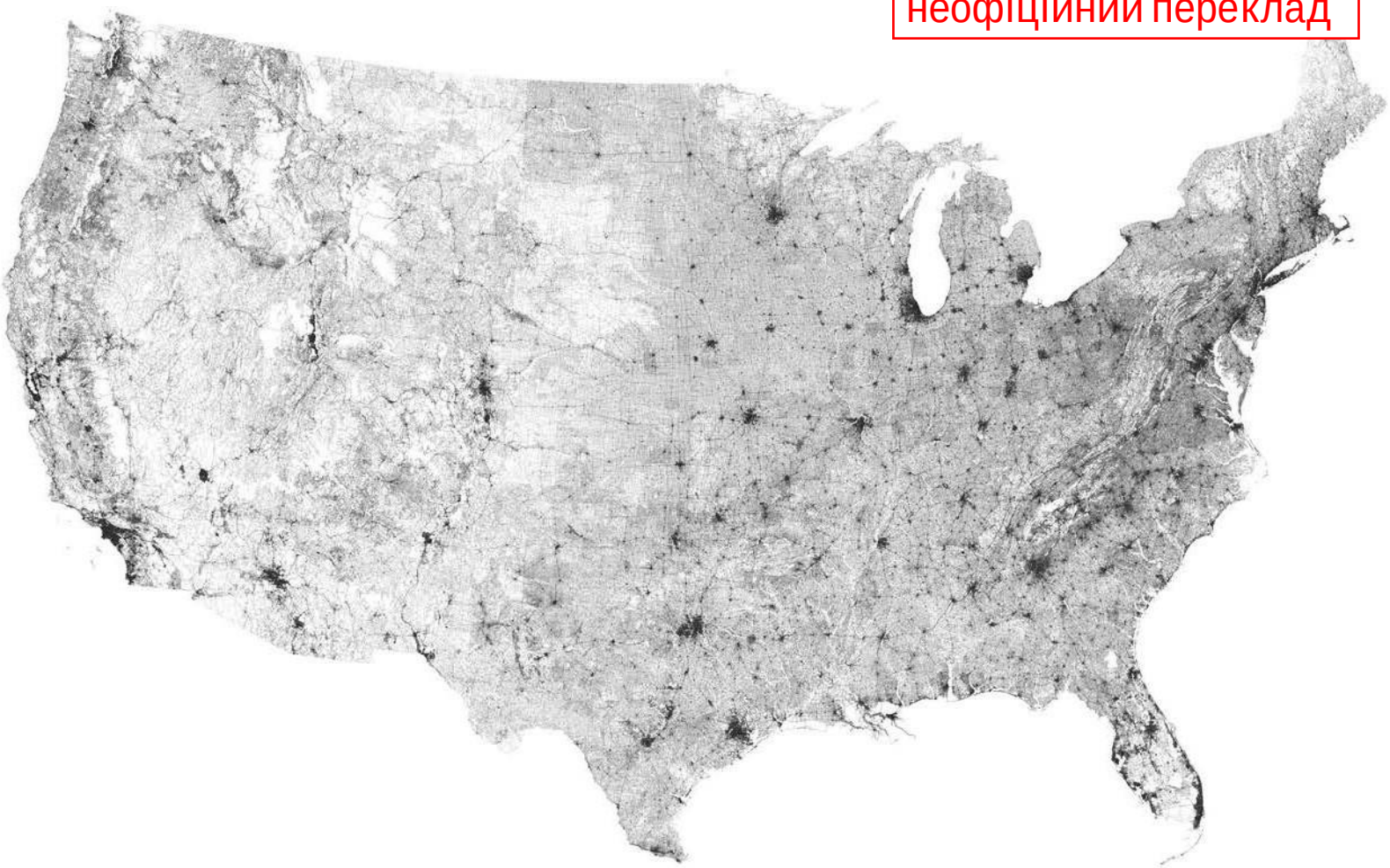
неофіційний переклад



Національна система захисту

Друге видання
*Червень **2016** року*

Цей текст є неофіційним перекладом документу, розміщеного на відкритому інформаційному ресурсі Департаменту національної безпеки Сполучених Штатів Америки (DHS), та може використовуватись лише з інформаційною та науковою метою.
Посилання на офіційний оригінал документа:

https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf

Експлуатаційна структура

Національна система захисту описує спосіб захисту суспільства від терористичних актів, стихійних лих та інших загроз і небезпек. Процеси захисту та керівні принципи, що містяться в цій Національній системі захисту, забезпечують уніфікований підхід, який може бути адаптований до конкретних вимог місії захисту, діяльності місії, юрисдикцій та секторів. Динамічний характер ризиків, з якими стикається держава, вимагає національного підходу, який можна адаптувати до цього мінливого і все більш нестабільного ландшафту.

Ця Концепція описує основні можливості, ролі та обов'язки, а також мережу координаційних структур, які сприяють захисту окремих осіб, громад та нації в цілому. Вона зосереджена на діях, спрямованих на захист від найбільших ризиків для нації у спосіб, що дозволяє процвітати американським інтересам, прагненням і способу життя.

Партнерства на всіх рівнях влади, а також з приватним і некомерційним секторами координують розвиток і забезпечення 11 основних національних спроможностей у сфері захисту. Ці зусилля ґрунтуються на принципах стійкості та масштабованості, врахування ризиків та спільної відповідальності.

Національна система захисту спирається на існуючі координаційні структури для сприяння інтеграції, синхронізації та стійкості в різних юрисдикціях і сферах відповідальності. Координаційні структури, які сприяють виконанню місії захисту, включають оперативні центри; робочі групи правоохоронних органів; координаційні ради секторів критичної інфраструктури, урядові та міжсекторальні координаційні ради; керівні ради; регіональні консорціуми; механізми обміну інформацією, такі як об'єднані центри штатів і великих міських районів; мережі спостереження за станом здоров'я; а також організації державно-приватного партнерства на всіх рівнях.[1] Як національна доктрина, ця Національна система захисту забезпечує об'єднуючий підхід для узгодження діяльності у сфері захисту з різноманітними видами діяльності та координаційними структурами місії.

Ці партнерства можуть охоплювати функціональні сфери, сектори критичної інфраструктури та географічні кордони. Вони дозволяють обмінюватися досвідом та інформацією і є джерелом потенційних ресурсів через угоди про взаємодопомогу та взаємопідтримку. Партнери можуть використовувати Національну систему захисту для інформування та узгодження планування, підготовки, навчань та інших заходів, спрямованих на посилення безпекиокремих осіб, сімей, громад, організацій та юрисдикцій. Структурування планування, тренувань, навчань та операцій на основі спроможностей Національної системи захисту підвищує національну готовність.

Принципи, викладені в цій Національній системі захисту, покликані забезпечити загальну основу для

впровадження захисту як частини національної готовності. Національна система захисту сприяє спільному розумінню місії захисту, що сприяє більш ефективному обміну інформацією, оперативній сумісності та підвищенню ефективності діяльності у сфері захисту на національному рівні.

[1] Ця Нац система узгоджена з відповідними політичними директивами Президента та існуючою доктриною готовності. Наприклад, структурам, викладеним у Національному плані захисту інфраструктури (NIPP) 2013 року: Партнерство заради безпеки та стійкості критичної інфраструктури, який був розроблений на підтримку Президентської політичної директиви (ППД) 21: Безпека та стійкість критичної інфраструктури та Виконавчого наказу 13636: Покращення кібербезпеки критичної інфраструктури, є невід'ємною частиною місії захисту.

Перелік контрагентів

Вступ

Система національної готовності окреслює організований процес, спрямований на досягнення Цілей національної готовності. Система національної готовності об'єднує зусилля у п'яти сферах - запобігання, захист, пом'якшення наслідків, реагування та відновлення - задля створення безпечної та стійкої нації. Національна система захисту, яка є частиною Системи національної готовності, визначає стратегію і доктрину того, як все суспільство будує, підтримує і забезпечує основні можливості захисту, визначені в Цілях національної готовності, в інтегрований спосіб разом з іншими сферами діяльності. Це друге видання Національної системи захисту відображає розуміння і уроки, отримані з реальних інцидентів і з впровадження Національної системи готовності.

Запобігання: Потенціал, необхідний для уникнення, запобігання або припинення загрози або реального терористичного акту. У контексті національної готовності термін "запобігання" стосується запобігання неминучим загрозам.

Захист: Потенціал, необхідний для захисту країни від терористичних актів, а також техногенних і природних катастроф.

Пом'якшення наслідків: Можливості, необхідні для зменшення людських жертв і матеріальних збитків шляхом зменшення впливу катастроф.

Реагування: Можливості, необхідні для порятунку життів, захисту майна та навколишнього середовища, а також задоволення основних людських потреб після того, як стався інцидент.

Відновлення: Можливості, необхідні для надання допомоги громадам, що постраждали від інциденту для ефективного відновлення

Мета та організація Національної системи захисту

Національна система захисту описує, що має робити вся спільнота – від членів громади до вищих керівників уряду – для захисту від актів тероризму, стихійних лих та інших загроз чи небезпек.[2] На підтримку Цілі національної готовності ця Національна система захисту надає керівникам і фахівцям-практикам на всіх рівнях державного управління, приватного і некомерційних секторів та окремим особам рекомендації, що стосуються наступних питань

- Опис основних сил і засобів, необхідних для виконання місії захисту та створення умов для більш безпечної, захищеної та стійкої нації.
- Узгодження ключових ролей та обов'язків для забезпечення можливостей захисту.
- Опис координаційних структур, які дозволяють усім зацікавленим сторонам працювати разом.
- Закладення основи для оперативної координації та планування, що узгоджує зусилля у сфері захисту в межах усієї громади.

[2] Уся громада включає окремих осіб та громади, приватний та некомерційний сектори, релігійні організації та всі рівні управління (місцевий, регіональний/міський, штатний, племінний, територіальний, обласний та федеральний). У Цілі національної готовності громада визначається як "зосередження уваги на створенні умов для участі в заходах з національної готовності ширшого кола учасників з приватного та некомерційного секторів, включаючи неурядові організації та широку громадськість, у поєднанні з усіма рівнями влади, а також на Уряд, що здійснює управління з метою сприяння кращій координації та робочим стосункам. Використовується як синонім до "загальнонаціональний".

- Посилення здатності надавати основні функції і послуги у сфері захисту незалежно відзагрози чи небезпеки.

Національна система захисту побудована як єдиний документ, що забезпечує національну модель міждисциплінарної координації діяльності у сфері захисту. Місія захисту за своєю суттю є децентралізованою. Діяльність у рамках місії захисту здійснюється в різних секторах і юрисдикціях установами, організаціями та громадами, які діють під окремими повноваженнями.

У той час як Національна система готовності наголошує на Національній системі управління інцидентами (NI M S) як основі для організації операцій під час управління інцидентами, можливості захисту створюються, підтримуються і забезпечуються широким спектром організаційних механізмів.[3] Захист часто забезпечується в різних секторах і географічних регіонах, що вимагає децентралізованих, взаємно поінформованих дій. Це робить особливий акцент на обміні інформацією та автономії окремих спільнот, що здійснюють захист.

Принципи, викладені в Національній системі захисту, описують загальну схему, але невизначають національну організаційну структуру. Вони радше окреслюють засоби, за допомогою якихдержава спільно розбудовує спроможності та структуру, за допомогою якої децентралізовані організації, що підтримують місію захисту, спільно реалізують ці спроможності.

Процес і політика, описані в цьому документі, здійснюватимуться відповідно до чинних законів і нормативних актів.

