федеральний консультативний комітет
FBI	Федеральне бюро розслідувань
FEMA	Департамент внутрішньої безпеки/Федеральне агентство з управління надзвичайними ситуаціями
FSLC	Федеральна рада вищого керівництва
GCC	Урядова координаційна рада
ISAC	Центр обміну та аналізу інформації
JTTF	Об'єднана оперативна група з боротьби з тероризмом
NCCIC	Національний центр інтеграції кібербезпеки та комунікацій
NCIJTF	Національна об’єднана оперативна група з кіберрозслідувань
NCIPP	Національна програма визначення пріоритетів критичної інфраструктури
NICC	Національний координаційний центр інфраструктури
NIPP	Національний план захисту інфраструктури
NOC	Національний оперативний центр
NRF	Національна структура реагування
PCII	Захищена інформація критичної інфраструктури
PNT	Позиціонування, навігація та час
PPD	Політична директива президента
R&D	Дослідження та розробка
RC3	Регіональна координаційна рада консорціуму
RSF	Функція підтримки відновлення
SCADA	Наглядовий контроль і збір даних
SCC	Секторальна координаційна рада
SLTT	У штатах, місцевий, племінний і територіальний
SLTTGCC	Координаційна рада штату, місцевого, племінного та територіального уряду
SNRA	Стратегічна національна оцінка ризиків
SOP	Стандартна операційна процедура
SSA	Секторальне агентство
SSP	Секторальний план

THIRA	Виявлення загроз і небезпек, а також оцінка ризиків
U.S.	Сполучені Штати
U.S.C.	Кодекс Сполучених Штатів

Глосарій термінів

Багато визначень у цьому глосарії взято з формулювань, прийнятих у федеральних законах і/або включених до національних планів, включаючи Закон про національну безпеку 2002 року; Патріотичний акт США 2001 року; 2009 NIPP; Президентська політична директива (PPD) 8, Національна готовність; і PPD-21, Безпека та стійкість критичної інфраструктури. Додаткові визначення взято з Лексикону DHS. Джерело для кожного запису нижче слідує кожному визначенню. Для цілей цього Національного плану застосовуються ці визначення:

Усі небезпеки. Термін «усі небезпеки» означає загрозу або інцидент, природний чи спричинений людиною, який вимагає дій для захисту життя, власності, навколишнього середовища, здоров'я чи безпеки населення, а також для мінімізації збоїв у державній, соціальній чи економічній діяльності. Включає стихійні лиха, кіберінциденти, промислові аварії, пандемії, терористичні акти, диверсії та руйнівну злочинну діяльність, спрямовану проти критичної інфраструктури. (Джерело: PPD-21, 2013)

Актив. Особа, структура, об'єкт, інформація, матеріал або процес, що має цінність. (Джерело: DHS Lexicon, 2010)

Безперервність бізнесу. Діяльність, що виконується організацією, щоб гарантувати, що під час та після лиха основні функції організації підтримуються безперервно або відновлюються з мінімальними збоями. (Джерело: адаптовано з 2009 NIPP)

Наслідок. Наслідки події чи інциденту, включаючи кількість смертей, поранень та інші наслідки для здоров'я людей, а також прямі та непрямі економічні наслідки та інші негативні наслідки для суспільства. (Джерело: Адаптовано з Лексикону DHS, 2010)

Системи управління. Комп'ютерні системи, які використовуються в багатьох інфраструктурах і галузях промисловості для моніторингу та керування чутливими процесами та фізичними функціями. Ці системи зазвичай збирають вимірювальні та оперативні дані, обробляють і відображають інформацію, а також передають команди керування локальному або віддаленому обладнанню або людино-машинним інтерфейсам (операторам). Приклади типів систем керування включають системи SCADA, системи керування процесами та розподілені системи керування. (Джерело: 2009 NIPP)

Критична інфраструктура. Системи та активи, будь то фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що непрацездатність або знищення таких систем і активів матиме негативний вплив на безпеку, національну економічну безпеку, охорону здоров'я, безпеку національній громадськості чи будь-яку комбінацію цих негативних впливів. (Джерело: §1016(e) Патріотичного акту США 2001 року (42 U.S.C. §5195c(e))

Спільнота критичної інфраструктури. Власники та оператори критичної інфраструктури, як державні, так і приватні; Федеральні відомства та агентства; Уряди штатів, місцеві, племінні та територіальні уряди та регіональні організації; та інші організації з приватного та некомерційного секторів, які відіграють роль у забезпеченні та зміцненні стійкості критично важливої інфраструктури країни та/або просуванні практик та ідей в цій сфері. (Джерело: NIPP 2013: Партнерство для безпеки та стійкості критичної інфраструктури)

Міжсекторальна рада критичної інфраструктури. Рада приватного сектору, до складу якої входять голови та заступники голів Секторальної координаційної ради. Ця рада координує міжсекторальні питання, ініціативи та взаємозалежності для підтримки безпеки та стійкості критичної інфраструктури. (Джерело: адаптовано з 2009 NIPP)

Інформація про критичну інфраструктуру (CII). Інформація, яка зазвичай не є загальнодоступною і пов'язана з безпекою критичної інфраструктури або захищених систем. CII складається із записів та інформації щодо будь-якого з наведеного нижче:

- Фактичне, потенційне або загрозливе втручання, атака, компрометація або виведення з ладу критичної інфраструктури чи захищених систем шляхом фізичної або комп'ютерної атаки чи іншої подібної поведінки (включно з неправильним використанням або несанкціонованим доступом до всіх типів комунікацій і систем

передачі даних), що порушує федеральний, державний або місцевий закон, завдає шкоди міждержавній торгівлі Сполучених Штатів, або загрожує громадському здоров'ю чи безпеці.

- Здатність критичної інфраструктури або захищеної системи протистояти такому втручанню, компрометації або виведенню з ладу, включаючи будь-яку заплановану або оцінку, що вже відбулась, прогноз або оцінку вразливості критичної інфраструктури/захищеної системи, включаючи тестування безпеки, оцінку ризиків, ризик планування управління, або аудит ризиків.
- Будь-яка запланована чи минула операційна проблема чи рішення щодо критичної інфраструктури чи захищених систем, включаючи ремонт, відновлення, страхування, у тій мірі, в якій це пов'язано з втручанням, компрометацією чи непрацездатністю. (Джерело: Закон CII 2002 р., 6 U.S.C. § 131)

Власники та оператори критичної інфраструктури. Ті суб'єкти, які відповідають за повсякденну роботу та інвестиції в певний об'єкт критичної інфраструктури. (Джерело: адаптовано з 2009 NIPP)

Партнер критичної інфраструктури. Ті федеральні державні установи, Уряди штатів, місцеві, племінні та територіальні уряди та регіональні організації, державні та приватні власники та оператори та представницькі організації, регіональні організації та коаліції, академічні та професійні організації, а також певні некомерційні та приватні волонтерські організації, які поділяють відповідальність за забезпечення та посилення стійкості критичної інфраструктури країни. (Джерело: адаптовано з 2009 NIPP)

Консультативна рада партнерства з критичної інфраструктури (CIPAC). Рада, створена DHS відповідно до 6 U.S.C. §451 для сприяння ефективній взаємодії та координації діяльності критичної інфраструктури між Федеральним урядом, приватним сектором та Урядом штатів, місцевих, племінних та територіальних урядів та регіональних організацій. (Джерело: Статут CIPAC)

Структура управління ризиками критичної інфраструктури. Структура планування та прийняття рішень, яка описує процес встановлення цілей і завдань, визначення інфраструктури, оцінки ризиків, впровадження діяльності з управління ризиками та вимірювання ефективності для інформування про постійне вдосконалення безпеки та стійкості критичної інфраструктури. (Джерело: адаптовано з 2009 NIPP)

Кібербезпека. Запобігання пошкодженню, несанкціонованому використанню або експлуатації та, якщо необхідно, відновлення електронних інформаційних і комунікаційних систем та інформації, що в них міститься, для забезпечення конфіденційності, цілісності та доступності; включає захист і відновлення, за потреби, інформаційних мереж і дротових, бездротових, супутникових, точок доступу громадської безпеки, а також систем зв'язку 911 і систем управління. (Джерело: 2009 NIPP)

Кіберсистема. Будь-яка комбінація засобів, обладнання, персоналу, процедур і комунікацій, інтегрованих для надання кіберпослуг; приклади включають бізнес-системи, системи контролю та системи контролю доступу. (Джерело: 2009 NIPP)

Залежність. Односпрямована залежність активу, системи, мережі або їх колекції (в межах сектору або між секторами) від вхідних даних, взаємодії чи іншої вимоги з інших джерел для належного функціонування. (Джерело: 2009 NIPP)

Розпорядження 13636. Указ, який вимагає від федерального уряду тісно координувати роботу з власниками та операторами критичної інфраструктури для покращення обміну інформацією про кібербезпеку; розробити технологічно нейтральну структуру кібербезпеки; а також заохочувати впровадження надійних практик кібербезпеки. (Виконавчий наказ 13636,17 «Покращення кібербезпеки критичної інфраструктури», лютий 2013 р.)

Функції екстреної підтримки (ESF). Первинні, але не єдино-виняткові, федеральні координаційні структури для створення, підтримки та надання основних засобів реагування. ESF є життєво важливими для реагування на інциденти, пов'язані із Законом Стаффорда, але також можуть використовуватися для інших інцидентів. (Джерело: Національна структура реагування, 2013 р)

Федеральні департаменти та агентства. Будь-який орган Сполучених Штатів, який є "агентством" згідно з 44 U.S.C. §3502(1), за винятком тих, які вважаються незалежними регулюючими агентствами, згідно з визначенням, наведеним в 44 U.S.C. §3502(5). (Джерело: PPD-21, 2013)

Функція. Послуга, процес або операція, виконані активом, системою, мережею або організацією. (Джерело: DHS Лексикон, 2010)

Центр фьюжн. Координаційний центр штату та великих міст для отримання, аналізу, збору та обміну інформацією про загрози між федеральним урядом, Урядом штатів, місцеві, племінні та територіальні уряди та регіональні організаціїі партнерами з приватного сектора. (Джерело: Адаптовано з Лексикону DHS, 2010)

Урядова координаційна рада (GCC). Урядовий аналог Секторальної координаційної ради для кожного сектору, створений для забезпечення міжвідомчої та міжурядової координації; складається з представників різних рівнів управління (федерального та Уряду штатів, місцеві, племінні та територіальні уряди та регіональні організації) залежно від ризику та операційної ситуації в кожному секторі. (Джерело: 2009 NIPP)

Небезпека. Природне чи штучне джерело або причина шкоди чи труднощів. (Джерело: DHS Lexicon, 2010)

Інцидент. Подія, спричинена як дією людини, так і природніми явищами, яка може призвести до шкоди і вимагати дії, включаючи великі катастрофи, надзвичайні ситуації, терористичні атаки, загрози тероризмом, лісові та міські пожежі, повені, витоки небезпечних речовин, ядерні аварії, авіакатастрофи, землетруси, урагани, торнадо, тропічні шторми, катастрофи пов'язані з війною, громадські заходи з охорони здоров'я та медичні надзвичайні ситуації, кібератаки, відмови/аварії кіберсистем, та інші події, які вимагають надзвичайної реакції. (Джерело: DHS Лексикон, 2010)

Інформаційно-аналітичні центри (ISACs). Операційні структури, створені власниками та операторами критичної інфраструктури для збору, аналізу, належного очищення та поширення розвідувальної інформації, пов'язаної з критичною інфраструктурою. Інформаційно-аналітичні центри (ISACs) забезпечують можливість оповіщення про загрози та повідомлення про інциденти цілодобово і мають здатність досягати та обмінюватися інформацією в межах своїх секторів, між секторами, а також між урядовими та приватними зацікавленими сторонами. (Джерело: Президентський розпорядження про прийняття рішень № 63, 1998 р.)

Організація з аналізу та обміну інформацією. Будь-яка офіційна чи неофіційна організація чи співробітництво, створене або використане організаціями державного чи приватного сектору з метою:

(a) Збір та аналіз інформації про критичну інфраструктуру, щоб краще зрозуміти проблеми безпеки та взаємозалежності, пов’язані з критичною інфраструктурою та захищеними системами, щоб забезпечити їх доступність, цілісність та надійність;

(b) Передача або розкриття інформації про критичну інфраструктуру, щоб допомогти запобігти, виявити, пом’якшити або відновити наслідки втручання, компрометації або проблеми з непрацездатністю, пов’язаної з критичною інфраструктурою чи захищеними системами; та

(c) Добровільне розповсюдження інформації про критичну інфраструктуру своїм членам, штатним, місцевим і федеральним урядам або будь-яким іншим організаціям, які можуть допомогти в досягненні цілей, зазначених у підпараграфах (a) і (b). (Джерело: Закон про національну безпеку 2002 року, 6 U.S.C. § 131)

Інфраструктура. Каркас взаємозалежних мереж та систем, що включає впізнавані галузі промисловості, установи (включаючи людей та процедури) та розподільні можливості, які забезпечують надійний потік продуктів та послуг, необхідних для оборони та економічної безпеки Сполучених Штатів, безперебійної роботи уряду на всіх рівнях та суспільства в цілому; відповідно до визначення в Законі про національну безпеку, інфраструктура включає фізичні, кібернетичні та/або людські елементи. (Джерело: DHS Лексикон, 2010)

Взаємозалежність. Взаємозалежні відносини між суб'єктами (об'єктами, індивідами або групами); ступінь взаємозалежності не обов'язково повинен бути рівним для обидвох сторін. (Джерело: DHS Lexicon, 2010)

Об'єднані оперативні групи з боротьби з тероризмом (JTTFs). Співпрацюючі місцеві робочі групи ФБР, які очолюються Федеральним Бюро Розслідувань (FBI) та складаються з висококваліфікованих федеральних, штатних та місцевих правоохоронних та розвідувальних агентств, призначених для збору розвідувальної інформації щодо терористичної діяльності та проведення розслідувань. Місцеві робочі групи ФБР отримують і розглядають повідомлення про можливу терористичну діяльність, надіслані приватними партнерами та громадськістю. (Джерело: Федеральне Бюро Розслідувань (FBI), 2013))

Пом'якшення. Спроможності, необхідні для зменшення втрат людей і майна шляхом зменшення впливу катастроф. (Джерело: PPD-8, 2011)

Національна об’єднана оперативна група з кіберрозслідувань. Міжвідомчий національний координаційний центр для координації, інтеграції та обміну відповідною інформацією, пов’язаною з розслідуваннями кіберзагроз, з федеральними агентствами, у тому числі DHS, а також штатних, місцевих і міжнародних партнерів з правоохоронних

органів. (Джерело: веб-сайт ФБР, www.fbi.gov)

Національний центр інтеграції кібербезпеки та комунікацій. Національний центр критичної кіберінфраструктури, визначений міністром національної безпеки, який забезпечує безпеку федеральних цивільних агенцій у кіберпросторі; надає підтримку та експертизу партнерам з приватного сектору та Урядам штатів, місцевим, племінним та територіальним урядам та регіональним організаціям; координує роботу з міжнародними партнерами; координує зусилля Федерального уряду щодо пом'якшення наслідків і відновлення після значних кібернетичних інцидентів і інцидентів зв'язку. (Джерело: веб-сайт DHS, www.dhs.gov)

Національний координаційний центр інфраструктури. Національний центр критичної інфраструктури, призначений Секретарем Міністерства національної безпеки, який координує національну мережу, присвячену безпеці та стійкості критичної інфраструктури Сполучених Штатів, забезпечуючи цілодобове відстеження ситуації шляхом обміну інформацією, а також сприяє єдності зусиль. (Джерело: Веб-сайт Міністерства нац безпеки, www.dhs.gov))

Центр національних операцій Міністерства внутрішньої безпеки. Операційний центр, який працює цілодобово з метою забезпечення оперативного відстеження ситуації в країні, координації заходів реагування на інциденти, а також випуску попереджень та бюлетенів про загрози національній безпеці, спільно з Офісом розвідки та аналізу, а також видачі конкретних захисних заходів.(Source: DHS Web site, www.dhs.gov)

Національна готовність. Дії, вжиті для планування, організації, оснащення, навчання та тренувань для створення та підтримки можливостей, необхідних для запобігання, захисту, пом'якшення наслідків, реагування та відновлення від тих загроз, які становлять найбільший ризик для безпеки Нації. (Джерело: PPD-8, 2011)

Мережа. Група компонентів, які обмінюються інформацією або взаємодіють один з одним для виконання функції. (Джерело: 2009 NIPP)

Партнерство. Тісна співпраця між сторонами, які мають спільні інтереси для досягнення спільного бачення. (Джерело: NIPP 2013: Партнерство для безпеки та стійкості критичної інфраструктури)

Президентська політична директива 8 (PPD-8). Сприяє інтегрованому загальнонаціональному підходу до національної готовності до загроз, які становлять найбільший ризик для безпеки країни, включаючи терористичні акти, кібератаки, пандемії та катастрофічні стихійні лиха; наказує федеральному уряду розробити національну систему готовності для створення та покращення можливостей, необхідних для підтримки національної готовності в п'яти сферах, охоплених PPD: запобігання, захист, пом'якшення, реагування та відновлення. (Джерело: PPD-8, 2011)

Президентська політична директива 21 (PPD-21). Метою є роз'яснення ролей і обов'язків у федеральному уряді та встановлення більш ефективного партнерства з власниками, операторами та Урядом штатів, місцевими, племінними та територіальними урядами та регіональними організаціями для підвищення безпеки та стійкості критичної інфраструктури. (Джерело: PPD-21,18 2013)

Запобігання. Можливості, необхідні для уникнення, запобігання або припинення загрози або фактичного акту тероризму.(Джерело: PPD-8, 2011)

Захищена інформація критичної інфраструктури (PCII). Уся інформація про критичну інфраструктуру, яка була належним чином подана та перевірена відповідно до Закону про інформацію про критичну інфраструктуру та імплементаційної Директиви; Уся інформація, надіслана в Офіс програми PCII або уповноваженій особі з прямою заявою, вважається PCII, доки Офіс програми PCII не визначить інше. (Джерело: Закон CII 2002 р., 6 U.S.C. § 131)

Захист. Спроможності, необхідні для захисту батьківщини від актів тероризму, техногенних або природних катаклізмів. (Джерело: PPD-8, 2011)

Відновлення. Можливості, необхідні для надання допомоги громадам, які постраждали від інциденту, для ефективного відновлення, включаючи, але не обмежуючись, відновленням систем інфраструктури; забезпечення належного тимчасового та довгострокового житла для постраждалих; відновлення охорони здоров'я, соціальних і громадських послуг; сприяння економічному розвитку; відновлення природних і культурних ресурсів. (Джерело: PPD-8, 2011)

Функції підтримки відновлення (RSF). Координаційні структури ключових функціональних сфер допомоги під час відновлення; RSF підтримують органи місцевого самоврядування, сприяючи вирішенню проблем, покращуючи доступ до ресурсів і сприяючи координації між штатними та федеральними агентствами, неурядовими партнерами та зацікавленими сторонами. (Джерело: National Disaster Recovery Framework, 2011)

Регіональні. Суб'єкти та інтереси, що охоплюють географічні області від великих мульти-штатних до метрополітенських областей, різняться за організаційною структурою та ключовими ініціативами, але сприяють залученню та співпраці між власниками та операторами критичної інфраструктури, урядом та іншими ключовими зацікавленими сторонами в даному регіоні. (Джерело: Regional Partnerships: Enabling Regional Critical Infrastructure Resilience, RC3, березень 2011)

Регіональна координаційна рада консорціуму. Включає регіональні групи та коаліції по всій країні, які беруть участь у різноманітних ініціативах для підвищення безпеки критичної інфраструктури та стійкості в державному та приватному секторах. (Джерело: адаптовано з 2009 NIPP)

Стійкість. Здатність готуватися до мінливих умов і адаптуватися до них, протистояти збоям і швидко відновлюватися після них; включає здатність протистояти навмисним атакам, нещасним випадкам або природним загрозам чи інцидентам і відновлюватися після них. (Джерело: PPD-21, 2013)

Реагування. Спроможності, необхідні для порятунку життів, захисту майна та навколишнього середовища, а також задоволення основних людських потреб після інциденту. (Джерело: PPD-8, 2011)

Ризик. Потенціал для небажаного результату після інциденту чи події, який визначається ймовірністю його настання та пов’язаними з ним наслідками. (Джерело: DHS Lexicon, 2010)

Прийняття рішень з урахуванням ризику. Визначення курсу дії, який базується на оцінці ризику, очікуваному впливу цього курсу дії на ризик та інших відповідних факторах. (Джерело: 2009 NIPP)