Цільова аудиторія

Хоча Національна система захисту призначена для забезпечення керівництва для всієї спільноти, вона зосереджується на потребах тих, хто бере участь у забезпеченні та застосуванні основних сил і засобів захисту, визначених у Цілях національної готовності. До них належать керівники вищого рівня, які несуть безпосередню відповідальність за реалізацію основних сил і засобів у рамках місії захисту. До таких лідерів належать, зокрема, керівники державних і корпоративних структур, представники правоохоронних органів, служб безпеки, систем охорони здоров'я, пожежної охорони, екстреної медичної допомоги та управління в надзвичайних ситуаціях, власники та оператори об'єктів критичної інфраструктури, а також інші особи, наділені юридичними або законодавчими повноваженнями в сфері діяльності місії.

Фахівці та спільноти з питань захисту надають свої послуги іншим спільнотам та окремим особам, які працюють в інших сферах місій, в інших сферах забезпечення безпеки та іншим афілійованим групам. Ці громади є клієнтами фахівців з питань захисту та ключовим елементом планування і відповідального надання послуг із захисту.

Залучення всієї громади має вирішальне значення для успіху місії, а індивідуальна та громадська готовність є ключовим компонентом. Забезпечуючи рівний доступ до необхідних знань і навичок, ця Національна система захисту має на меті дати можливість усій громаді зробити свій внесок у забезпечення національної готовності та отримати вигоду від неї. Це стосується дітей;[4] людей похилого віку; осіб з інвалідністю та інших осіб з обмеженими можливостями та функціональними потребами;[5] осіб релігійного, расового та етнічного походження; та

[3] Коли сили і засоби захисту та персонал надаються для підтримки операцій з ліквідації інциденту, вони відповідають вимогам HMI та відповідним структурам управління інцидентами для планування та проведення операцій.

[4] Діти потребують унікального набору міркувань щодо основних можливостей, які містяться в цьому документі. Їхні потреби необхідно враховувати в рамках будь-якого інтегрованого планування.

[5] Доступ та функціональні потреби стосується осіб, які можуть мати додаткові потреби до, під час та після інциденту у функціональних сферах, включаючи: підтримання здоров'я, незалежність, комунікацію, транспорт, , послуги, медичну допомогу тощо. Особи, які потребують додаткової допомоги у реагуванні, можуть включати тих, хто має інвалідність, проживає в інституційних установах, є особами похилого віку, дітьми,

представникам різних культур, мають обмежене володіння англійською мовою або не говорять англійською, а також мають проблеми з транспортуванням.

люди з обмеженим знанням англійської мови. Їхній внесок має бути інтегрований у загальнонаціональні зусилля, а їхні потреби мають бути враховані при плануванні та реалізації основних можливостей всієї спільноти.

Засоби

Основні засоби захисту є ключовим компонентом готовності. Структури і засоби, необхідні для досягнення кінцевої мети місії захисту, значною мірою ґрунтуються на існуючій доктрині, планах і діяльності. Місія захисту включає дії зі стримування загроз, зменшення вразливостей або мінімізації наслідків, пов'язаних з інцидентом. Ефективний захист ґрунтується на тісній координації та узгодженні практик у межах усієї спільноти, а також з міжнародними партнерами та організаціями.

Національна структура захисту зосереджується на основних можливостях захисту, які застосовуються як у стабільних умовах, так і під час прийняття ескалаційних рішень та посилених операцій із захисту до або під час інциденту та у відповідь на підвищену загрозу. Стабільні умови вимагають рутинних, звичайних, повсякденних операцій. Посилені умови вимагають посилених операцій, які проводяться під час тимчасових періодів підвищеної загрози, підвищеної готовності або під час періодів реагування на інциденти на підтримку запланованих спеціальних заходів, які потребують додаткової або посиленої діяльності із захисту.[6] Національна система захисту та запобігання вділяє три основні можливості захисту, і очікується, що ці можливості будуть діяти безперебійно, коли це буде потрібно. З цієї причини Національна система захисту тісно пов'язана з Рамковою програмою запобігання. Національна система захисту стосується основних сил і засобів, які сприяють захисту нації на національному рівні.

Основні можливості Захисту дозволяють здійснювати цілий ряд заходів, які включають, але не обмежуються наступним:[7]

- **Прикордонна безпека**. Захист повітряних, наземних, морських портів і кордонів США від нелегальних потоків людей і товарів, а також сприяння законним подорожам і торгівлі.

- **Захист критичної інфраструктури.** Захист фізичних та кібер-елементів критичної інфраструктури. Сюди входять дії, спрямовані на стримування загрози, зменшення вразливості або мінімізацію наслідків, пов'язаних з терористичною атакою, стихійним лихом або техногенною катастрофою. Захист критичної інфраструктури є елементом безпеки та стійкості критичної інфраструктури, як детально описано в Політичній директиві Президента України (ППД) 21: Безпека та стійкість критичної інфраструктури.[8]

---

[6] Це включає в себе підвищену загрозу тероризму, як описано в Національній системі консультування з питань тероризму (National Terrorism Advisory System, або NTAS), і моніторинг усіх загроз, а також підвищену активність щодо нових і постійних ризиків, пов'язаних з можливостями захисту.

[7] Як і всі заходи на підтримку Цілей національної готовності, заходи у сфері "Захисту" повинні узгоджуватися з усіма відповідними законами та політиками, особливо тими, що стосуються приватного життя та громадянських прав і прав людини, такими як Закон про американців з інвалідністю 1990 року, Закон про реабілітацію 1973 року та Закон про громадянські права 1964 року.

[8] Критична інфраструктура, як визначено в ППР-21, включає системи та активи, фізичні або віртуальні, які є життєво важливими, що непрацездатність або руйнування таких об'єктів може мати негативний вплив на безпеку, економіку, громадську безпеку чи здоров'я, навколишнє середовище або будь-яку комбінацію цих аспектів. Безпека та стійкість критичної інфраструктури охоплює такі сектори, як хімічна промисловість; комерційні об'єкти; комунікації; критично важливе виробництво; греблі; оборонна промислова база; аварійно-рятувальні служби; енергетика; фінансові послуги; харчова промисловість та сільське господарство; урядові установи; охорона здоров'я; інформаційні технології; ядерні реактори, матеріали та відходи; транспортні системи; а також системи водопостачання та

- **Кібербезпека**. Захист кіберсередовища та інфраструктури від несанкціонованого або зловмисного доступу, використання або експлуатації при одночасному захисті приватності, громадянських прав свобод.

- **Захист від загроз, пов'язаних зі зброєю масового знищення (ЗМЗ).** Захист нації від загроз, пов'язаних зі зброєю масового знищення та пов'язаними з нею матеріалами і технологіями, включно з їх зловмисним придбанням, переміщенням і використанням на території Сполучених Штатів.

- **Захист сільського господарства та продовольства**. Захист мереж і систем сільського господарства та харчової промисловості від усіх видів загроз та інцидентів.[9]

- **Безпека здоров'я.** Забезпечення готовності нації та її населення до загроз здоров'ю або інцидентів з потенційно негативними наслідками для здоров'я, захисту від них та стійкості до них.

- **Імміграційна безпека.** Захист нації від нелегальної імміграції за допомогою ефективних і дієвих імміграційних систем і процесів, які поважають права людини і громадянина.

- **Морська безпека**. Захист морської інфраструктури, ресурсів і морської транспортної системи США від тероризму та інших загроз і небезпек, а також захист батьківщини від нападу з моря, з дотриманням громадянських прав, повагою до приватного життя і захисту цивільних прав. і надаючи можливість законним мандрівникам і товарам ефективно пересуватися без побоювання заподіяння шкоди або значних перешкод.

- **Охорона вищого керівництва та спеціальних заходів.** Захист ключового керівництва від ворожих дій з боку терористів та інших зловмисників, а також забезпечення безпеки під час заходів національного значення.[10]

- **Транспортна безпека.** Захист морської інфраструктури, ресурсів і морської транспортної системи США від тероризму та інших загроз і небезпек, а також захист батьківщини від нападу з моря, з одночасним дотриманням громадянських прав, повагою до недоторканності приватного життя і захищених громадянських свобод, а також наданням можливості законним мандрівникам і товарам ефективно пересуватися без побоювання заподіяння шкоди або значних перебоїв.

Керівні принципи

Наступні принципи керують розробкою та підтримкою основних можливостей системи захисту:

1. **Стійкість та масштабованість.** Ефективне надання основних можливостей для захисту мінімізує ризики від усіх загроз і небезпек:

   a. **Стійкість.** Стійкість - це здатність готуватися та адаптуватися до мінливих умов, а також витримувати та швидко відновлюватися після збоїв.[11] Її можна підвищити шляхом забезпечення

[9] Основні сили та засоби захисту відповідають політиці, визначеній у Директиві Президента з питань внутрішньої безпеки (HSPD) 9: Оборона сільського господарства та продовольства США, що включає визначення та пріоритезацію критично важливої інфраструктури сектору; розвиток обізнаності та можливостей раннього попередження; зменшення вразливостей; та вдосконалення процедур перевірки .

[10] Ключовими лідерами вважаються чинні та колишні президенти, віце-президенти, члени їхніх сімей та інші особи, яким надано такий захист відповідно до Розділу 18 Зводу законів США, розділів 3056 і 3056A. Події національного значення поділяються на дві категорії: Події національної особливої безпеки (НОПБ), як визначено в Розділі 18, Розділі 3056 Зводу законів США і додатково роз'яснено в ППД-22, і події, які офіційно оцінюються в рамках процесу оцінки спеціальних подій (SEAR) міжвідомчою Робочою групою з питань спеціальних подій (РГСП), створеною міжвідомчою

робочою групою з питань спеціальних подій (РГСП) МЗС, ФБР, УСБ і ФСБ,на основі інформації, наданої федеральними, штатними та місцевими правоохоронними органами.

[11] Див. Білий дім, PPD-21: Безпека та стійкість критичної інфраструктури (Вашингтон, округ Колумбія,Білий дім, 2013).

основних можливостей для захисту і включати в себе широкий спектр заходів, включаючи вдосконалення протоколів безпеки; зміцнення об'єктів; прийняття резервування; включення стійкості до небезпек в проектування і технічне обслуговування об'єктів; ініціювання активних або пасивних контрзаходів; встановлення систем безпеки; використання "самовідновлювальних" технологій; сприяння програмам гарантій для персоналу; впровадження заходів кібербезпеки; навчання і тренінги; планування безперервності і операцій; а також заходи з відновлення і відбудови.[12]

b. **Масштабованість**. можливості Масштабованості призначені для задоволення непередбачуваних, мінливих потреб різного географічного масштабу, складності та інтенсивності. Масштабованість дозволяє засобам захисту функціонувати в різних юрисдикціях і секторах, розширюючись відповідно до динамічних вимог місії.

2. **Ризик-орієнтована культура**. Культура ризик-орієнтованості підтримує можливості захисту і вимагає:

   a. **Пильність і ситуаційну обізнаність** через національну систему моніторингу нових загроз і небезпек та ризиків.

   b. **Обмін інформацією та прийняття рішень щодо ризиків** через координаційні механізми, які дозволяють надавати відповідну інформацію зацікавленим сторонам, які будуть використовувати її для аналізу та дій.

3. **Спільна відповідальність**. Захист є найбільш ефективним як спільна відповідальність, що впроваджується через:

   a. **Зацікавлених партнерств** для обміну інформацією, ідеями, підходами та ефективними практиками; сприяння плануванню забезпечення безпеки та розподілу ресурсів; створення ефективних координаційних структур між партнерами; підвищення обізнаності громадськості.

   b. Інтегровані **процеси** в усіх органах влади та партнерів приватного та некомерційного секторів для більш ефективного досягнення спільного бачення безпечної та захищеної нації.