Сектор. Логічна сукупність активів, систем або мереж, які забезпечують спільну функцію для економіки, уряду чи суспільства; Національний план стосується 16 секторів критичної інфраструктури, визначених у PPD-21. (Джерело: адаптовано з 2009 NIPP)

Секторальна координаційна рада (SCC). Ці ради, які є аналогом Координаційних Рад Критичних Інфраструктур (GCC) у приватному секторі, є самоорганізованими, самоврядованими та самокерованими організаціями, які представляють спектр ключових зацікавлених сторін в межах конкретного сектору; виступають як головні точки уряду для співпраці з кожним сектором у розробці та координації широкого спектру заходів та питань забезпечення безпеки та стійкості критичної інфраструктури. (Джерело: Адаптовано з 2009 року NIPP)

Секторальне агентство (SSA). Федеральний департамент або агентство, призначене PPD-21, яке відповідає за надання інституційних знань і спеціалізованого досвіду, а також за керівництво, сприяння або підтримку програм безпеки та стійкості та пов’язаних з ними заходів у визначеному секторі критичної інфраструктури в середовищі всіх небезпек. (Джерело: PPD-21, 2013)

Секторальний план (SSP). Планувальні документи, які доповнюють і адаптують застосування Національного плану до конкретних характеристик і ландшафту ризиків кожного сектора критичної інфраструктури; розроблено SSA у тісній співпраці з SCC та іншими партнерами сеткору. (Джерело: адаптовано з 2009 NIPP)

Безпечний/Безпека. Зменшення ризику для критичної інфраструктури за допомогою фізичних засобів або захисних кіберзаходів від вторгнень, атак або наслідків природних чи техногенних катастроф. (Джерело: PPD-21, 2013)

Постійний режим функціонування. Стан рутинної, нормальної, повсякденної роботи, в контрасті з тимчасовими періодами підвищеної готовності або оперативної відповіді на загрози чи інциденти. (Джерело: DHS Лексикон, 2010)

Система. Будь-яка комбінація засобів, обладнання, персоналу, процедур і комунікацій, інтегрованих для певної мети. (Джерело: DHS Lexicon, 2010)

Тероризм. Передумовлена загроза або акт насильства проти осіб, майна, або економічних або екологічних об'єктів, які не є бойовими цілями, з метою викликати страх, запугати, змусити або вплинути на уряд, цивільне населення або його окремий сегмент, з метою реалізації політичних, соціальних, ідеологічних або релігійних цілей. (Джерело: DHS Лексикон, 2010)

Загроза. Природне або спричинене людиною явище, особа, організація або дія, яка має або вказує на потенційну шкоду життю, інформації, діяльності, навколишньому середовищу та/або власності. (Джерело: DHS Lexicon, 2010)

Виявлення загроз і небезпек, а також оцінка ризиків (THIRA). Інструмент, який дозволяє регіональним, штатним або міським юрисдикціям розуміти свої загрози та небезпеки, а також визначати, як впливи можуть змінюватися залежно від часу

виникнення, сезону, місця розташування та інших факторів. Ця інформація допомагає юрисдикції встановлювати обґрунтовані та відстоювані цілі щодо вмінь у готовності. (Джерело: Веб-сайт FEMA, www.fema.gov)

Ціннісна пропозиція. Заява, яка окреслює ділові та національні інтереси в діях із забезпечення безпеки та стійкості критичної інфраструктури та формулює переваги, отримані партнерами завдяки співпраці в механізмах, описаних у Національному плані. (Джерело: адаптовано з 2009 NIPP)

Вразливість. Фізична особливість або функціональна властивість, який робить об'єкт відкритим для експлуатації або чутливим до певної небезпеки. (Джерело: DHS Lexicon, 2010)

ДОДАТОК А. Національна структура партнерства

Механізми співпраці між власниками та операторами інфраструктури приватного сектору та урядовими агентствами спочатку були встановлені через План національного захисту критичної інфраструктури (NIPP) і подальше вдосконалені через Президентську політичну директиву №21 (PPD-21). PPD-21 розділила критичну інфраструктуру нації на 16 секторів, визначивши секторальні агенства (SSA) для кожного з секторів, та встановивши вимогу щодо партнерства між Федеральним урядом, власниками та операторами критичної інфраструктури, та штатними, місцевими, племінними та територіальними урядовими органами (SLTT). Ця структура секторальної та міжгсекторальної партнерських рад, що складається з секторальних координаційних рад (SCC), урядових координаційних рад (GCC), SSA та міжсекторальних рад, об'єднує партнерів з федерального уряду та SLTT, регіональні організації, приватний сектор та неурядові організації для співпраці над програмами та підходами безпеки критичної інфраструктури та стійкості, а також для досягнення національних цілей і завдань. Ці ради забезпечують первинні організаційні структури для координації зусиль і діяльності з безпеки критичної інфраструктури та стійкості всередині та між 16 секторами.

Секторальні координаційні структури

Координація між публічним та приватним секторами щодо безпеки та стійкості критичної інфраструктури здійснюється шляхом спільних зусиль партнерів в сфері критичної інфраструктури (включаючи SCCs, GCCs, міжсекторні ради та SSAs). Кожен з партнерів служить інтересам власної виборчої аудиторії, крім того, забезпечує взаємодію з іншими партнерами. Особливості партнерів представлені нижче.

Секторальні координаційні ради – SCC є самоорганізованими, самокерованими та самоврядними радами, які дозволяють власникам і операторам, їхнім торговим асоціаціям, постачальникам та іншим взаємодіяти щодо широкого спектру секторальних стратегій, політики та діяльності. SCC служать органами координації щодо секторальної політики та планування, для співпраці з SSA та GCC для вирішення всього спектру питань безпеки критичної інфраструктури та стійкості окремого сектору. Таким чином, вони є основними точками співпраці уряду з сектором в сфері безпеки критичної інфраструктури та стійкості. Крім того, SCC заохочуються брати участь у заходах із встановлення добровільних практик, що гарантують включення перспектив сектору.

Інші основні функції SCC можуть включати наступне:

- Служити механізмом стратегічної комунікації та координації між власниками, операторами та постачальниками, а також, у відповідних випадках, з урядом під час нових загроз або операцій реагування та відновлення, як це визначено сектором;
- Визначення, впровадження та підтримка відповідних можливостей та механізмів обміну інформацією в секторах, де не існує структури обміну інформацією;
- Заохочувати представницьке членство в секторі;
- Брати участь у плануванні, пов'язаному з переглядом Національного плану, розробкою та переглядом секторальних планів (SSP), а також переглядати щорічні подання до DHS щодо секторальних заходів;
- Сприяти інклюзивній організації та координації розробки секторальної політики щодо планування безпеки, стійкості та готовності критичної інфраструктури, навчань та тренінгів, інформування громадськості та пов'язаних заходів із впровадження та вимог;
- Визначати, розробляти та обмінюватися інформацією з представниками сектору, як державного, так і приватного, щодо ефективних методів кібербезпеки (робочі групи з кібербезпеки, оцінка ризиків, стратегії та плани);

- Розуміти та повідомляти про потреби сектору щодо державної підтримки;
- Надавати інформацію уряду щодо секторальних науково-дослідних робіт та вимог.

Урядові координаційні ради – GCC забезпечують міжвідомчу, міжурядову та міжюрисдикційну координацію всередині та між секторами. Вони складаються з представників різних рівнів управління (федерального та SLTT), відповідно до робочого ландшафту кожного окремого сектора. Кожну GCC очолює представник від призначеного SSA, відповідальний за забезпечення належного представництва в раді та забезпечення міжсекторальної координації з урядами SLTT. Помічник секретаря з питань захисту інфраструктури або призначена ним/нею особа є співголовами всіх GCC. GCC координує стратегії, діяльність, політику та комунікацію між державними установами в кожному секторі. GCC працює над координацією та підтримкою зусиль SCC.

Інші основні функції GCC можуть включати наступне:

- Забезпечення міжвідомчої стратегічної комунікації та координації на секторальному рівні через партнерство з DHS, SSA та іншими допоміжними установами на різних рівнях управління;
- Участь у плануванні, пов'язаному з переглядом Національного плану та розробкою та переглядом SSPs;
- Координувати стратегічні комунікації, обговорення, а також вирішення питань між державними установами в секторі;
- Сприяти впровадженню процесів управління фізичними та кібернетичними ризиками в усьому секторі;
- Розширення обміну урядовою інформацією в секторі та сприяння багатоканальному обміну інформацією між державним і приватним секторами;
- Визначати та підтримувати можливості та механізми обміну інформацією, які найбільше підходять для організацій SLTT;
- Координація та підтримка зусиль SCC щодо планування, впровадження та виконання місії безпеки та стійкості критичної інфраструктури країни.

Секторальні агентства SSA – Визнаючи існуючі статутні чи регулятивні повноваження певних федеральних міністерств і відомств, а також використовуючи існуючі секторальні зв'язки, SSA служать федеральним інтерфейсом для визначення пріоритетів і координації зусиль у галузі безпеки та стійкості та виконують обов'язки з управління інцидентами для своїх секторів. Що стосується секторів, які підлягають федеральному регулюванню або регулюванню штату, SSA співпрацює з регулюючим органом у відповідних випадках. SSA сприяють загальносекторальному обміну інформацією та підтримують національну програму безпеки та стійкості, розглядаючи спільні національні пріоритети та звітуючи про прогрес у досягненні результатів щодо безпеки та стійкості. Додаток В містить більш детальну інформацію про конкретні ролі та обов'язки SSA.

Секторальні координаційні структури

NIPP визначає чотири основні міжсекторні ради, які беруть участь у плануванні, пов'язаному з розробкою національних пріоритетів та відповідних політичних та планувальних документів, за допомогою яких буде проводитись керування заходами у сфері безпеки та стійкості критичної інфраструктури на національному рівні, включаючи цей національний план. Усі міжсекторні ради матимуть статути, включаючи підзаконні акти; ці документи будуть доступні публічно, щоб забезпечити прозоре управління. Кожна з цих рад описана нижче.

Секторальна рада критичної інфраструктури – Секторальна рада критичної інфраструктури є форумом SCC для вирішення секторальних проблем і взаємозалежностей. Рада складається з голів та заступників голів SCC або офіційно призначених ними осіб. Члени Ради можуть призначити Голову та заступника Голови Ради. Основна діяльність Ради включає:

- Забезпечення міжсекторальної стратегічної та політичної координації на вищому рівні через партнерство з DHS, FSLC, SLTTGCC та RC3;
- Виявлення та поширення найкращих практик безпеки та стійкості критичної інфраструктури в усіх секторах;

- Визначення сфер, у яких секторальна співпраця може просувати національні пріоритети;
- Участь у розробці та реалізації Національного плану.

Федеральна рада вищого керівництва (FSLC) – FSLC складається з вищих посадових осіб призначених SSA та інших федеральних департаментів і агентств, визначених у PPD-21. FSLC сприяє покращенню федерального зв'язку та координації між секторами, зосередженими на безпеці та стійкості критичної інфраструктури. До основних напрямків діяльності Ради входить:

- Досягнення консенсусу щодо стратегій управління ризиками;
- Оцінка та сприяння реалізації програм безпеки та стійкості критичної інфраструктури з урахуванням ризиків;
- Координація стратегічних питань і вирішення проблем між SLTTGCC, міжсекторальною радою критичної інфраструктури та RC3;
- Розширення співпраці всередині та між секторами та з міжнародним співтовариством;
- Підтримка та відстеження виконання Національного плану в усіх органах виконавчої влади;
- Підтримка розробки запитів на ресурси для виконання федеральної місії;
- Оцінка та звітування про прогрес Федеральної безпеки критичної інфраструктури та діяльності щодо стійкості.

Координаційна рада штату, місцевого, племінного та територіального урядів (SLTTGCC) – SLTTGCC служить форумом для сприяння залученню партнерів SLTT як активних учасників заходів із забезпечення безпеки та стійкості національної критичної інфраструктури, а також для забезпечення організаційної структури для координації між вказівками, стратегіями і програмами SLTT на урядовому рівні. SLTTGCC:

- Забезпечує міжюрисдикційні стратегічні комунікації та координацію на вищому рівні через партнерство з федеральним урядом та власниками та операторами критичної інфраструктури;
- Координує стратегічні питання та вирішення проблем між федеральними департаментами та агентствами та партнерами SLTT;
- Координує роботу з FSLC, Міжсекторальною радою з критичної інфраструктури та RC3 для підтримки зусиль із планування, впровадження та виконання місії безпеки та стійкості критичної інфраструктури країни;
- Надає DHS інформацію про ініціативи, заходи та найкращі практики на рівні безпеки та стійкості SLTT;
- Співпрацює з DHS у створенні тестових майданчиків демонстраційних проектів для підтримки інновацій.

Регіональна координаційна рада консорціуму (RC3) – RC3 забезпечує структуру, яка підтримує існуючі регіональні групи в їхніх зусиллях сприяти діяльності зі стійкості в державному та приватному секторах. RC3, що складається з різноманітних регіональних груп з усієї країни, підтримує свої організації-члени шляхом підвищення обізнаності, освіти та наставництва з різноманітних тем, проектів та ініціатив. RC3 бере участь у різноманітних ініціативах із покращення безпеки та стійкості критичної інфраструктури, зменшення вразливості та пом'якшення наслідків, зокрема::

- Співробітництво з Міжсекторальною радою критичної інфраструктури, FSLC і SLTTGCC для покращення обміну інформацією та комунікації в рамках національного партнерства та визначення способів, як чотири ради можуть використовувати членство та знання одна одної;
- Проведення вебінарів для покращення розуміння партнерами Національного плану та його впровадження;
- Проведення регіональних навчань з реагування на катастрофи та відновлення після них у поєднанні з існуючими регіональними семінарами;
- Визначення найкращих практик і стандартів використання інструментів соціальних медіа для забезпечення безпеки та стійкості критичної інфраструктури;
- Розробка стратегії комунікації та співпраці, яка охоплює технології соціальних медіа та використовує засоби контролю, а також практики, які є ефективними, результативними та співмірними з виникаючим середовищем ризиків;
- Допомога в розробці та координації штатних і місцевих Реєстрів критичної інфраструктури.

Організації аналізу та обміну інформацією

За останнє десятиліття було створено декілька організацій приватного сектору, які займаються обміном інформацією та аналізом. ISAC є прикладами успішних організацій з обміну інформацією.

ISACs – ISAC служать оперативними та розповсюджувальними механізмами для багатьох секторів і підсекторів і сприяють обміну інформацією між урядом і приватним сектором. ISAC тісно співпрацюють з SCC у секторах. Вони призначені для забезпечення глибокого аналізу всередині сектору та сприяють координації дій з реагування сектора під час інцидентів, включаючи обмін інформацією всередині секторів, між секторами та між зацікавленими сторонами державного та приватного секторів. Урядові установи також можуть покладатися на ISAC для отримання ситуаційної обізнаності та для покращення своєї здатності надавати своєчасні дані, які можна застосувати до цільових організацій. Основними видами діяльності ISAC є:

- Створення довірених спільнот та платформ для секторів критичної інфраструктури, що дозволяють обмінюватися своєчасною, практично застосовною та надійною інформацією для забезпечення ситуаційної обізнаності;
- Забезпечення поглибленого комплексного аналізу загроз та інцидентів у секторі та забезпечення агрегації та анонімізації даних;
- Надавати інформацію про загрози (з усіма можливими ризиками) та звіт про інциденти для покращення заходів з управління ризиками;
- Започатковувати та підтримувати співпрацю з центрами операцій, такими як Центр національної інфраструктури (NICC) та Центр кібербезпеки критичної інфраструктури (NCCIC);
- Брати участь у плануванні, координації та проведенні вправ, якщо це необхідно.

Консультативна рада партнерства з критичної інфраструктури

Консультативна рада партнерства з критичної інфраструктури (CIPAC) була створена DHS у 2006 році як механізм підтримки інтересів секторів та спільної участі в обговореннях у сфері критичної інфраструктури, а також участі в широкому спектрі заходів. Форуми CIPAC мають консультативну роль, підтримуючи обговорення критичних питань у сфері інфраструктури, які необхідні для досягнення консенсусу або під час надання офіційних рекомендацій федеральному уряду. Обговорення та заходи, вжиті після звернення до CIPAC, включають наступне:

- Планувати, координувати та обмінюватися інформацією щодо секторальних або міжсекторальних питань;
- Консультування щодо операційної діяльності, пов’язаної з безпекою та стійкістю критичної інфраструктури, як у штатному режимі, так і під час реагування на інциденти;
- Сприяти розробці та впровадженню національних політик і планів, включаючи цей Національний план і SSP;
- Подавати федеральному уряду рекомендації щодо програм, інструментів і можливостей критичної інфраструктури.

CIPAC може скликати представників GCC і SCC, коли є потреба досягти консенсусу з певного питання. Таким чином, CIPAC може використовуватися на секторальному, міжсекторальному рівні або на рівні робочої групи, залежно від теми та мети обговорення. Зустрічі, форуми та інші заходи CIPAC відвідують представники уряду та приватного сектору, і часто включають запрошених експертів із певної тематики.

Обмін інформацією для забезпечення безпеки та стійкості критичної інфраструктури

Крім інформації, поширеної від спеціальних служб та інших національних механізмів партнерства, існують федеральні організації з аналізу та обміну інформацією, які вирішують національні питання, а також виконують оперативні ролі для підтримки органів влади на рівні штатів, місцевих урядів та приватних власників та операторів. Вони включають Національний Центр Координації Інфраструктури (NICC), Національний Центр Кібербезпеки та Зв'язків (NCCIC), Національний Операційний Центр (NOC) та Національна Спільна Робоча Група З Розслідування Кіберзлочинів (NCIJTF).

NICC та NCCIC – PPD-21 зазначає, що "Мають бути два національні центри критичної інфраструктури, які працюють під керівництвом DHS - один для фізичної інфраструктури [NICC] та інший для кібернетичної інфраструктури [NCCIC]. Вони мають функціонувати в інтегрованому вигляді та служити точками фокусу для партнерів з критичної інфраструктури з метою отримання ситуаційної обізнаності та інтегрованої, дієвої інформації для захисту фізичних та кібернетичних аспектів критичної інфраструктури." NICC виступає як центр обміну та синтезу інформації, який отримує дані про критичну інфраструктуру та надає цю інформацію приймачам рішень на різних рівнях для швидкого та обґрунтованого прийняття рішень в штатному режимі, в умовах підвищеної готовності та під час реагування на події. Центр з кібербезпеки та зв'язку (NCCIC) - це центр обміну інформацією, аналізу та реагування на події, який працює цілодобово. У ньому відбувається обмін інформацією та співпраця між урядом, приватним сектором та міжнародними партнерами з питань реагування на події та зменшення впливу значних інцидентів. Це також місце розробки та видачі попереджень та планування стратегічних та тактичних заходів для боротьби з майбутньою зловмисною діяльністю з питань кібербезпеки. PPD-21 також вимагає наявності інтегрованого компонента аналізу, який працює в співпраці з обома центрами, щоб контекстуалізувати та сприяти більш глибокому розумінню інформаційних потоків, що протікають через два центри.

Ці центри, спільно з функцією інтегрованого аналізу, забезпечують надання загальної ситуаційної обізнаності різним секторам критичної інфраструктури на основі внеску партнерів, а також надають більш глибоку, широку та контекстну інформацію, ніж окремі компоненти системи.

NOC – NOC є головним оперативним центром при DHS, що складається з NOC Watch, Intelligence Watch and Warning, National Watch Center FEMA і National Coordination Center Response, а також NICC. NOC забезпечує ситуаційну обізнаність і загальну оперативну картину для всього федерального уряду та для урядів SLTT у разі стихійного лиха, терористичного акту чи іншої техногенної катастрофи. NOC також гарантує, що важлива інформація, пов’язана з тероризмом і стихійними лихами, досягне урядових органів.

NCIJTF – ФБР відповідає за роботу NCIJTF, міжагентурного центру кібербезпеки, що має основну відповідальність за розробку та обмін інформацією, пов'язаною з розслідуваннями кіберзагроз, а також за координацію та інтеграцію відповідних оперативних заходів з протидії кіберзагрозам, включаючи загрози критичній інфраструктурі. NCIJTF - це альянс рівноправних агентств з взаємодоповнюючими місіями з охорони національних кіберінтересів. Представники з федеральних агентств, включаючи DHS, а також з правоохоронних органів на рівні штатів, місцевих органів влади та міжнародних партнерів з правоохоронних органів, мають доступ до комплексного уявлення про кіберзагрози, працюючи разом в середовищі співпраці.