Основа ризиків

Ризик - це потенційна можливість небажаного результату внаслідок інциденту, події або явища, що визначається ймовірністю інциденту та пов'язаними з ним наслідками.[13] Він оцінюється на основі відповідних загроз і небезпек, вразливостей і наслідків. У сфері діяльності місії "Захист" акцент на оцінці ризиків сприяє розумінню того, що потрібно захищати, і гарантує, що безпека, стійкість будуть визначальними при прийнятті рішень.

Результати Стратегічної національної оцінки ризиків (СНОР), що містяться у другому виданні Цілей національної готовності, вказують на те, що широкий спектр загроз і небезпек продовжує становити значний ризик для країни, підтверджуючи необхідність впровадження підходу до планування готовності, що враховує всі небезпеки ібазується на можливостях. Результати, що містяться в Цілях, включають

- Природні небезпеки, включаючи урагани, землетруси, торнадо, посухи, лісові пожежі, зимові бурі та повені, становлять значний ризик по всій країні. Зміна клімату може призвести до посилення наслідків погодних небезпек.
- Вірулентний штам пандемічного грипу може вбити сотні тисяч американців, зачепити мільйони інших і призвести до економічних втрат. Інші інфекційні захворювання людей і тварин, у тому числі ті, що ще не виявлені, можуть становити значні ризики.

[12] Напрями місії "Захист" і "Пом'якшення наслідків" працюють разом задля підвищення стійкості. Пояснення відмінностей і подібностей між захистом і пом'якшенням див. у розділі "Основні можливості" цього документа .

[13] Керівний комітет з питань ризиків Міністерства внутрішньої безпеки, *DHS Risk Lexicon*, Вашингтон, округ Колумбія, 2011.

- Техногенні та аварійні небезпеки, такі як збої в роботі транспортної системи, прориви дамб, викиди хімічних речовин, можуть призвести до численних людських жертв та серйозних економічних збитків. впливів. Крім того, ці небезпеки можуть посилюватися через старіння інфраструктури.

- Терористичні організації можуть намагатися придбати, створити та використати зброю масового знищення. Звичайні терористичні атаки, що використовують фізичні загрози, такі як вибухівка та збройні напади, становлять постійний ризик для нації.

- Зловмисна кібердіяльність може мати катастрофічні наслідки, які, в свою чергу, можуть призвести до інших небезпек, таких як збої в електромережах або збої у фінансовій системі. Ці каскадні небезпеки збільшують потенційний вплив кіберінцидентів. Загрози кібербезпеці мають зростаючу складність, а також взаємопов'язані із системами критичної інфраструктури, що ставить під загрозу безпеку, економіку та громадську безпеку і здоров'я країни.

- Деякі інциденти, такі як вибухи або землетруси, зазвичай спричиняють більш локальні наслідки. в той час як інші інциденти, такі як людські пандемії, можуть спричинити розосереджені впливи по всій країні, створюючи таким чином різні типи впливів, які повинні враховувати фахівці з планування щодо готовності.

На додаток до цих небезпек, зміна клімату може негативно вплинути на кількість загроз і небезпек. Підвищення рівня моря, дедалі потужніші шторми та сильніші зливи вже призводять до збільшення ризику повеней. Посухи та лісові пожежі стають все частішими і сильнішими в деяких регіонах країни.

Результати SNRA, що містяться в Цілях, зосереджені на непередбачуваних подіях, які, як правило, визначаються початковою та кінцевою точками. Ці результати не стосуються низки штатних ризиків, таких як порушення перетину кордонів і правил торгівлі, нелегальна імміграція, незаконний обіг наркотиків та порушення прав інтелектуальної власності, які становлять значну частину штатного захисту. Визнання штатних і постійних обов'язків у сфері захисту, а також результати SNRA, що містяться в Цілях, супроводжували розробку Національної системи захисту і мають бути покладені в основу аналізу на рівні громади. Крім того, вся громада повинна бути здатна надавати основні функції та послуги під час реальної загрози або інциденту, щоб забезпечити надання основних можливостей для всіх сфер діяльності місії.

Ролі та обов'язки

До виконання місії захисту залучено багато осіб, організацій та установ. Партнери у сфері захисту мають різні повноваження, можливості та ресурси, які, будучи узгодженими з урахуванням ризиків, створюють основу для захисту на національному рівні.

Захист здійснюється за різних умов. Ролі та обов'язки партнерів у сфері захисту відображають децентралізовану модель координації та незалежних дій, яка є складовою національного підходу до захисту.

Особи, сім'ї та домогосподарства

Громади поділяють відповідальність за розуміння загроз і небезпек у своїй місцевості. Окремі особи, сім'ї та домогосподарства повинні вживати захисних заходів з урахуванням ризиків, ґрунтуючись на цих знаннях. Особи, сім'ї та домогосподарства отримують інформацію про потенційні загрози та небезпеки з таких джерел, як засоби масової інформації, місцеві служби з надзвичайних ситуацій, системи оповіщення та інформування населення, просвітницькі кампанії в громадах та механізми обміну інформацією.

Спільноти

Спільноти - це об'єднані групи, які мають спільні цілі, цінності чи завдання і можуть діяти незалежно від географічних кордонів чи юрисдикції. Спільноти об'єднують людей у різний спосіб із

різних причин. Вони мають можливість просувати та реалізовувати основні можливості в рамках місії захисту, а також обмінюватися інформацією та ефективними практиками. Спільноти можуть включати релігійні організації; сусідські партнерства; людей з обмеженими можливостями та функціональними потребами, наприклад, людей з інвалідністю; людей з різних релігійних, расових та етнічних спільнот; онлайн-спільноти; коаліції з питань конкретних небезпек або охорони здоров'я; та професійні асоціації. Спільноти відіграють важливу роль у розробці та забезпеченні можливостей захисту, часто беручи на себе ініціативу у встановленні стандартів захисту, укладанні угод про взаємодопомогу та створенні механізмів для обміну інформацією. З цієї причини громади відіграють центральну роль у розробці планів захисту, а також у визначенні та впровадженні рішень для вирішення проблем у сфері захисту. Оскільки ризики перетинають географічні та юрисдикційні кордони, спільноти є важливими партнерами для розуміння того, як управляти складними питаннями захисту в різних сферах відповідальності.

Підприємства приватного сектору

До суб'єктів приватного сектору належать підприємства, промисловість, приватні школи та університети. Особлива увага при захисті приділяється власникам та операторам інфраструктури країни. Власники та оператори інфраструктури як приватного, так і державного сектору розробляють та впроваджують захисні заходи, що базуються на програмах з оцінки ризиків та стратегії забезпечення стійкості інфраструктури, а також пов'язаної з нею інформації та операцій, що перебувають під їхнім контролем.[14] Власники та оператори підтримують ситуаційну обізнаність, постійно вживають заходів для нарощування потенціалу захисту та здійснюють інвестиції в безпеку та стійкість, що є необхідними компонентами ведення бізнесу та планування безперервності надання послуг. Суб'єкти приватного сектору працюють разом із суб'єктами державного сектору через створені галузеві координаційні органи, підпорядковані відповідним законодавчим органам, з метою обміну інформацією та спільного реагування на суспільні ризики. Суб'єкти приватного сектору також відіграють центральну роль у розробці регуляторних заходів, спрямованих на управління ризиками в усіх секторах інфраструктури.

Міжнародне співробітництво

Хоча національна система захисту зосереджені здебільшого на внутрішній діяльності, можливості захисту часто взаємопов'язані на глобальному рівні. Тому зусилля у сфері захисту з іноземними державами, регіональними та міжнародними організаціями зосереджені на налагодженні партнерства з міжнародними зацікавленими сторонами, виконанні угод та інструментів, які впливають на захист, а також на вирішенні міжсекторальних і глобальних питань. Міжнародне співробітництво має важливе значення для розвитку та реалізації основних можливостей місії захисту. Діяльність у сфері захисту з міжнародними партнерами вимагає координації з Державним департаментом США та, за необхідності, з іншими державними органами на місцевому, регіональному/міському, штатному, племінному, територіальному, острівному,[15] та федеральному рівнях.

Неурядові організації

НУО заохочуються до створення або участі в регіональних та громадських партнерствах з питань готовності до надзвичайних ситуацій з метою вироблення спільного розумінняризиків та способів їх подолання в рамках їхніх із захисту. Там, де це доречно, НУО та релігійні організації

[14] Для цілей Національної системи захисту "власники та оператори" включають власників та операторів як приватних підприємств та інфраструктури, так і інфраструктури, що перебуває у державній власності (наприклад, громадські роботи та комунальні послуги).

[15] Для цілей Національної системи захисту острівні території включають Гуам, Співдружність Британських Північні Маріанські острови, Американське Самоа та Віргінські острови США.

також сприяють виконанню місії захисту, надаючи допомогу всім членам громади, окремим особам і домогосподарствам отримувати інформацію та ресурси з питань захисту.

Місцеві органи влади

Місцеві органи влади несуть відповідальність за громадську безпеку, захист, здоров'я та добробут населення на території своєї юрисдикції. Місцеві органи влади сприяють координації поточних планів захисту та реалізації основних можливостей, а також взаємодії та обміну інформацією з суб'єктами приватного сектору, власниками та операторами інфраструктури, іншими юрисдикціями та регіональними утвореннями. Місцеві органи влади також вирішують географічні питання пов’язані із захистом,включаючи транскордонні проблеми, залежність і взаємозалежність між установами та підприємствами, а також, за необхідності, укладають угоди для міжюрисдикційної та державно-приватної координації. Місцеві органи влади також несуть відповідальність за те, щоб усі громадяни отримували своєчасну інформацію в різних доступних форматах.

Уряди штатів, племен, територій та острівних територій

Уряди штатів, племен, територій та острівних територій відповідають за виконання місії захисту, захист суспільного добробуту та забезпечення безперебійного надання основних послуг та інформації для захисту громадського здоров'я і безпеки громадам та об'єктам інфраструктури в межах їхньої юрисдикції. Вони вирішують транскордонні питання та організаційні взаємозалежності, а також укладають координаційні угоди. Ці уряди відіграють невід'ємну роль як канал координації діяльності федеральних агентств та місцевих органів влади.

Федеральний уряд

Президент очолює зусилля федерального уряду у сфері захисту, спрямовані на підготовку країни до всіх небезпек, включаючи стихійні лиха, терористичні акти та інші надзвичайні ситуації. Федеральний уряд забезпечує лідерство, координацію та інтеграцію для розвитку і забезпечення силами і засобами захисту. Федеральні міністерства і відомства забезпечують виконання національної політики і здійснюють законодавчі та регуляторні повноваження щодо широкого спектру програм захисту і надають допомогу в ряді сфер, включаючи фінансування, дослідження, координація, безперервність операцій і планування, нагляд, реалізацію і правозастосування.

Для виконання місії захисту всі федеральні відомства та агентства співпрацюють між собою, а також з місцевими, регіональними/міськими, штатними, племінними, територіальними, острівними органами влади, федеральним урядом, членами громад, приватним та некомерційним сектором. Федеральний уряд, працюючи з усіма цими партнерами, робить свій внесок у розвиток і надання основних можливостей шляхом впровадження національних законів, встановлення правил, керівних принципів і стандартів, покликаних захистити громадськість, забезпечуючи при цьому вільний потік комерції та захист приватного життя, громадянських прав і свобод. Федеральний уряд надає інтегровані можливості та ресурси для забезпечення громадської безпеки на випадок потенційних або фактичних інцидентів, що потребують скоординованого реагування на федеральному рівні.