Співпраця спільноти критичної інфраструктури

Структури партнерства, описані вище, призначені для стимулювання участі суб'єктів критичної інфраструктури та зацікавлених сторін по всій країні. Ці структури також сприяють узгодженості процесу забезпечення ефективної співпраці в спільноті критичної інфраструктури. Це не означає, що партнерство на рівні сектору та міжсектору мають бути повністю репліковані на регіональному, штатному та місцевому рівнях, однак їх доведена корисність може служити моделлю та приносити цінність на різних рівнях.

Додаткові регіональні партнерства об’єднали різноманітні інтереси (в т.ч. операційні інтереси) в межах державних кордонів, районів, секторів інфраструктури для створення організацій для вирішення спільних проблем. Співпраця на регіональному рівні вимагає гнучкості для залучення інших суб’єктів, які відіграють важливу роль у забезпеченні безпеки та стійкості критичної інфраструктури, таких як підрозділи InfraGard ФБР, координатори зі зброї масового знищення (WMD), польові розвідувальні групи та об’єднані оперативні групи з боротьби з тероризмом (JTTF). JTTF — це міжвідомчі цільові групи, створені для об’єднання ресурсів, персоналу, навичок і знань місцевих, штатних, племінних, територіальних і федеральних правоохоронних органів, а також розвідувального співтовариства в єдину команду, яка виявляє, розслідує, аналізує, реагує на терористичні загрози або інциденти. Про підозрілу діяльність, яка може бути пов’язана з тероризмом, необхідно негайно повідомляти найближчому JTTF для розслідування та вирішення проблеми. JTTFs слід розглядати як центри прийому повідомлень про підозрілу діяльність, яка може мати відношення до тероризму. JTTFs обмінюються інформацією з іншими регіональними правоохоронними органами, партнерами критичної інфраструктури, а також з фьюжн-центрами на рівні штатів та міських агломерацій. Domestic Security Alliance Council також співпрацює з ФБР.

DHS і ФБР мають надійні програми захисту критичної інфраструктури, розроблені для виявлення терористичних загроз, пов’язаних із критичною інфраструктурою. Наприклад, Загальнонаціональна ініціатива звітування про підозрілу діяльність (NSI) передбачає партнерство DHS і ФБР для підвищення обізнаності шляхом розробки продуктів з оцінки загроз та цільової публікації брошур, плакатів та повідомлень для громадського та приватного секторів. Ці повідомлення адаптовані до конкретної загрози та призначені для отримання повідомлень про підозрілу діяльність від спільноти, щоб ці загрози могли бути швидко перенаправлені до найближчого JTTF для розслідування та вирішення. Кампанія DHS «Якщо ти щось бачиш, скажи щосьTM» є прикладом такого публічного обміну повідомленнями.

Ф’южн-центри на рівні штатів та великих міських агломерацій допомагають власникам і операторам критичної інфраструктури та урядовим партнерам бути в курсі загроз та вразливостей, що з'являються. Представники місцевих та регіональних урядів (наприклад, відповідальні за управління надзвичайними ситуаціями, громадським здоров'ям та громадською безпекою) можуть регулярно співпрацювати з ф’южн-центрами для отримання, аналізу, збирання та обміну інформацією про правопорушення та захист серед партнерів на рівні штату, місцевих та федеральних рівнів. Додатково, консультанти Міністерства національної безпеки, адаптивної безпеки, кібербезпеки, координатори ФБР щодо знищення зброї масового знищення, координатори InfraGard та члени JTTF також взаємодіють з ф’южн-центрами.

Штатний компонент партнерства критичної інфраструктури виходить за межі SLTTGCC і включає штатні коаліції та оперативні партнерства, а також, де це можливо, секторальні агентства штатного рівня, які підтримують надання основних послуг, таких як енергетика, телекомунікації, водопостачання та транспорт. Ці штатані та регіональні партнерства розробляють інтегровані плани готовності, безпеки та стійкості на основі аналізу ризиків, який враховує місцеві та регіональні фактори.

Місцеві партнерства щодо критичної інфраструктури часто пов’язані з місцевими торговими палатами, бізнес-круглими столами або подібними коаліціями компаній приватного сектора. Вони також включають державно-приватні партнерства, а також громадські організації, які підтримують готовність, реагування та відновлення.

PPD-21 закликає до міжнародної співпраці як частини національної єдності зусиль для посилення безпеки та стійкості. З цією метою федеральний, приватний сектор і міжнародні партнери співпрацюють над впровадженням узгоджених заходів безпеки глобальної інфраструктури для захисту від поточних і майбутніх фізичних і кібернетичних загроз. Міжнародне співробітництво відбувається в багатьох сферах, включаючи обмін інформацією, впровадження існуючих угод, що впливають на безпеку та стійкість критичної інфраструктури, розробку політик транскордонної координації ініціатив із забезпечення безпеки та стійкості, вирішення міжсекторальних і глобальних проблем, таких як кібербезпека, а також покращення розуміння прикордонних взаємозалежностей критичної інфраструктури.

Додаток B. Ролі, обов’язки та можливості партнерів і зацікавлених сторін у критичній інфраструктурі

PPD-21: "Ефективні національні зусилля щодо посилення безпеки та стійкості критичної інфраструктури повинні керуватися національним планом, який визначає ролі та обов'язки (на основі досвіду, можливостей і обов'язків) SSA, інших федеральних департаментів та агентств, організацій SLTT, а також власників та операторів критичної інфраструктури".

Визнаючи обмеження ресурсів, за яких працюють як державні, так і приватні партнери, ролі та види діяльності, описані в цьому додатку, не визначені як вимоги до будь-якого партнера чи групи зацікавлених сторін. Багато ролей і обов’язків, описаних нижче, надаються для довідки, щоб мати загальне усвідомлення можливих ролей у спільноті критичної інфраструктури.

Цей додаток включає ролі та обов'язки федерального уряду, визначені в PPD-21 і описані в документі "Функціональні відносини забезпечення безпеки та стійкості критичної інфраструктури", розробленому Інтегрованою робочою групою Департаменту національної безпеки (DHS) та опублікованому в червні 2013 року.
Деякі додаткові ролі та обов’язки, описані в NIPP 2009 року, залишаються застосовними, а також включені сюди для федерального уряду, власників і операторів критичної інфраструктури, урядів SLTT, консультативних рад і комітетів, а також наукових і дослідницьких організацій.
Існують певні ролі та можливості, які розподіляються між різними групами партнерів. Вони повторюються нижче (і адаптовані, де це необхідно) для кожного партнера, до якого вони застосовуються. Це дозволяє членам спільноти критичної інфраструктури ознайомитися з розділом цього додатку, який найбільше підходить для них.

Міністр національної безпеки

PPD-21 визначає наступні ролі та обов’язки Міністру національної безпеки.

Міністр національної безпеки забезпечує стратегічне керівництво, сприяє національній єдності зусиль і координує всі федеральні зусилля для сприяння безпеці та стійкості критичної інфраструктури країни. Виконуючи обов'язки Закону про національну безпеку 2002 року з поправками, Міністр національної безпеки:

- Оцінює національний потенціал, можливості та виклики у забезпеченні безпеки та створенні стійкої критичної інфраструктури;
- Аналізує загрози, вразливі місця та потенційні наслідки всіх небезпек для критичної інфраструктури;
- Визначає функції забезпечення безпеки та стійкості, необхідні для ефективної взаємодії державно-приватного сектору з усіма секторами критичної інфраструктури;
- Розробляє національний план та метрики взаємодії зі спеціальними службами, іншими партнерами критичної інфраструктури;
- Інтегрує та координує діяльність Федерального уряду щодо безпеки та стійкості міжсекторальної критичної інфраструктури;
- Інтегрує та координує діяльність Федерального уряду щодо безпеки та стійкості міжсекторової критичної інфраструктури;
- Звітує про ефективність національних зусиль щодо посилення національної безпеки та стійкості критичної інфраструктури.

Міністр національної безпеки є головною федеральною посадовою особою з управління внутрішніми інцидентами та координації федеральної діяльності щодо готовності відповідно до PPD-8, включаючи координацію реагування федерального уряду на значні кібернетичні або фізичні інциденти, що впливають на критичну інфраструктуру. Міністр національної безпеки координує роботу з іншими членами виконавчої гілки влади, якщо це доцільно, для підтримки єдиного комплексного підходу до внутрішнього управління інцидентами, щоб усі рівні уряду країни мали можливість ефективно та результативно працювати разом, використовуючи національний підхід до управління інцидентами.

PPD-21 визначає додаткові ролі та обов'язки Міністра національної безпеки, в тому числі:

- Визначати та пріоритезувати критичну інфраструктуру, враховуючи фізичні та кібер загрози, вразливості та наслідки, у співпраці з відповідними службами та іншими федеральними відомствами та агентствами;
- Підтримувати національні центри критичної інфраструктури, які забезпечують ситуаційну обізнаність, яка включає інтегровану, дієву інформацію про нові тенденції, неминучі загрози та стан інцидентів, які можуть вплинути на критичну інфраструктуру;
- У координації з SSA та іншими федеральними департаментами та відомствами надавати аналіз, експертизу та іншу технічну допомогу власникам і операторам критичної інфраструктури та сприяти доступу та обміну інформацією та розвідданими, необхідними для посилення безпеки та стійкості критичної інфраструктури;
- Проводити комплексну оцінку вразливостей критичної інфраструктури країни в координації з SSA та у співпраці з організаціями SLTT та власниками та операторами критичної інфраструктури;
- Координація реагування федерального уряду на значні кібернетичні або фізичні інциденти, що впливають на критичну інфраструктуру, відповідно до законних повноважень;
- Надавати підтримку Генеральному прокурору та правоохоронним органам у виконанні їх обов'язків щодо розслідування та переслідування загроз та атак на критичну інфраструктуру;
- Координація та використання досвіду SSA та інших відповідних федеральних департаментів і агентств для картографування геопросторових зображень, аналізу та сортування критичної інфраструктури за допомогою використання комерційних супутникових і бортових систем, а також наявних можливостей інших департаментів і агентств;
- Щорічно звітувати про стан національної критичної інфраструктури, як того вимагає закон.