Федеральні відомства та агентства мають різні обов'язки щодо захисту. Федеральний міжвідомчий оперативний план у сфері захисту (FIOP) містить детальний опис того, як федеральні відомства та агенції беруть участь у забезпеченні основних сил і засобів та роблять свій внесок у їхню діяльність.[16]

- Міністерство національної безпеки[17]
- Департамент сільського господарства
- Департамент торгівлі
- Міністерство оборони
- Міністерство енергетики
- Міністерство охорони здоров'я та соціальних послуг[18]
- Міністерство внутрішніх справ

[16] FIOPs є обов'язковим компонентом Національної системи готовності. Його мета полягає в тому, щоб забезпечити керівництво федерального уряду з метою успішного впровадження системи захисту. План дій щодо захисту розглядається далі в розділі "Оперативне планування" цього документу.

[17] За розпорядженням Президента, Міністр національної безпеки є головною федеральною посадовою особою, відповідальною за управління національними інцидентами. Відповідно до Закону про національну безпеку від 2002 року, міністр є координатором з питань природних і техногенних криз та планування на випадок надзвичайних ситуацій. Основними завданнями МНБ є запобігання терористичним атакам на території Сполучених Штатів; зменшення вразливості Сполучених Штатів до тероризму; мінімізація шкоди та допомога у відновленні після терористичних атак, що сталися на території Сполучених Штатів; виконання всіх функцій організацій, переданих Міністерству, в тому числі шляхом виконання функцій координатора з питань природних і техногенних криз та планування на випадок надзвичайних ситуацій. З метою захисту від терористичних атак, великих катастроф та інших надзвичайних ситуацій, пом'якшення їх наслідків і, за необхідності, запобігання їм, Міністр відповідає за визначення стратегічних пріоритетів і координацію внутрішніх зусиль міністерств і відомств виконавчої влади щодо забезпечення готовності до всіх видів небезпек, консультуючись з місцевими органами влади, органами влади штатів, племен і територій, неурядовими організаціями, партнерами з приватного сектору та широкою громадськістю (за винятком тих видів діяльності, які можуть порушувати повноваження генерального прокурора або директора ФБР). Національний оперативний центр - головний оперативний центр DHS.

[18] Закон про готовність до пандемії та всіх небезпек наказує Міністру охорони здоров'я та соціальних служб розробити Національне стратегія безпеки охорони здоров'я з акцентом на здоров'я людини. На додаток до департаментів і відомств, перелічених тут за їхню унікальну роль у сфері охорони здоров'я людей, тварин і довкілля, Національну стратегію охорони здоров'я підтримують Міністерства національної безпеки, оборони, освіти, юстиції, праці, державного департаменту і транспорту, Федеральна комісія зв'язку, Управління кадрового менеджменту та Адміністрація Президента.

- Міністерство юстиції[19]
- Державний департамент США[20]
- Міністерство транспорту
- Міністерство фінансів
- Агентство з охорони навколишнього середовища
- Адміністрація загальних служб
- Офіс директора Національної розвідки.[21]

Повноваження місії захисту визначаються місцевими, регіональними/міськими, штатними, племінними, територіальними, острівними законами, нормативними актами, постановами та іншими директивами, що мають законодавчу силу, а також федеральними законами. Директиви та нормативні акти національної політики спрямовують федеральні відомства до здійснення заходів із захисту в межах кількох секторів критично важливої інфраструктури та між ними. Національна система захисту не змінює і не замінює

жодних існуючих обов'язків і повноважень, визначених законами, директивами або політиками. Закон зобов'язує федеральні відомства та агентства забезпечувати доступ до комунікацій, фізичний доступ та програмний доступ, щоб усі громадяни мали рівний доступ та рівні можливості.

---

[19] Генеральний прокурор несе відповідальність за кримінальні розслідування терористичних актів або терористичних загроз, скоєних окремими особами або групами осіб на території Сполучених Штатів, або спрямованих проти громадян Сполучених Штатів чи установ за кордоном, якщо такі акти підпадають під федеральну кримінальну юрисдикцію Сполучених Штатів, а також за пов'язану з ними діяльність зі збору розвідувальної інформації на території Сполучених Штатів, відповідно до Закону про національну безпеку від 1947 року (зі змінами) та інших чинних законів, Виконавчого наказу № 12333 (зі змінами), а також процедур, схвалених генеральним прокурором на підставі цього виконавчого наказу. Генеральний прокурор, який зазвичай діє через директора ФБР, також несе головну відповідальність за пошук і знешкодження ЗМЗ на території США. Генеральний прокурор, зазвичай діючи через Директора ФБР, очолює і координує оперативне реагування правоохоронних органів, правоохоронну діяльність на місцях, а також пов'язану з нею слідчу і відповідну розвідувальну діяльність, пов'язану з терористичними загрозами та інцидентами в США, на їх території, в територіальних водах або на суднах під прапором США. Це включає координацію діяльності правоохоронних органів з виявлення, запобігання, упередження та припинення терористичних загроз. Під час безпосередньої загрози ФБР очолює і координує оперативне реагування правоохоронних органів, а також правоохоронну і слідчу діяльність на місці події через Директора ФБР на місці події (OSC). Після терористичної загрози або фактичного інциденту, що підпадає під кримінальну юрисдикцію Сполучених Штатів, всі можливості Сполучених Штатів, відповідно до законодавства США та діяльності інших федеральних департаментів і відомств щодо захисту національної безпеки, спрямовуються на допомогу Генеральному прокурору у встановленні осіб, які вчинили злочин, та притягненні їх до кримінальної відповідальності. ОБС ФБР зберігає повноваження вживати відповідних правоохоронних заходів у будь-який час під час реагування, включаючи звільнення заручників, тактичне реагування, забезпечення безпеки і знешкодження бомб, а також контролювати місця злочинів, у тому числі пов'язаних зі зброєю масового знищення, їхню безпеку і роботу з доказами на всіх етапах реагування. ФБР керує превентивним реагуванням і контр терористичними операціями через Центр стратегічних інформаційних операцій і 56 об'єднаних оперативних центрів місцевих відділень ФБР. Для отримання додаткової інформації див. Рамкову програму запобігання або Превентивну програму запобігання FIOP.

[20] У рамках повсякденної дипломатичної діяльності від імені уряду США Державний департамент відповідає за встановлення та підтримку міжнародних партнерських відносин, які мають важливе значення для розвитку та забезпечення основних сил і засобів у сфері дії місії "Захист".

[21] Директор національної розвідки очолює розвідувальне співтовариство, виконує функції головного радника Президента з питань розвідки, пов'язаних з національною безпекою, а також здійснює нагляд і керівництво реалізацією Національної розвідувальної програми. Розвідувальне співтовариство, що складається з федерального уряду, функціонує відповідно до законів, виконавчих наказів, нормативних актів і політики для підтримки місій уряду США, пов'язаних з національною безпекою. На додаток до елементів розвідувального співтовариства, що виконують конкретні завдання з національної безпеки, Офіс директора національної розвідки утримує низку місій і центрів підтримки, які надають унікальні можливості, що в сукупності сприяють забезпеченню всіх основних сил і засобів для захисту.

Коефіцієнт капіталізації

Ціль національної готовності визначає основні сили і засоби та завдання для кожної з п'яти сфер діяльності місії. У Таблиці 1 наведено перелік основних сил і засобів за сферами діяльності місії та висвітлено
взаємозв'язок сил і засобів захисту з усією системою національної готовності. Більшість з цих основних сил і засобів існують і використовуються щодня для забезпечення сталого захисту. Підхід до подальшого розвитку і надання цих основних сил і засобів буде відрізнятися в залежності від району проведення місії.

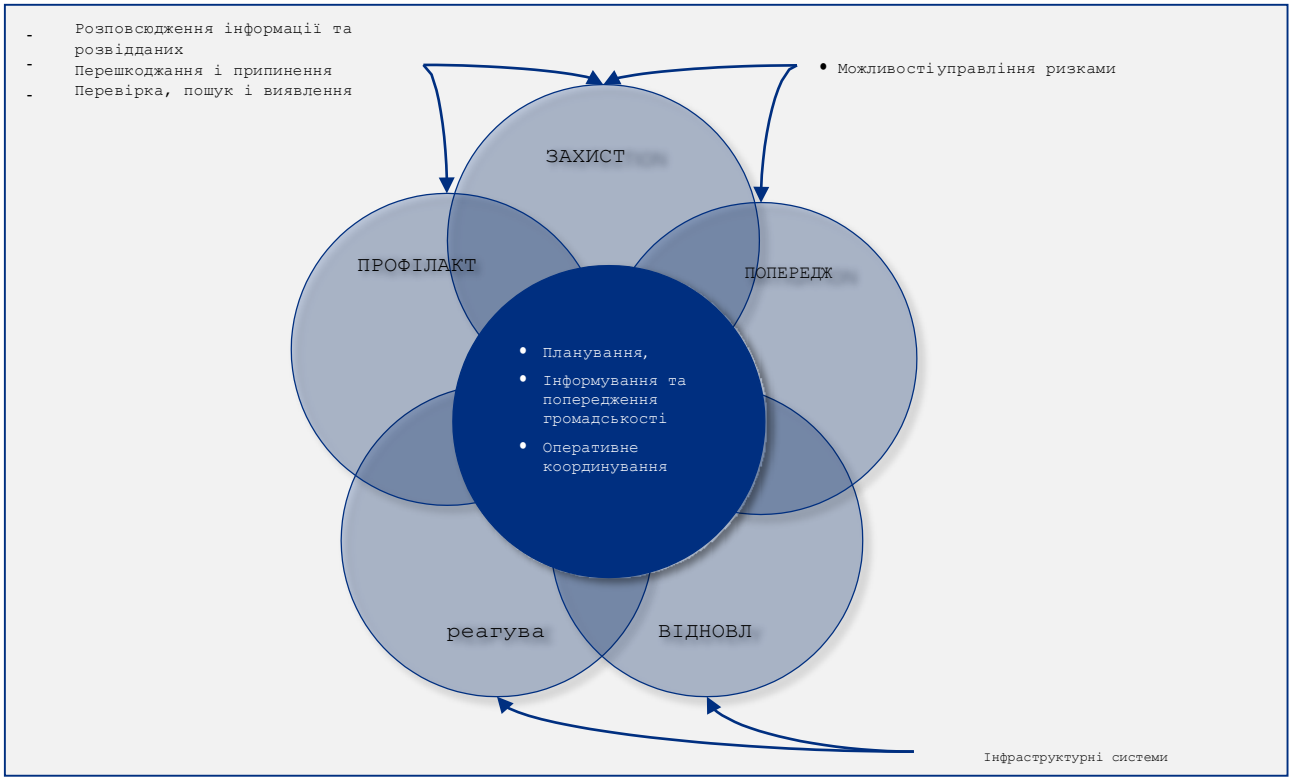
Таблиця 1: Основні спроможності за напрямками місії[22]

<table>
<tr><th>Профілактика</th><th>Захист</th><th>Пом'якшення</th><th>Реагування</th><th>Відновлення</th></tr>
<tr><td colspan="5">Планування</td></tr>
<tr><td colspan="5">Інформування та оповіщення громадськості</td></tr>
<tr><td colspan="5">Оперативна координація</td></tr>
<tr><td colspan="2">Обмін інформацією та розвідданими</td><td rowspan="4">Стійкість громади
Довгострокове зменшення вразливостей
Оцінка ризиківта стійкості до стихійних лих
Ідентифікація загроз та небезпек</td><td colspan="2">Інфраструктурні системи</td></tr>
<tr><td colspan="2">Заборона та підрив</td><td rowspan="3">Критично важливі перевезення
Екологічне реагування/охорона здоров'я та безпека
Послуги з управління летальними випадками
Управління пожежами та гасіння пожеж
Послуги масового догляду
Логістика та управління ланцюгами поставок
Послуги масового догляду
Масові пошуково-рятувальніоперації
Безпека, охорона та забезпечення правопорядку на місці подій
Оперативні Комунікації
Громадське здоров'я, охорона здоров'я та екстрена медична допомога
Оцінка ситуації</td><td rowspan="3">Відновлення економіки
Охорона здоров'я та соціальні послуги
Житло
Природні та культурні ресурси</td></tr>
<tr><td colspan="2">Перевірка, пошук і виявлення</td></tr>
<tr><td>Криміналістика та атрибуція</td><td>Контроль доступу та ідентифікація особи
Кібербезпека
Заходи фізичного захисту
Управління ризиками для програм та заходів захисту
Цілісність та безпека ланцюга постачання</td></tr>
</table>

[22] Ціль національної готовності окреслює основні спроможності для кожної сфери діяльності місії.