Додаткові ролі та обов'язки DHS включають:

- Створити та підтримувати комплексну, багаторівневу та динамічну мережу обміну інформацією, призначену для надання своєчасної та дієвої інформації про загрози, оцінки та попередження партнерам в державному та приватному секторах (включаючи захист конфіденційної інформації, добровільно наданої приватним сектором), а також сприяти розробці секторальних і міжсекторальних систем, механізмів і процесів обміну інформацією та аналізу;
- Спонсорувати дослідження та розробки, демонстраційні проекти та пілотні програми, пов'язані з безпекою критичної інфраструктури та стійкістю;
- Проводити за участю SSA моделювання та симуляції для аналізу секторальних, міжсекторальних і регіональних залежностей і взаємозалежностей (включаючи кіберзалежності), а також ділитися результатами з партнерами з критичної інфраструктури, якщо це необхідно;
- Фіксувати та використовувати уроки, отримані під час навчань, фактичних інцидентів та попередніх заходів мінімізації наслідків стихійного лиха, в діяльності з забезпечення безпеки та стійкості критичної інфраструктури;
- Визначення необхідності та координація заходів забезпечення безпеки та стійкості додаткових категорій критичної інфраструктури з часом, відповідно до потреб.

Секторальні агентства (**SSA**)

PPD-21 визначає наступні ролі та обов’язки SSA.

Кожен сектор критичної інфраструктури має унікальні характеристики, операційні моделі та профілі ризику. Федеральні секторальні агентства або міжсекторальні агентства, відповідають кожному сектору, мають інституційні знання та спеціалізований досвід щодо свого сектора(ів). Враховуючи існуючі законодавчі або регуляторні повноваження конкретних федеральних відомств та агентств, і використовуючи наявний секторальний досвід та взаємини, SSA:

- Координувати роботу з DHS та іншими федеральними департаментами та відомствами, а також співпрацювати з власниками та операторами критичної інфраструктури, де це доцільно, з незалежними регуляторними органами та з організаціями SLTT, якщо це доречно для впровадження PPD-21;
- Виконувати роль щоденної федеральної точки зв'язку для динамічної пріоритизації та координації діяльності, специфічної для сектору;
- Виконувати обов'язки з управління інцидентами відповідно до законних повноважень та інших відповідних політик, директив або правил;
- Надавати, підтримувати або сприяти технічній допомозі та консультаціям для цього сектору для виявлення вразливостей та допомоги у пом’якшенні інцидентів, якщо це доречно;
- Підтримувати вимоги Міністра національної безпеки щодо звітності, надаючи на щорічній основі інформацію про критичну інфраструктуру окремих секторів.

SSA наведено в таблиці B-1 нижче.

Таблиця B-1 – Секторальні агентства та сектори критичної інфраструктури

Сеткоральне агентство	**Сектор критичної інфраструктури**
Міністерство сільського господарства США (a) Міністерство охорони здоров'я і соціальних служб США	Харчування та сільське господарство
Міністерство оборони (b)	Оборонно-промислова база
Департамент енергетики (c)	Енергетичний (d)
Міністерство охорони здоров'я і соціальних служб США	Охорона здоров'я та громадське здоров'я
Міністерство фінансів США	Фінансові послуги
Управління з охорони довкілля США	Послуги водопостачання та водовідведення
Міністерство національної безпеки США	хімічний Критичне виробництво Інформаційні технології Комерційні об'єкти Дамби Ядерні реактори, матеріали та відходи Комунікації Аварійні служби
Міністерство національної безпеки США, Адміністрація служб загального призначення	Державні установи (e)
Міністерство національної безпеки США, Міністерство транспорту США	Транспортні системи

[a] Міністерство сільського господарства США відповідає за сільське господарство та продовольство (м'ясо, птиця та перероблені яєчні продукти).

b Департамент охорони здоров'я та соціальних служб відповідає за харчові продукти, крім м'яса, птиці та оброблених яєчних продуктів.

c Ніщо в цьому плані не послаблює та іншим чином не впливає на повноваження Міністра оборони над Міністерством оборони (DoD), включаючи ланцюг командування збройними силами від Президента як Головнокомандувача до Міністра оборони та командувача збройних сил, а також не впливає на процедури військового командування та контролю.

d Енергетичний сектор включає виробництво, переробку, зберігання та розподіл нафти, газу та електроенергії. Міністерство національної безпеки є SSA для комерційних ядерно-енергетичних установок і дамб.

e Міністерство освіти є SSA для підсектору навчальних закладів Сектору державних закладів; Міністерство внутрішніх справ є SSA для підсектору національних пам'яток і ікон Сектору державних установ.

Інші федеральні відомства та агентства

Як зазначено в PPD-21, федеральні відомства та агентства повинні своєчасно надавати інформацію Міністру національної безпеки та національним центрам критичної інфраструктури, необхідну для міжсекторального аналізу та для отримання ситуаційної обізнаності у сфері критичної інфраструктури; центри, у свою чергу, обмінюватимуться інформацією з відповідними партнерами у сфері критичної інфраструктури.

Федеральні відомства та агентства, які не є SSA, але мають унікальні обов'язки, функції чи досвід у певному секторі критичної інфраструктури (наприклад, члени GCC), допомагають у ідентифікації та оцінці критичної інфраструктури з високим ступенем ризику та співпрацюють з партнерами для обміну інформацією щодо безпеки та стійкості критичної інфраструктури в межах сектору, якщо це необхідно.

Наступні відомства та агентства (деякі з яких також виконують роль SSA), мають спеціалізовані або допоміжні функції, пов'язані з безпекою та стійкістю критичної інфраструктури, які мають виконуватися іншими федеральними департаментами та агентствами та незалежними регуляторними органами або разом з ними, якщо це доречно.

Державний департамент США

Державний секретар несе безпосередню відповідальність за політику та заходи щодо захисту громадян США та об'єктів США за кордоном, і є керівником зовнішніх відносин, політики, діяльності та просування інтересів США за кордоном. У рамках повсякденної дипломатичної діяльності від імені уряду США Державний департамент (DOS) відповідає за встановлення та підтримку міжнародних відносин, які є важливими для забезпечення безпеки та стійкості критичної інфраструктури. DOS, у координації з DHS, SSA та іншими федеральними департаментами та агентствами, координує роботу з іноземними урядами, міжнародними організаціями та приватним сектором США через Консультативну раду з безпеки за кордоном (OSAC), щоб посилити безпеку та стійкість критичної інфраструктури, розташованої за межами Сполучених Штатів, і сприяти обміну найкращими практиками та отриманими уроками у сфері забезпечення безпеки та стійкості критичної інфраструктури.

Міністерство оборони США

Для підтримки безпеки та стійкості критичної інфраструктури Міністерство оборони (DoD) керує, забезпечує безпеку та стійкість критичної інфраструктури, що належить Міністерству оборони або з якою укладено контракт; захищає націю від атак у всіх сферах, включаючи кібер сферу; збирає дані зовнішньої розвідки та встановлює відповідність в рамках національних вимог і вимог Міністерства оборони; забезпечує безпеку національних систем безпеки та військових систем; розслідує злочинну кіберактивність під військовою юрисдикцією. Агентство криптологічної розвідки США, як частина Міністерства оборони та розвідувального співтовариства, надає підтримку зовнішньої розвідки та інформаційну підтримку DHS, інших департаментів і агентств відповідно до Указу 12333.

Міністерство юстиції США

Міністерство юстиції (DOJ), у тому числі Федеральне бюро розслідувань (ФБР), веде антитерористичні та контррозвідувальну та пов'язану правоохоронну діяльність у секторах критичної інфраструктури. Міністерство юстиції розслідує, запобігає, переслідує та іншими способами знижує загрози зовнішньої розвідки, терористичних та інших загроз для національної критичної інфраструктури, а також фактичні напади чи спроби нападів на критично важливу інфраструктуру країни чи саботаж. ФБР також проводить внутрішній збір, аналіз і розповсюдження інформації про кіберзагрози та відповідає за роботу Національної об'єднаної оперативної групи з кіберрозслідувань (NCIJTF). NCIJTF є міжвідомчим національним координаційним центром, який координує, об'єднує та ділиться відповідною інформацією, пов'язаною з розслідуваннями кіберзагроз, з представниками DHS, розвідувального співтовариства та Міністерства оборони, а також співпрацює з SSA та іншими агенціями, якщо це необхідно.

Міністерство внутрішніх справ США

Міністерство внутрішніх справ у співпраці з SSA визначає пріоритети та координує зусилля щодо забезпечення безпеки та стійкості національних пам'яток і символів для сектору державних установ, а також передбачає заходи зменшення ризиків для цих критичних активів, забезпечуючи їх використання.

Міністерство торгівлі США

Міністерство торгівлі у співпраці з DHS, SSA та іншими відповідними федеральними департаментами та агентствами залучає приватний сектор, науково-дослідницькі, академічні та урядові організації для покращення безпеки технологій та інструментів, пов'язаних із кіберсистемами, і забезпечує доступність промислової продукції, матеріалів і послуг для задоволення вимог внутрішньої безпеки.

Розвідувальне співтовариство США

Розвідувальне співтовариство, очолюване Директором національної розвідки, має відповідні повноваження та координаційні механізми для надання, оцінки розвід даних щодо загроз критичній інфраструктурі та координації розвідувальної та іншої конфіденційної інформації, пов'язаної з критичною інфраструктурою. Крім того, він віджстежує політику інформаційної безпеки, директиви, стандарти та вказівки щодо захисту систем національної безпеки відповідно до указів Президента, чинного законодавства та на підставі повноважень керівників агенцій, які контролюють або мають повноваження щодо таких національних систем безпеки.

Адміністрація служб загального призначення

Адміністрація служб загального призначення, консультуючись із Міністерством оборони, Міністерством охорони здоров'я та іншими федеральними департаментами та відомствами, надає або підтримує загальнодержавні контракти щодо систем критичної інфраструктури та гарантує, що такі контракти передбачають права перевірки безпеки та стійкості критичної інфраструктури.

Комісія ядерного регулювання

Комісія ядерного регулювання (NRC) регулює захист комерційних ядерних електростанцій та ядерних реакторів, які використовуються для наукових, випробувальних та тренувальних цілей; регулює захист ядерних матеріалів в медичних, промислових та академічних установах, а також виробництва ядерного палива; транспортування, зберігання та утилізації ядерних матеріалів та відходів. NRC співпрацює, з DHS, DOJ, Міністерством енергетики, Агентством охорони довкілля, Міністерством охорони здоров'я та соціальних послуг та іншими федеральними відомствами, в міру необхідності.