Національна система

Ціль національної готовності визначає 11 основних спроможностей для місії "Захист". Три з них (планування, інформування та попередження громадськості, оперативна координація) охоплюють усі сфери діяльності місії. Крім того, сфери діяльності місії із захисту і запобігання мають три спільні ключові спроможності: Обмін інформацією та розвідданими; Перешкоджання і припинення протиправної діяльності; Перевірка, пошук і виявлення. Наскрізні спроможності між цими сферами діяльності створюють можливості для інтеграції та спільного розвитку сил і засобів. Сфера місії "Запобігання" зосереджена на розвідувальній, правоохоронній діяльності та діяльності з національної безпеки, що запобігає здійсненню зловмисником терористичної атаки на території Сполучених Штатів. Захист і запобігання мають спільну мету. Вони складаються з більшої кількості спільних



елементів і покладаються на багато однакових базових можливостей. Усі процеси захисту та запобігання, описані в цій концепції, розроблені таким чином, щоб діяти одночасно та доповнювати один одного. Захист і запобігання мають спільні можливості, безпосередньо пов'язані з ризиками управління. У сфері захисту ця спроможність полягає в управлінні ризиками для програм і заходів у сфері захисту. У сфері пом'якшення наслідків управління ризиками ґрунтується на довгостроковому зменшенні вразливостей, оцінці ризиків і стійкості до катастроф, а також на виявленні загроз і небезпек. Напрями місії "Захист" і "Пом'якшення наслідків" координуються через процес управління ризиками, оскільки вони виявляють загрози і небезпеки та працюють над зменшенням вразливостей. Рисунок 1 - це спрощена схема, яка концептуально ілюструє взаємозв'язок між усіма напрямами місії. На малюнку особлива увага приділяється зв'язкам і спільним або спорідненим основним можливостям, які узгоджують зусилля в контексті захисту і запобігання, а також захисту і пом'якшення наслідків. Крім того, захист пов'язаний з реагуванням і відновленням за допомогою різних основних сил і засобів, таких як інфраструктурні системи і відповідні координаційні структури.

Рисунок 1: З'єднання основних можливостей

У сукупності, основні сили і засоби місії "Захист" створюють основу для безпечної і стійкої нації, яка захищена від тероризму та інших загроз таким чином, що дозволяє процвітати американським інтересам, прагненням і способу життя.

Ціль національної готовності встановлює завдання для кожної з основних спроможностей місії захисту. Цільові показники були використані для визначення критично важливих завдань, перелічених на наступних сторінках. Критичні завдання є специфічними для місії захисту і можуть бути використані для визначення індивідуальних цілей і завдань.

Критично важливі завдання, пов'язані з основними можливостями захисту не є завданнями для якоїсь однієї юрисдикції або відомства; скоріше, їх виконання вимагає національнихзусиль за участю всієї спільноти.

Наскрізні основні спроможності

Наступні три основні спроможності охоплюють усі п'ять сфер діяльності місії: Планування, інформування та попередження громадськості і оперативне координування.

Планування

Опис: Проведення систематичного процесу із залученням усієї спільноти, за необхідності, до розробки підходів стратегічного, оперативного та/або тактичного рівнів для досягнення визначених цілей. Планування включає розробку та підтримку міждисциплінарних планів, які забезпечують спільне керівництво всіма видами діяльності місії з захисту.

Критичні завдання:

- Ініціювати процес планування, який ґрунтується на існуючих планах в рамках Національної системи планування.
- Створювати партнерства, які сприятимуть скоординованому обміну інформацією між ними для підтримки захисту критично важливої інфраструктури в межах однієї або декількох юрисдикцій та секторів.
- Ідентифікувати та визначити пріоритети критично важливої інфраструктури, а також пріоритети щодо управління ризиками.
- Проводити оцінку вразливостей, аналізувати ризики, виявляти прогалини в можливостях і координувати захисні заходи на постійній основі спільно з приватним і некомерційним секторами, а також місцевими, регіональними/міськими, державними, племінними, територіальними, острівними та федеральними організаціями та установами.
- Визначити спільні цілі щодо захисту в рамках діяльності в сферах місії та між ними.
- Впроваджувати плани та програми з безпеки, захисту, стійкості та безперервності, а також тренінги та навчання, а також вживати коритувальних заходів.
- Інтегрувати планування захисту для всієї громади та людей з тваринами (включно з домашніми та службовими тваринами); розробити та задокументувати плани безперервності надання послуг та допоміжні процедури таким чином, щоб при впровадженні ці плани тапроцедури передбачали безперервне виконання основних функцій за будь-яких обставин.
- Забезпечити, щоб планування і діяльність із захисту взаємно підтримували, не суперечили і не впливали негативно на інші плани і діяльність у сфері місії, особливо за допомогою аналітичних продуктів і продуктів з управління ризиками, а також взаємодоповнюючих концепцій.

Інформування та попередження громадськості

Опис: Надавати скоординовану, оперативну, достовірну та практичну інформацію всій громаді, використовуючи чіткі, послідовні, доступні та культурно і мовно прийнятні методи для ефективної

передачі інформації про будь-яку загрозу або небезпеку, а також, у разі необхідності, про заходи, що вживаються, та допомогу, яка надається.

У системі інформування та оповіщення населення використовуються ефективні та доступні індикатори та системи оповіщення для інформування операторів, співробітників служб безпеки та громадськості про значні загрози та небезпеки (включаючи оповіщення, засоби виявлення та інші необхідні ресурси).[23]

Критичні завдання

- Проводити інформаційні кампанії для підвищення пильності.
- Визначити вимоги до інформації зацікавлених сторін у сфері захисту та обміну інформацією.
- Визначити вимоги та процеси обміну інформацією для задоволення комунікаційних потреб усієї громади.
- Створити доступні механізми та надати повний спектр підтримки, необхідної для належного та постійного обміну інформацією між усіма рівнями влади, приватним сектором, релігійними організаціями, неурядовими організаціями та громадськістю.
- Оперативно ділитися дієвою інформацією з громадськістю та між усіма рівнями влади, приватним та комерційним сектором.
- Використовувати всі відповідні засоби комунікації, такі як Інтегрована система оповіщення населення, Національна система консультування з питань тероризму, а також сайти та соціальні мережі.
- Протидіяти повідомленням про насильницький екстремізм у соціальних мережах та інших формах публічної інформації.

Оперативна координація

Опис: Створити та підтримувати єдину та скоординовану операційну структуру та процес, які належним чином інтегрують зацікавлених сторонів та підтримують реалізацію основних спроможностей.

Оперативна координація підтримує мережування, планування та координацію між партнерами у сфері захисту.

Критичні завдання

- Створити спільні концепції операцій для забезпечення сил і засобів захисту.
- Співпрацювати з відповідними партнерами у сфері захисту.
- Визначати юрисдикційні пріоритети, цілі, стратегії та розподіл ресурсів.
- Встановлювати чіткі лінії та способи комунікації між організаціями та юрисдикціями, що беруть участь у проекті.
- Визначати та доводити до відома чіткі ролі та обов'язки щодо напрямів діяльності.
- Інтегрувати та синхронізувати дії організацій та юрисдикцій-учасниць для забезпечення єдності зусиль.
- Координувати дії на всіх рівнях влади та між ними, а також з критично важливими приватними та некомерційними організаціями для захисту від потенційних загроз, проведення правоохоронних розслідувань або участі у правоохоронних та захисних заходах на основі юрисдикційних повноважень.

- розробити системи або процеси, які дозволяють різним сторонам або організаціям, що беруть участь в місії захисту, взаємодіяти та обмінюватися інформацією між собою безперешкодно, незалежно від їхніх власних систем або технологій зв'язку.

[23] Системи інформування та оповіщення населення повинні забезпечувати ефективну комунікацію для людей з інвалідністю, наприклад, аудіо- та відеосупроводження мультимедійних матеріалів, а також доступні веб-сайти. Інформування та оповіщення громадськості також повинно здійснюватися різними мовами та за допомогою культурно різноманітних засобів масової інформації.

- співпрацювати та налагоджувати координацію між різними секторами або областями діяльності, що стосуються захисту, з метою забезпечення відповідних здатностей та ресурсів для національної готовності.

Основні можливості захисту та запобігання

Наступні основні спроможності охоплюють сфери місії "Захист і запобігання": Обмін розвідданими та інформацією; Перешкоджання і припинення; Перевірка, пошук і виявлення. Ці спроможності розглядаються тут у контексті захисту. Опис цих сил і засобів в контексті запобігання див. в Рамковій програмі запобігання.

Обмін розвідданими та інформацією

Опис: Обмін розвідувальною інформацією - це надання своєчасної, точної та дієвої інформації, що є результатом планування, збору, використання, обробки, аналізу, виробництва, розповсюдження, оцінки та зворотного зв'язку наявної інформації щодо загроз Сполученим Штатам, їх населенню, майну або інтересам; заходи, спрямовані на розробку, поширення або використання зброї масового знищення (WMD) або будь-яких інших питань, пов'язаних з національною або внутрішньою безпекою США, здійснюваних на місцевому, штатному, племінному, територіальному, федеральному та інших рівнях уряду, а також іншими зацікавленими сторонами.[24]

Обмін інформацією - це можливість обмінюватися розвідданими, інформацією, даними або знаннями між державними або приватними структурами, залежно від обставин.

Розвіддані та інформація мають важливе значення для стратегічного розвитку інших можливостей захисту та інформування про заходи забезпечення захисту. Усі дії в рамках Національної системи захисту базуються на моніторингу, зборі та аналізі розвідувальних даних та інформації. Розвідка та обмін інформацією вимагають розвитку аналітичного потенціалу, а також розробки і використання мереж, процедур і форматів для поширення аналітичних продуктів.

У контексті захисту, розвідка і обмін інформацією передбачають ефективне виконання розвідувального циклу та інших процесів збору і обміну інформацією на місцевому, регіональному рівнях, на рівні штатів, племен, територій, острівних територій і на федеральному рівні, а також у приватному і некомерційному секторах і серед громадськості з метою розвитку ситуаційної обізнаності про потенційні загрози і небезпеки на території Сполучених Штатів Америки.

Обмін інформацією використовуючи партнерські стосунки у поєднанні зі скоординованою взаємодією, що підвищує ситуаційну обізнаність, посилює місію захисту.
Уряд США сприяє розвитку культури обміну інформацією, впроваджує нові технології та вдосконалює свою політику і процедури на підтримку зобов'язання ділитися своєчасною, актуальною і дієвою розвідувальною та іншою інформацією з найширшою аудиторією.