Федеральна комісія зі зв'язку США

Федеральна комісія зі зв'язку, у межах, дозволених законом, користується своїми повноваженнями та знаннями, щоб співпрацювати з DHS і Державним департаментом, а також іншими федеральними департаментами, агентствами та SSA, якщо це необхідно, щоб: (1) визначити пріоритети комунікаційної інфраструктури ; (2) визначити вразливі місця Сектору зв'язку та співпрацювати з промисловістю та іншими зацікавленими сторонами для усунення цих вразливостей; (3) працювати із зацікавленими сторонами, включаючи промисловість, і залучати іноземні уряди та міжнародні організації для підвищення безпеки та стійкості критичної інфраструктури в Секторі зв'язку та сприяти розробці та впровадженню передового досвіду забезпечення безпеки та стійкості критичної комунікаційної інфраструктури.

Федеральні та штатні регуляторні агентства

Деякі сектори координуються федеральними або штатними регуляторними органами, які не є SSA. У цих випадках регуляторні агентства володіють унікальним уявленням про функціонування критичної інфраструктури, яку вони контролюють, і мають певні можливості у сфері критичної інфраструктури, у тому числі:

- сприяння обміну інформацією з власниками та операторами критичної інфраструктури під час реагування на інциденти, а також відновлення після них;
- Заохочення власників і операторів критичної інфраструктури до участі в державно-приватному партнерстві (наприклад, через регіональні коаліції);
- Участь у GCC та координація з SSA ініціатив щодо безпеки та стійкості критичної інфраструктури;
- Забезпечення стійкості сектора через процес розробки політик та нагляду.

Власники та оператори критичної інфраструктури

Власники та оператори критичної інфраструктури в державному та приватному секторах розробляють і впроваджують програми безпеки та стійкості для критичної інфраструктури, що знаходиться під їхнім контролем. Власники та оператори вживають заходів для підтримки планування управління ризиками та інвестицій у забезпечення безпеки як необхідного компонента бізнес-планування. У сучасному середовищі ризиків ці заходи зазвичай включають переоцінку та коригування планів безперервності бізнесу та управління в надзвичайних ситуаціях, посилення стійкості та резервування бізнес-процесів і систем, захист об'єктів від фізичних і кібератак, зниження вразливості до стихійних лих, захист від внутрішніх загроз та посилення координації із зовнішніми організаціями, щоб уникнути або мінімізувати вплив на навколишні громади чи на інших секторальних партнерів.

Для багатьох підприємств приватного сектору рівень інвестицій у безпеку відображає компроміс між ризиком та наслідками, який ґрунтується на двох факторах: (1) те, що відомо про середовище ризику, і (2) економічно обґрунтованими та стійкими факторами, такими як конкурентоспроможність ринку або обмежені ресурси. У контексті першого чинника федеральний уряд має унікальну позицію, щоб допомогти прийняти важливі рішення про інвестиції в інфраструктуру та оперативне планування в усіх секторах. Власники та оператори можуть звертатися до уряду та організацій з обміну інформацією та аналізу, таких як ISAC, як до джерела найкращих методів забезпечення безпеки, а також для індикації атак або природних небезпек, попереджень та оцінки загроз.

Що стосується другого фактора, власники та оператори можуть покладатися на державні установи або брати участь у колективних зусиллях з іншими власниками та операторами для усунення ризиків за межами їх власності або в ситуаціях, коли поточна загроза перевищує здатність підприємства захистити себе або вимагає необґрунтований рівень додаткових інвестицій для зменшення ризику. У цій ситуації партнери державного та приватного секторів на всіх рівнях співпрацюють, щоб забезпечити безпеку та стійкість критичної інфраструктури національного рівня, забезпечити своєчасне попередження та сприяти створенню середовища, в якому власники та оператори критичної інфраструктури можуть виконувати свої обов'язки.

Власники та оператори критичної інфраструктури беруть участь у багатьох заходах із зменшення ризиків, включаючи зусилля з обміну інформацією про кібербезпеку (наприклад, секторальні робочі групи з кібербезпеки, Міжсекторна робоча група з кібербезпеки та Об'єднана робоча група промислових систем контролю), оцінки кіберризиків, навчання, реагування на кіберінциденти та заходи з відновлення після них, а також розробка кіберметрик. Ролі власників і операторів значно відрізняються всередині та між секторами. Деякі сектори мають статутні та нормативні рамки, які впливають на діяльність приватного сектору з забезпечення безпеки в цьому секторі; однак, більшість підприємств керуються вільним акцентом на забезпеченні безпеки та стійкості, або дотримуються рекомендацій найкращих практик, розроблених секторальними організаціями.

У цьому різноманітному ландшафті власники та оператори критичної інфраструктури можуть сприяти забезпеченню безпеки та стійкості національної критичної інфраструктури за допомогою ряду заходів. Ця діяльність може включати, але не обмежуватись: проведенням оцінки ризиків критичної інфраструктури; розумінням залежностей і взаємозалежностей; розробкою та координацією планів реагування на надзвичайні ситуації з відповідними федеральними та SLTT урядовими організаціями; створенням планів і програм безперервності надання послуг, які сприяють виконанню рятувальних функцій під час інциденту; участю у навчаннях, орієнтованих на критичну інфраструктуру разом із партнерами державного та приватного секторів; а також технічною експертизою в сфері забезпечення безпеки та стійкості критичної інфраструктури.

Уряди штатів, місцеві, племінні та територіальні уряди та регіональні організації (**SLTT**)

SLTT реалізують місію внутрішньої безпеки, захищають громадську безпеку та добробут, а також забезпечують надання основних послуг громадам і секторам у межах своєї юрисдикції. Також вони забезпечують безпеку та стійкість критичної інфраструктури, що знаходиться під їхнім контролем, а також інфраструктури, що належить та експлуатується іншими сторонами в межах їхньої юрисдикції. Їхні зусилля мають вирішальне значення для ефективного планування та впровадження заходів забезпечення безпеки та стійкості критичної інфраструктури. Оскільки представники уряду SLTT часто прибувають першими на місце надзвичайної події, вони відіграють ключову роль у проведенні оперативних заходів з відновлення критичної інфраструктури після події. Місцеві, племінні та територіальні уряди також є посередниками для запитів про допомогу від федерального рівня, коли загроза або

надзвичайна ситуація не може бути вирішена на рівні партнерів у публічному та приватному секторах на нижчих юрисдикційних рівнях.

Програми безпеки та стійкості критичної інфраструктури є важливим компонентом стратегій національної безпеки SLTT, зокрема щодо встановлення пріоритетів фінансування та інформування щодо інвестиційних рішень у сфері безпеки та стійкості критичної інфраструктури. Для забезпечення безпеки критичної інфраструктури, її стійкості та продуктивності ці програми мають стосуватися всіх основних елементів Національного плану (якщо це доцільно), включаючи ключові міжюрисдикційні зв'язки забезпечення безпеки та обміну інформацією, а також конкретні заходи з управління ризиками критичної інфраструктури. Ці програми відіграють основну роль у ідентифікації та захисті критичної інфраструктури на регіональному та місцевому рівнях, а також підтримують зусилля DHS та SSA щодо виявлення, забезпечення безпеки та стійкості критичної інфраструктури національного значення.

Уряди штатів і територій

Уряди штатів і територій встановлюють партнерські стосунки, сприяють скоординованому обміну інформацією та забезпечують планування та готовність до забезпечення безпеки та стійкості критичної інфраструктури в межах своєї юрисдикції. Вони є ключовими координаційними центрами, які об'єднують уряди, можливості та ресурси з попередження, захисту, пом'якшення наслідків, реагування та відновлення після інцидентів між місцевими установами, різними секторами та регіональними органами. Штати та території отримують інформацію про критичну інфраструктуру від федерального уряду для підтримки національних і державних програм забезпечення безпеки та стійкості критичної інфраструктури. Крім того, Штати та Території надають інформацію DHS щодо пріоритетів, вимог та потреб у фінансуванні, пов'язаному з критичною інфраструктурою, в рамках процесу надання дотацій або оновлення стратегій національної безпеки.

Штати та території повинні співпрацювати з секторальними агентствами на штатному та територіальному рівнях, щоб підтримувати бачення, місію та цілі Національного плану в секторах (якщо це доцільно), і залучати експертів із відповідної тематики на секторальному рівні.

Програми Штатів та Територій повинні враховувати всі відповідні аспекти забезпечення безпеки та стійкості критичної інфраструктури, використовувати підтримку в рамках програми державної допомоги з безпеки нації, які застосовуються в межах місії з національної безпеки, та відображати пріоритетні заходи в своїх стратегіях, щоб забезпечити ефективне розподілення ресурсів. Ефективні зусилля з безпеки та стійкості критичної інфраструктури на рівні штату та регіону повинні бути інтегровані в загальну структуру програми національної безпеки на штатному чи територіальному рівнях, щоб гарантувати, що зусилля з запобігання, захисту, пом'якшення, реагування та відновлення є синхронізованими та взаємно підтримуючими.

Безпека та стійкість критичної інфраструктури на штатному або територіальному рівні повинні охоплювати всі сектори, які знаходяться в межах юрисдикції, і підтримувати національні, штатні та місцеві пріоритети. Програма також має чітко розглядати унікальні географічні проблеми, включаючи транскордонні питання, а також взаємозалежність між секторами та юрисдикціями в межах цих географічних кордонів.

Органи місцевого самоврядування

Органи місцевого самоврядування надають важливі державні послуги та функції разом із власниками та операторами приватного сектору. У деяких секторах органи місцевого самоврядування через свої відділи з комунальних робіт управляють та володіють критично важливою інфраструктурою, такою як водопостачання, каналізація та електричні мережі. Більшість збоїв або стихійних лих, які впливають на критичну інфраструктуру, починаються і закінчуються як локальні ситуації. Зазвичай місцеві органи влади мають функцію первинного реагування та відновлення після інциденту, доки не стане доступною скоординована підтримка інших джерел, незалежно від того, хто володіє чи керує постраждалим активом, системою чи мережею. У результаті місцеві органи влади є ключовими гравцями в рамках партнерства щодо критичної інфраструктури. Вони сприяють готовності до надзвичайних ситуацій, а також залучають місцевих партнерів, включаючи урядові агенції, власників та операторів критичної інфраструктури, а також приватних громадян у громадах, які вони обслуговують.