Критичні завдання

- Моніторити, аналізувати та оцінювати позитивні та негативні наслідки змін в оперативному середовищі з точки зору загроз та небезпек для громадської безпеки, здоров'я та захисту населення. Діляться результатами аналізу через:
  - Участь у громадських, місцевих, регіональних, штатних, племінних, територіальних та національних освітніх та просвітницьких програмах;
  - Участь у регулярному обміні інформацією з питань безпеки, включаючи оцінку загроз,

попередження про можливі атаки, індикатори та попередження про загрози.

[24] Процеси розвідувального циклу включають такі етапи: планування; керівництво; збір, використання, обробка та аналіз наявної інформації; виробництво; розповсюдження; оцінка та зворотній зв'язок.

- Визначити вимоги до розвідувальних даних та обміну інформацією для зацікавлених сторін у сфері захисту, а також до обміну інформацією.

- Розробити або визначити та забезпечити доступ до механізмів і процедур обміну розвідданими та інформацією між державними, приватними, релігійними та урядовими партнерами з питань захисту.[25]

- Використовувати процеси розвідки для підготовки та надання актуальних, своєчасних, доступних і дієвих розвідувальних та інформаційних продуктів іншим, в тому числі партнерам в інших сферах діяльності місії.

- Дотримуватися належних механізмів захисту конфіденційної та секретної інформації, а також захисту приватного життя, громадянських прав і свобод.

Перешкоджання та припинення

Опис: Затримати, перехопити, зупинити або убезпечити загрози та/або небезпеки. Ці загрози та небезпеки включають людей, матеріали або діяльність, які становлять загрозу для нації, в тому числі внутрішня і транснаціональна злочинна і терористична діяльність, а також зловмисне переміщення і придбання/передача хімічних, біологічних, радіологічних, ядерних і вибухових (ХБРЯ) матеріалів і пов'язаних з ними технологій.

У контексті захисту ці сили і засоби включають в себе заходи з перешкоджання і припинення діяльності, що проводяться у відповідь на загрози, або зосередження сил і засобів під час особливих подій.

Заходи з перешкоджання та припинення, що проводяться правоохоронними органами та співробітниками служб безпеки державного і приватного секторів під час виконання своїх повсякденних обов'язків, включають здійснення контролю та забезпечення виконання законодавства на кордонах Сполучених Штатів Америки, включаючи прикордонні пункти в'їзду та виїзду, а також території між ними.

Критичні завдання

- Стримувати переміщення та діяльність терористів на території Сполучених Штатів.
- Забезпечити здатність виявляти ХБРЯ-пристрої або протидіяти ХБРЯ-загрозам.
- Затримувати транспортні засоби, вантажі та осіб, пов'язаних з потенційною загрозою.

- Впровадження заходів із забезпечення громадського здоров'я з метою зменшення поширення загроз захворювань за кордоном і запобігання перетинанню національних кордонів таких загроз.

- Запобігати фінансуванню тероризму або проводити заходи з протидії придбанню зброї, пов'язаних з нею технологій або іншої матеріальної підтримки, щоб не допустити її потрапляння до цільової аудиторії.

- Посилити видиму присутність правоохоронних органів для стримування або запобігання загрозам на шляху до потенційної цілі (цілей).

- Втручання з метою захисту від поширення насильницького екстремізму в американських громадах.

[25] Обмін інформацією повинен забезпечувати ефективну комунікацію з особами з обмеженими можливостями та функціональними потребами, включаючи людей з обмеженим знанням англійської мови та людей з інвалідністю, у тому числі глухих або слабочуючих, а також сліпих або людей зі слабким зором. Ефективна комунікація з особами з обмеженими можливостями та функціональними потребами включає використання відповідних допоміжних засобів та послуг, таких як мова жестів, перекладачі, субтитрування аудіо- та відеоматеріалів і доступних для користувачів веб-сайтів, спілкування різними мовами та використання культурно різноманітних засобів масової інформації.

- Використовуйте засоби пошуку та виявлення у цільових районах у взаємодії з місцевими силами, регіональними/міськими, штатними, племінними, територіальними, острівними територіями, федеральними службовцями або іншими федеральними агентствами (залежно від загрози).

Перевірка, пошук і виявлення

Опис: Ідентифікація, виявлення або локалізація загроз та/або небезпек шляхом активного і пасивного спостереження та пошукових процедур. Ця діяльність може включати використання систематичних перевірок та оцінок, біонагляду, сенсорних технологій, фізичного розслідування та розвідки.

У контексті захисту ця спроможність включає перевірку вантажів, транспортних засобів, пошти, багажу та людей, а також виявлення Засобі масового знищення, традиційних і нових загроз та небезпек, що викликають занепокоєння.

Заходи з перевірки, пошуку та виявлення захищають мешканців та критично важливі об'єкти, системи та мережі від найнебезпечніших загроз для країни, не створюючи при цьому надмірних перешкод для комерційної діяльності.

Критичні завдання

- Визначати потенційні загрози від людей або мереж.
- Розвивати і залучати національне співтовариство (окремих осіб, сім'ї, громади, а також місцеві,штатні, племінні та територіальні органи влади і партнерів з приватного сектору).
- Перевіряти осіб, багаж, пошту, вантажі та транспортні засоби, використовуючи технічні, нетехнічні, інтрузивні та ненав'язливі засоби, не створюючи при цьому надмірних перешкод для комерції. Розглянути додаткові заходи щодо осіб, транспортних засобів та предметів підвищеного ризику:
  - Проведення операцій з пошуку та виявлення ХБРЯ.
  - Проводити пасивне та активне виявлення ХБРЯ агентів.
  - Безпечна робота в небезпечному середовищі.
  - Розглянути можливість розгортання федеральних команд з метою підвищення ефективності місцевих, регіональних, штатних, племінних, територіальних та федеральних органів влади, включаючи використання засобів оцінки і усвідомлення подій.
- Здійснювати біонагляд за даними, що стосуються здоров'я людини, тварин, рослин, продуктів харчування, води та навколишнього середовища.

Основні можливості, унікальні для захисту

Решта основних можливостей є унікальними для Захисту: Контроль доступу та ідентифікація особи; кібербезпека; заходи фізичного захисту; управління ризиками для програм і заходів захисту; цілісність і безпека ланцюга постачання.

Контроль доступу та ідентифікація особи

Опис: Застосовувати та підтримувати необхідні фізичні, технологічні та кіберзаходи для контролю

доступу до критично важливих об'єктів та систем.

Ця здатність ґрунтується на впровадженні та підтримці протоколів для перевірки особи, авторизації, надання або відмови у фізичному та кібердоступі до певних місць, інформації та мереж

Критичні завдання

- Перевіряти особу, щоб надати або заборонити фізичний і кібердоступ до фізичних і кіберактивів, мереж, додатків і систем, які можуть бути використані для заподіяння шкоди.
- Контролювати та обмежувати доступ до критично важливих об'єктів та систем, та надавати такий доступ лише уповноваженими особами, які здійснюють законну діяльність.

Кібербезпека

Опис: Захист (і, за необхідності, відновлення) електронних комунікаційних систем, інформації та послуг від пошкодження, несанкціонованого використання та експлуатації.

Заходи з кібербезпеки забезпечують безпеку, надійність, цілісність та доступність критично важливої інформації, документації та комунікаційних систем і послуг через спільні ініціативи та зусилля з забезпечення кібербезпеки.

Критичні завдання

- Впроваджувати контрзаходи, технології та політики для захисту фізичних і кібер-активів, мереж, додатків і систем, які можуть бути використані для завдання шкоди.
- Захищати, наскільки це можливо, державні та приватні мережі та критично важливу інфраструктуру (напр, комунікаційні, фінансові, електромережі, мережі водопостачання та транспортні системи), на основі результатів оцінки вразливостей, заходів щодо зниження ризиків та здатностей реагування на інциденти.
- Формалізація відносин (Розробка договорів, процедур та механізмів співпраці) з урядовими органами, комерційними компаніями та іншими суб'єктами з метою швидкого відповідного реагування на кіберінциденти, обміну інформацією, співпраці в розслідуванні та подоланні наслідків.
- Формалізація відносин (Розробка договорів, процедур та механізмів співпраці) між різними спеціалізованими групами, організаціями або відділами, які відповідають за кібербезпеку, та тими, які відповідають за фізичні системи, що залежать від кібербезпеки, такі як критична інфраструктура.
- Формалізація відносин між постачальниками інформаційно-комунікаційних технологій та інформаційних систем і їхніми клієнтами для забезпечення постійної кібербезпеки продуктів, бізнес-планування та переходу до реагування і відновлення в разі потреби.
- Ділитися дієвою інформацією про кіберзагрози з національним та міжнародним урядом, а також приватним сектором, щоб сприяти спільній ситуаційній обізнаності.
- Впроваджувати стандарти, що враховують ризики, для забезпечення безпеки, надійності, цілісності та доступності критично важливої інформації, документації та комунікаційних систем і послуг за допомогою спільних ініціатив та зусиль у сфері кібербезпеки.
- Виявляти та аналізувати зловмисну активність і підтримувати заходи з її мінімізації.
- Співпрацювати з партнерами для розробки планів і процесів, що сприятимуть скоординованому реагуванню на інциденти.
- Використовувати ресурси правоохоронних органів та розвідки для виявлення, відстеження,

розслідування та переслідування зловмисників, які загрожують безпеці державних та приватних інформаційних систем країни.

- Створювати стійкі кіберсистеми, які забезпечують безперебійне виконання основних функцій.

Заходи фізичного захисту

Опис: Впроваджувати та підтримувати ризик-орієнтовані контрзаходи та політику захисту людей, кордонів, споруд, матеріалів, продуктів та систем, пов'язаних з ключовими оперативними заходами та критично важливими секторами інфраструктури.

Ця спроможність включає зменшення або пом'якшення ризиків, в тому числі дії, спрямовані на усунення загроз, вразливостей та/або наслідків, шляхом контролю за пересуванням і захисту кордонів, критичної інфраструктури та батьківщини.

Критичні завдання

- Визначати пріоритети активів, систем, мереж та функцій, які потребують захисту.
- Визначити необхідний фізичний захист, контрзаходи (включаючи медичні та немедикаментозні заходи), а також політики через оцінку ризиків ключових оперативних діяльностей та інфраструктури.
- Захист критичних функцій життєзабезпечення, які включають енергетику, комунікації, транспорт, управління водними ресурсами та стічними водами.
- Розробляти та впроваджувати плани безпеки, в тому числі плани безперервності бізнесу, які враховують ризики.
- Розробляти та впроваджувати заходи фізичної безпеки, контрзаходи, політики та процедури, що базуються на оцінці ризиків.
- Впровадити тренінги з безпеки для працівників, зосереджені на ситуаційній обізнаності та реагуванні.
- Розробляти та впроваджувати програми та практики біозахисту та біобезпеки.
- Використовувати федеральні програми закупівель, якщо це доцільно, для забезпечення максимальної економічної ефективності, безпеки та інтероперабельності закупівель.

Управління ризиками для програм та заходів захисту

Опис: Виявлення, оцінка та визначення пріоритетності ризиків для обґрунтування заходів захисту, контрзаходів та інвестицій. Ця мета досягається шляхом впровадження та підтримки процесів оцінки ризиків для виявлення та визначення пріоритетності активів, систем, мереж та функцій, а також впровадження та належних інструментів для виявлення та оцінки загроз, вразливостей та наслідків.

Управління ризиками - це системний та аналітичний процес, який розглядає ймовірність того, що загроза може завдати шкоди активу, особі чи функції, а також визначає дії для зменшення ризику та пом'якшення наслідків. Оцінка загроз - це інструмент підтримки прийняття рішень, який може допомогти у плануванні програми безпеки. Оцінка загроз виявляє і надає оцінку загрозам на основі різних факторів, включаючи можливості, наміри та інші наслідки інциденту.

Критичні завдання

- Своєчасно і точно збирати необхідні дані для ефективного виявлення ризиків.
- Розробити та використовувати відповідні інструменти для виявлення та оцінки загроз, вразливостей та наслідків.
- Розбудовувати спроможність громад аналізувати та оцінювати ризики та стійкість.
- Визначати, впроваджувати та контролювати плани управління ризиками.

- Оновлювати оцінки ризиків з метою переоцінки ризиків на основі змін у таких сферах: фізичне середовище(включаючи вплив зміни клімату), старіння інфраструктури, розвиток технологій, нові проекти та ініціативи з мінімізації наслідків, перевірка/валідація після події, нові технології або вдосконалені методології та оновлені дані.

- Перевіряти, калібрувати та вдосконалювати оцінки ризиків, спираючись на досвід, засвоєні уроки та знання, що виходять за рамки необроблених даних або моделей.

- Використовувати оцінку ризиків для визначення потенційних загроз, вразливостей та наслідків різних сценаріїв подій, що можуть відбутися, та на їх основі розробити тренувальні сценарії та проекти з мінімізації ризиків.

- Розробити єдиний підхід до інвестування в безпечну та стійку інфраструктуру, щоб громади могли протистояти наслідкам катастроф, ефективно реагувати на них, швидко відновлюватися, адаптуватися до мінливих умов та управляти ризиками у майбутньому.

Цілісність та безпека ланцюга постачання

Опис: Посилення безпеки та стійкості ланцюга постачання. Ця можливість залежить від захисту та забезпечення стійкості ключових вузлів, методів транспортування між вузлами та матеріалів, що перебувають у дорозі між постачальником і споживачем.

Розгалужений характер глобального ланцюга поставок робить його вразливим до навмисних або стихійних збоїв. Мультимодальний, міжнародний характер глобального ланцюга поставок вимагає широких зусиль, які включають участь зацікавлених сторін державного та приватного секторів, як на міжнародному, так і на національному рівнях. Захист ґрунтується на багаторівневому, заснованому на оцінці ризиків і збалансованому підході, за якого необхідні заходи безпеки та планування стійкості інтегровані в ланцюги поставок.

Критичні завдання

- Інтегрувати процеси безпеки в операції ланцюга поставок, щоб виявити проблемні питання та вирішити їх якомога раніше.

- Проаналізувати ключові залежності та взаємозалежності, пов'язані з операціями ланцюга поставок.[26]

- Використовувати принципи управління ризиками для виявлення, зменшення вразливостей та захисту ключових активів, інфраструктури та систем підтримки.

- Впроваджувати фізичні засоби захисту, контрзаходи та політики для захисту та підвищення стійкості ключових вузлів, методів транспортування між вузлами та матеріалів під час транспортування.

- Використовувати можливості перевірки виявлення товарів, які не відповідають їх заявленому опису, є не задекларованими або забороненими; а також для запобігання компрометації або помилковому направленню вантажу під час його переміщення через логістичну систему.

- Використовуйте різноманітні заходи захисту від різноманітних традиційних та асиметричних загроз. Ці рівні включають розвідку і аналіз інформації; належне використання технологій; закони, правила і політики; належним чином підготовлений і оснащений персонал; ефективні партнерства.

[26] Залежність - це односпрямована залежність від ввідних даних, взаємодії або іншого джерела для того, щоб функціонувати належним чином. Взаємозалежність - це взаємозалежні відносини між об'єктами, особами або групами. Ступінь взаємозалежності не обов'язково має бути однаковим в обох напрямках.

Сприятливі умови та міжнародна співпраця

Координаційні структури - це механізми, які підтримують і забезпечують основні спроможності. Національна система захисту спирається на широкий спектр існуючих координаційних структур по всій країні. Координаційні структури сприяють зміцненню співпраці та визначають єдиний підхід, який узгоджує діяльність юрисдикцій, місій та сфери відповідальності для вирішення складних та міждисциплінарних питань захисту. Координаційні структури підтримують стабільну діяльність місії з питань захисту і зміцнюють здатність держави посилювати свою обороноздатність у періоди підвищеної готовності, реагування на інциденти або на підтримку запланованих спеціальних заходів. Ці структури використовуються для планування, реалізації програм навчання і тренувань, сприяння обміну інформацією, формування пріоритетів досліджень і розробок та технічних вимог, усунення вразливостей, узгодження ресурсів і сприяння реалізації сил і засобів захисту. До координаційних структур, які сприяють виконанню місії "Захист", належать оперативні центри, оперативні групи правоохоронних органів, партнерства у сфері критичної інфраструктури, керівні ради, регіональні консорціуми, механізми обміну інформацією, такі як центри об'єднання штатів і великих міських районів, мережі спостереження за станом здоров'я, а також організації державно-приватного партнерства на всіх рівнях.

У цьому розділі окреслено національні категорії координаційних структур і представлено уніфікований підхід до того, як ці структури працюють разом для виконання місії захисту.

- Громадські, місцеві, племінні, штатні та регіональні координаційні структури
  - Партнерства
  - Оперативна координація
  - Координація через усталені системи та принципи
- Федеральні координаційні структури
  - Рада національної безпеки
  - Федеральні відомства та агентства
  - Міжвідомча координація
- Робота з координаційними структурами

Громадські, місцеві, племінні, штатні та регіональні координаційні структури

Координація через партнерства

Координація місій із захисту здійснюється через існуючі партнерства на всіх рівнях влади, а також з приватним і некомерційним сектором. Існують численні приклади існуючих партнерств або коаліцій у сфері захисту - від програм на рівні мікрорайонів до регіональних державно-приватних рад, спільних робочих груп, коаліцій у сфері охорони здоров'я та координаційних рад із захисту інфраструктури. Багато створених громадських та регіональних груп сприяють заходам з підтримки захисту та готовності. Ці партнерства можуть виходити за межі секторів критичної інфраструктури та географічних кордонів. Вони дозволяють обмінюватися досвідом та інформацією і є джерелом потенційних ресурсів через угоди про взаємодопомогу та взаємо підтримку.

Наприклад, Національний план захисту інфраструктури (National Infrastructure Protection Plan, NIPP) сприяє розподілу відповідальності за безпеку та стійкість критичної інфраструктури між усіма рівнями влади та власниками і операторами критичної інфраструктури. Хоча це не єдине державно-приватне

партнерство в США, це партнерство зосереджується на безпеці та стійкості критично важливої інфраструктури. Секторальні агентства (SSA) надають експертну допомогу та беруть участь у повсякденній діяльності з безпеки та стійкості критичної інфраструктури у визначених секторах.[27] У кожному секторі налагоджені партнерські відносини із зацікавленими сторонами, включаючи власників та операторів ОКІ, місцеві, регіональні/міські, штатні, племінні, територіальні, острівні та федеральні органи влади, правоохоронні органи, торгові асоціації та радників з питань національної безпеки на рівні штатів. Створені секторальні, урядові та міжсекторальні ради, а також механізми обміну інформацією, такі як Організації з обміну інформацією є одними з основних структур для планування захисту, управління ризиками та впровадження програм захисту для покращення фізичної та кібербезпеки. Секторальні агентства відповідають за співпрацю з державними та приватними партнерами з метою розробки програм і стратегій безпеки та стійкості.

Через специфічні виклики та взаємозалежності, з якими стикаються окремі регіони, а також широкий спектр і різноманітність державного, приватного та некомерційного секторів, регіональні зусилля часто є складними і можуть включати багато різних аспектів або елементів. Приклади регіональних партнерств, створених для розгляду регіональних питань, варіюються від партнерства Тихоокеанського північно-західного економічного регіону (PNWER)28 , робочі групи якого займаються такими питаннями, як безпека кордонів, сільське господарство і енергетика, до регіональних партнерств, які зосереджуються переважно на одному секторі інфраструктури, як, наприклад, Багатодержавне партнерство з безпеки в сільському господарстві.[29]

Добровільна співпраця між державним і приватним секторами та обмін інформацією між державним, приватним та некомерційним сектором має важливе значення для досягнення критично важливих цілей щодо основних спроможностей в рамках місії "Захист" та програм підтримки.

Оперативна координація

У більшості юрисдикцій скоординоване надання можливостей для захисту відбувається через децентралізовану координацію всієї громади. Державні та великі міські об'єднані центри підтримують і забезпечують оперативну координацію, виступаючи в ролі координаційних центрів на місцевому, племінному та штатному рівнях для отримання, аналізу, збору та обміну інформацією про загрози між урядом, приватним і некомерційним секторами. Аналогічно, місцеві, племінні та секторальні оперативні центри слугують для узгодження та розподілу ресурсів на підтримку партнерів місії "Захист". Міністерство національної безпеки США координує діяльність з безпеки і стійкості критичної інфраструктури через Національний інфраструктурний координаційний центр і Національний центр інтеграції кібербезпеки і комунікацій, але також підтримує поточну оперативну координацію через секторальні координаційні структури, які спрямовують національні зусилля на координацію між партнерами з державного і приватного секторів. Об'єднані антитерористичні робочі групи - це багатоюрисдикційні робочі групи під керівництвом ФБР, створені для проведення розслідувань, пов'язаних з тероризмом, які базуються в більш ніж 100 містах по всій країні. Об'єднані антитерористичні групи ФБР зосереджують свою увагу на питаннях, пов'язаних з тероризмом, з особливим акцентом на розслідуваннях тероризму, що мають місцеві, регіональні, національні та міжнародні наслідки. Координація між цими центрами та цільовими групами, а також обмін інформацією з оперативними та об'єднаними центрами допомагають інформувати про діяльність із запобігання, захисту, реагування та відновлення. Ці центри також надають інформацію для планування заходів із запобігання.

---

[27] Секторальні агентства, які надають експертну допомогу та щоденну взаємодію для забезпечення безпеки та стійкості критичної інфраструктури у визначених секторах, визначені в PPD-21: Безпека та стійкість критичної інфраструктури. ППД-21 також передбачає, що на додаток до обов'язків, покладених на АСО, інші федеральні департаменти та відомства мають спеціальні функції , пов'язані з безпекою та стійкістю критичної інфраструктури.

[28] Заснована у 1991 році, PN W ER є статутним, двонаціональним, державно-приватним партнерством. PN W ER сприяє роботі групи державних і приватних лідерів для вирішення питань, що впливають на економіку Тихоокеанського північно-західного регіону.

[29] Засноване у 2004 році Міждержавне партнерство з безпеки в сільському господарстві - це консорціум з 14 держав, який визнає, що сільськогосподарські катастрофи можуть мати регіональні, національні та глобальні наслідки.

Координація через усталені системи та принципи

Національна система захисту сприяє використанню принципів, подібних до тих, що містяться в NIMS,

для координації основних сил і засобів в рамках місії захисту на всіх рівнях влади, в приватному та комерційному секторах. Наприклад, NIMS надає керівні принципи, які дозволяють організаціям з різними юридичними, географічними та функціональними обов'язками ефективно координувати, планувати свою діяльність, а також взаємодіяти. Кожна організація-учасниця зберігає свої повноваження, відповідальність та підзвітність. Компоненти, концепції та принципи NIMS підтримують перехід організацій, які відіграють активну роль у багатьох сферах місії.