Конкретні заходи щодо безпеки та стійкості критичної інфраструктури на штатному, територіальному та місцевому

рівнях можуть включати, але не обмежуватися наступним:

- Виконанням функції координаційного центру та сприяння координації діяльності з забезпесення безпеки, стійкості критичної інфраструктури та реагування на надзвичайні ситуації, координації діяльності щодо програм готовності та підтримки надання ресурсів серед регіональних організацій, партнерів з приватного сектору та громадян;
- Розробка системного підходу до ідентифікації критичної інфраструктури, визначення ризиків, планування заходів мінімізації ризиків, пріоритетних інвестицій у безпеку та проведення тренувань з готовності серед всіх зацікавлених сторін в межах їх юрисдикції;
- Виявлення, впровадження та моніторинг підходу до управління ризиками та вжиття коригувальних дій, якщо необхідно;
- Участь у важливих національних, регіональних і місцевих програмах підвищення ситуаційної обізнаності з метою сприяння належному управлінню та захисту кіберсистем;
- Сприяння обміну інформацією про безпеку, включаючи оцінку загроз, індикатори атак, попередження про загрози та рекомендації, між різними суб'єктами та секторами в їхніх юрисдикціях та поза ними;
- Бути партнером у сфері критичної інфраструктури, включно з секторальними GCC; Координаційною радою штату, місцевими, племінними та територіальними урядами (SLTTGCC); та іншими відповідними механізмами управління та планування у сфері критичної інфраструктури;
- Забезпечення пріоритезації фінансування та ефективного розподілу ресурсів з урахуванням потреб та ефективності;
- Обмін інформацією про інфраструктуру, яка вважається важливою з точки зору національної, штатної, регіональної, місцевої, племінної та/або територіальної точки зору, щоб забезпечити безпеку та відновлення критично важливих державних послуг, об’єктів, комунальних послуг і життєво важливих функцій у межах їх юрисдикції;
- Документування та застосування вивчених уроків отриманих після попередніх заходів з мінімізації наслідків надзвичайних ситуацій, тренувань та реальних подій;
- Взаємодія з партнерами з метою сприяння освіті, навчанню та обізнаності щодо безпеки та стійкості критичної інфраструктури, щоб мотивувати активнішу участь власників та операторів;
- Реагування та забезпечення безпеки, у відповідних випадках, якщо місцевим організаціям бракує ресурсів, необхідних для усунення вразливостей;
- Визначення вимог до науково-дослідних робіт, пов’язаних з критичною інфраструктурою, і доведення їх до DHS;
- Співпраця з штатними та територіальними установами для забезпечення представництва відповідних партнерів з критичної інфраструктури.

Племінні уряди

Ролі та можливості племінних урядів щодо безпеки та стійкості критичної інфраструктури загалом віддзеркалюють ролі та можливості урядів штату та місцевого самоврядування. Племінні уряди несуть відповідальність за охорону здоров’я, добробут і безпеку громадян племені, а також безпеку критичної інфраструктури та безперервність надання основних послуг, що знаходяться під їхньою юрисдикцією. У рамках партнерства щодо критичної інфраструктури племінні уряди координують роботу з федеральними, штатними, місцевими та міжнародними партнерами, щоб досягти синергії у впровадженні систем безпеки та стійкості критичної інфраструктури в межах своєї юрисдикції. Це особливо важливо в контексті обміну інформацією, аналізу та управління ризиками, обізнаності, планування готовності, інвестицій і ініціатив у програми безпеки та стійкості.

Регіональні організації

Регіональне партнерство включає різноманітні ініціативи державного та приватного секторів, які зосереджуються на запобіганні, захисті, пом’якшенні, реагуванні та відновленні в межах визначеної географічної області. Конкретні регіональні ініціативи варіюються за масштабом від організацій, співпраця в галузі захисту та стійкості критичної інфраструктури може включати різні рівні юрисдикцій (наприклад, місцеві, регіональні, штатні) та партнерів з різних галузей економіки в межах однієї держави. В деяких випадках така співпраця може відбуватися між кількома штатами або навіть між різними країнами на міжнародному рівні. У багатьох випадках уряди

штатів також співпрацюють шляхом прийняття міждержавних угод для офіційного оформлення регіонального партнерства. Партнери, які керують або беруть участь в регіональних ініціативах, що включають більші території та сектори, мають можливість використовувати ширшу експертизу та взаємовідносини в цих областях, щоб:

- Сприяти співпраці між партнерами у впровадженні діяльності з оцінки ризиків критичної інфраструктури та управління ними;
- Сприяти освіті та обізнаності щодо безпеки критичної інфраструктури та зусиль щодо стійкості, що здійснюються в їхніх географічних регіонах;
- Брати участь у регіональних навчаннях і навчальних програмах, у тому числі з акцентом на безпеку критичної інфраструктури та співпрацю в сфері стійкості за межами сектору;
- Підтримувати оперативні заходи та постійні дії, що здійснюються відповідно до загроз, з метою підвищення безпеки та стійкості, а також підтримувати заходи з пом'якшення, реагування та відновлення;
- Співпрацювати з SLTT, міжнародними урядами та приватним сектором, якщо це доцільно, для оцінки регіональної та міжсекторальної взаємозалежності критичної інфраструктури, включаючи міркування щодо кібер сфери;
- Здійснювати відповідні регіональні планувальні заходи та укладати відповідні партнерські угоди, що дозволяють здійснювати регіональні заходи з безпеки та стійкості критичної інфраструктури, а також покращеного реагування на надзвичайні ситуації;
- Сприяти обміну інформацією та збору даних між регіональними учасниками та зовнішніми партнерами;
- Обмінюватися інформацією про прогрес і вимоги щодо безпеки та стійкості критичної інфраструктури з DHS, SSA, штатними та місцевими органами влади та іншими партнерами з критичної інфраструктури, якщо це необхідно;
- Брати участь у партнерстві з критичної інфраструктури.

Органи на рівні штату та регіону, такі як ради, комісії, правлінь, та інші структури

Низка правлінь, комісій, органів влади, рад та інших організацій на штатному, місцевому, племінному та регіональному рівнях виконують регулятивні, консультативні, політичні функції або функції нагляду за бізнесом, пов’язані з різними аспектами роботи критичної інфраструктури та безпеки всередині та між секторами. Деякі з цих організацій створюються через повноваження виконавчої чи законодавчої влади на штатному чи місцевому рівні з виборним, призначеним або добровільним членством. Ці групи включають, але не обмежуються, транспортними органами, комунальними комісіями, управлінням водопостачання та каналізації, парковою комісією, житловими органами, органами охорони здоров’я та іншими. Ці організації можуть служити секторальними агентствами на штатному рівні та надавати досвід, допомагати регуляторним органам або сприяти ухваленню інвестиційних рішень, пов’язаних із забезпеченням безпеки критичної інфраструктури та стійкості в межах певної юрисдикції чи географічного регіону.

Консультативні ради

Консультативні ради надають поради, рекомендації та експертизу уряду (наприклад, DHS, SSA та штатними або місцевим установам) щодо політики та діяльності із забезпечення безпеки та стійкості критичної інфраструктури. Ці організації також сприяють зміцненню державно-приватного партнерства та обміну інформацією. Вони часто забезпечують додатковий механізм взаємодії з уже існуючою групою керівників приватного сектору для отримання відгуків про політику та програми із забезпечення безпеки та стійкості критичної інфраструктури, а також для внесення пропозицій щодо підвищення ефективності та результативності конкретних державних програм. Приклади консультативних рад щодо забезпечення безпеки та стійкості критичної інфраструктури включають:

- Консультативну раду з національної безпеки: надає поради та рекомендації Міністру національної безпеки з відповідних питань; члени ради, призначені Секретарем DHS, включають експертів з штатних і місцевих органів влади, служб безпеки, груп фахівців, які першими реагують на надзвичайні ситуації, наукових кіл і приватного сектору.
- Старший консультативний комітет приватного сектору: підкомітет HSAC, який надає раді експертні поради від

лідерів приватного сектора.

- Консультативна рада з національної інфраструктури: надає Президенту через Міністра національної безпеки поради щодо безпеки фізичних і кіберсистем у всіх секторах критичної інфраструктури; включає до 30 членів, призначених Президентом, які обираються з приватного сектору, наукових кіл, а також штатних і місцевих органів влади. Раду було створено (і до неї внесено зміни) відповідно до Указів 13231, 13286, 13385 та 13652.
- Консультативний комітет з телекомунікаційної безпеки: надає Президенту секторальні консультації та експертизу щодо питань і проблем, пов’язаних із впровадженням Політики національної безпеки та готовності до надзвичайних ситуацій щодо забезпечення зв'язку; включає до 30 генеральних директорів компаній, що представляють великих постачальників послуг зв'язку та мереж, а також компанії з інформаційних технологій, фінансів та аерокосмічної галузі.

Наукові та дослідницькі центри

Наукові та дослідницькі спільноти відіграють важливу роль у забезпеченні безпеки та стійкості критичної інфраструктури на національному рівні, у тому числі:

- Створення центрів передового досвіду (тобто партнерства на базі університетів або науково-дослідних центрів, що фінансуються з федерального бюджету) для проведення незалежного аналізу питань безпеки та стійкості критичної інфраструктури;
- Підтримка досліджень, розробки, тестування, оцінки та розгортання технологій безпеки та стійкості;
- Підтримка розробки та впровадження концепцій, архітектур і технічних стратегій, пов’язаних із безпекою та стійкістю критичної інфраструктури;
- Аналіз, розробка та обмін найкращими практиками, пов’язаними з пріоритезацією критичної інфраструктури, зусиллями щодо безпеки та стійкості;
- Дослідження та надання інноваційного погляду на загрози та поведінкові аспекти тероризму та злочинної діяльності;
- Підготовка або розповсюдження інструкцій і описів найкращих практик фізичної та кібербезпеки;
- Розробка та забезпечення відповідного аналізу ризиків усіх небезпек і курсів з управління ризиками для спеціалістів із безпеки та стійкості критичної інфраструктури;
- Створення навчальних планів бакалаврату та магістратури та освітніх програм;
- Проведення досліджень для виявлення нових технологій і аналітичних методів, які можуть бути застосовані партнерами для підтримки зусиль із забезпечення безпеки та стійкості критичної інфраструктури;
- Брати участь у перегляді та підтвердженні підходів до аналізу ризиків та управлінні безпекою та стійкістю критичної інфраструктури;
- Взаємодія та надання ресурсної підтримки місцевим громадам у зусиллях щодо підвищення безпеки та стійкості фізичної та кібернетичної критичної інфраструктури.