Федеральні координаційні структури

На федеральному рівні існує низка координаційних структур, які сприяють налагодженню партнерських відносин, плануванню, обміну інформацією, а також синхронізації ресурсів та операцій в усіх аспектах місії захисту. Цей розділ присвячений координації на політичному рівні, що здійснюється керівництвом Білого дому, державно-приватним партнерством, а також структурам, які вже існують або мають бути створені для забезпечення скоординованого підходу до захисту в масштабах усієї спільноти.

Рада національної безпеки

Рада національної безпеки є головним політичним органом, який розглядає питання політики національної безпеки, що потребують втручання Президента. Рада національної безпеки консультує і допомагає Президенту в інтеграції всіх аспектів політики національної безпеки, що впливають на Сполучені Штати - внутрішньої, зовнішньої, військової, розвідувальної та економічної (спільно з Національною економічною радою). Разом з підпорядкованими їй комітетами, Рада національної безпеки є головним засобом координації діяльності департаментів і відомств виконавчої влади у розробці та впровадженні політики національної безпеки.

Федеральні відомства та агентства

На додаток до статутних та інших обов'язків міністра внутрішньої безпеки, міністр внутрішньої безпеки відповідає за координацію внутрішніх зусиль щодо забезпечення готовності до всіх видів небезпек усіх департаментів і відомств виконавчої влади, консультуючись з місцевими, державними, племінними і територіальними органами влади, приватним і некомерційним сектором, а також широкою громадськістю.[30] Керівники всіх департаментів і відомств виконавчої влади, які мають відношення до захисту, несуть відповідальність за національні зусилля щодо забезпечення готовності відповідно до їхніх статутних функцій і обов'язків.[31]

Федеральний уряд сприяє координації діяльності в рамках місії захисту через широкий спектр координаційних структур. Відповідно до Національної системи захисту, різні федеральні міністерства та відомства беруть на себе основні координуючі функції відповідно до своїх повноважень і характеру загроз або небезпек. Ці федеральні міністерства та відомства забезпечують основу для постійної координації та співпраці, необхідної для сприяння впровадженню та забезпечення постійного управління і підтримки Національної системи захисту та інших заходів з готовності до захисту.

Міністр національної безпеки скликає, за необхідності, нараду представників федеральних міністерств та відомств для обговорення та розгляду питань координації основних сил і засобів в рамках місії "Захист", зосереджуючи увагу на наступних аспектах:

[30] За винятком тих видів діяльності, які можуть втручатися в повноваження Генерального прокурора або директора ФБР.

[31] Конкретні законодавчі та інші обов'язки федеральних міністерств та відомств визначені в розділі "Ролі та обов'язки".

- планування та координація готовності здійснюється відповідно до Національної система Захисту та інших зусиль щодо реалізації Національної Системи Готовності.

- Обмін інформацією, що стосується діяльності у сфері захисту.
- Співпраця в рамках всієї спільноти.
- Основні проблеми та рекомендовані напрямки дій.
- Інтеграція із запобігання, пом'якшення наслідків, реагування та відновлення, шляхом координації з аналогічними групами в цих аспектах місії.

Міжвідомча координація

У відповідь на підвищені ризики або необхідність підвищеної активності щодо питань, пов'язаних із захистом Міністр національної безпеки може повідомити міністерствам та відомствам про необхідність підтримки ескалації процесу прийняття рішень, описаного в цій Національній системі захисту. Крім того, керівництво міністерств і відомств може повідомити Міністра національної безпеки про таку необхідність. Керівництво федеральних департаментів і агентств може збиратися на існуючі форуми Міністерства Національної Безпеки або міжвідомчі координаційні форуми для підтримки міжвідомчого планування захисту з метою управління та вирішення нагальних або невідкладних питань захисту. Така ескалація координації немає фіксованої функції або набору обов'язків, але скликається на основі характеру і вимог нагальних питань захисту. Під час штатного режиму функціонування, постійні міжвідомчі координаційні групи в рамках десяти координаційних заходів у сфері захисту скликаються для координації, планування та обміну інформацією між федеральним урядом.

Робота з різними координаційними структурами

Діяльність та місії у сфері захисту координуються в рамках низки повноважень, можливостей та функцій, що перетинаються. Закони, які надають повноваження державним органам, і професійні домовленості, які регулюють проведення місій із захисту, також забезпечують модель, за якою координується діяльність із захисту, щоб убезпечити країну від комплексних загроз і небезпек.Оскільки загрози і небезпеки впливають на різні сектори, а також виходять за межі секторів і юрисдикцій, заходи в рамках місії захисту уніфіковані шляхом встановлення зв'язків між існуючими координаційними структурами.

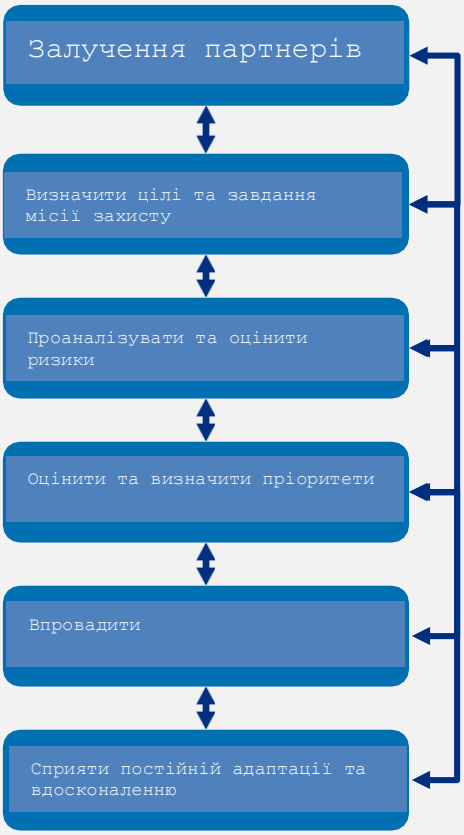
Координаційні структури інтегруються шляхом спільного розвитку національних сил і засобів, розробки спільних планів, аналітичних продуктів і каналів обміну інформацією, які охоплюють сфери діяльності місії з забезпечення готовності.

Заходи захисту для забезпечення основних спроможностей

Процес захисту в сталому режимі

Цей розділ підсумовує процес визначення заходів, необхідних для захисту від загроз і небезпек в сталому режимі. Відповідальність за захист у сталому режимі покладається на спільноту, що займається питаннями захисту, включаючи окремих осіб та їхні домогосподарства, органи влади всіх рівнів, приватний та некомерційний сектор.

Усім суб'єктам, відповідальним за захист, включаючи уряди всіх рівнів, власників і операторів критичної інфраструктури та бізнес, рекомендується використовувати сталий режим координації для визначення основних сил і засобів, необхідних для виконання місії із забезпечення захисту. На Рисунку 2 зображено сталий режим захисту.



Сталий режим захисту вимагає децентралізованого управління ризиками для ефективного виконання завдань. Як національна модель координації між різними партнерами, організаціями та зацікавленими сторонами у сфері захисту, стабільна координація діяльності у сфері захисту спирається на існуючі координаційні структури для обміну інформацією та підтримки обґрунтованої та адаптивної діяльності місії у сфері захисту.

Захист є безперервним процесом і вимагає адаптивної моделі організаційного навчання та міжвідомчої координації.

Рисунок 2: Сталий режим захисту

1. **Залучення партнерів.** На цьому етапі циклу захисту визначається розмір і сфера діяльності місцевих координаційних структур або юрисдикцій шляхом визначення додаткових партнерів у сфері захисту. Партнери у сфері захисту визначають основні можливості, необхідні для досягнення місій у сфері захисту, та окреслюють ролі та обов'язки кожного партнера у сфері захисту.

2. **Визначити цілі та завдання місії захисту.** Другий крок процесу полягає у визначенні того, що саме намагається захистити громада чи юрисдикція. Бажані цілі та завдання можуть відрізнятися в різних юрисдикціях або зонах відповідальності, залежно від ландшафту ризиків та операційного середовища. Цілі та завдання, розроблені спільно, допомагають створити спільне бачення бажаного довгострокового стану безпеки та критеріїв відновлення і повинні відображати цілі захисту для всіх партнерів. Партнери у сфері захисту також можуть спиратися на ці цілі під час управління ризиками, щоб найкращим чином визначити, які конкретні основні можливості захисту та стратегії зменшення ризиків і захисту найбільш суттєво підвищать безпеку в регіоні. Етапи процесу захисту повинні включати визначення можливостей для розбудови стійкості в процесі планування та реалізації заходів.

3. **Оцінка та аналіз ризиків.** На цьому етапі партнери у сфері захисту оцінюють та аналізують ризики,щоб отримати загальну картину ризиків. Конкретної методології для оцінки ризиків не передбачено.[32]
   Незалежно від методу, важливо оцінити потенційні загрози, небезпеки, вразливості та наслідки таким чином, щоб їх можна було порівняти та визначити пріоритети. На цьому етапі партнери місії "Захист" збирають дані про потенційні загрози та небезпеки, пов'язані з міжнародним та внутрішнім тероризмом, техногенними та природними катастрофами, зміною клімату та інфраструктурними збоями.
   Збір даних дозволяє виявити потенційні проблеми, виклики або вразливі місця, які можуть бути пов'язані з конкретною діяльністю або дозволяє виявити розмір і масштаб місії із захисту. Процес включає дослідження поточної та історичної інформації. Історична інформація корисна для оцінки ймовірності виникнення та наслідків потенційних загроз і небезпек. Ця інформація буде використана для оцінки ризиків.

4. **Оцінити та визначити пріоритети.** На цьому етапі партнери з питань захисту використовують результати аналізу ризиків, щоб оцінити свою діяльність у сфері захисту на предмет потенційних ризиків. Партнери також визначають пріоритетність своїх потреб і зусиль у сфері захисту, беручи до уваги цілі та завдання місії.

5. **Поінформовані, децентралізовані та уповноважені дії.** На цьому етапі партнери із захисту вживають заходів для досягнення визначених цілей і завдань захисту. Вони здійснюють захисні заходи, спрямовані на вирішення пріоритетних завдань, визначених на попередніх етапах, в рамках окремих повноважень і в координації з іншими партнерами місії.

6. **Сприяти постійній адаптації та вдосконаленню.** Цей крок включає дії, що забезпечують постійне вдосконалення, таке як проведення навчань та тренінгів, аналіз отриманих уроків та результатів оцінювання. Адаптація до мінливих ризиків відбувається паралельно з підвищенням ефективності. Цей процес може спонукати громаду переглянути будь- який з попередніх етапів.

Процес прийняття рішення про ескалацію захисту

Міжвідомча координація може бути переведена в періоди підвищеної загрози. У цьому випадку громади швидко координують діяльність із захисту (наприклад, обмін інформацією, розробку міжвідомчого плану дій, планування/координацію комунікацій, оцінку, аналіз і моделювання, оповіщення і розгортання ресурсів та інші необхідні заходи), консультуючись і координуючись з федеральними міністерствами і

відомствами та постраждалою юрисдикцією (юрисдикціями). На Рисунку 3 зображено процес прийняття рішення про ескалацію захисту.

[32] Посібник з комплексної готовності 201, друге видання, надає громадам додаткові рекомендації щодо проведення ідентифікації загроз і небезпек та оцінки ризиків (THIRA). Для забезпечення безпеки та стійкості критичної інфраструктури Національний план захисту інфраструктури містить критерії, яким мають відповідати методології оцінки ризиків. Для отримання додаткової інформації зверніться до Національного плану захисту інфраструктури.

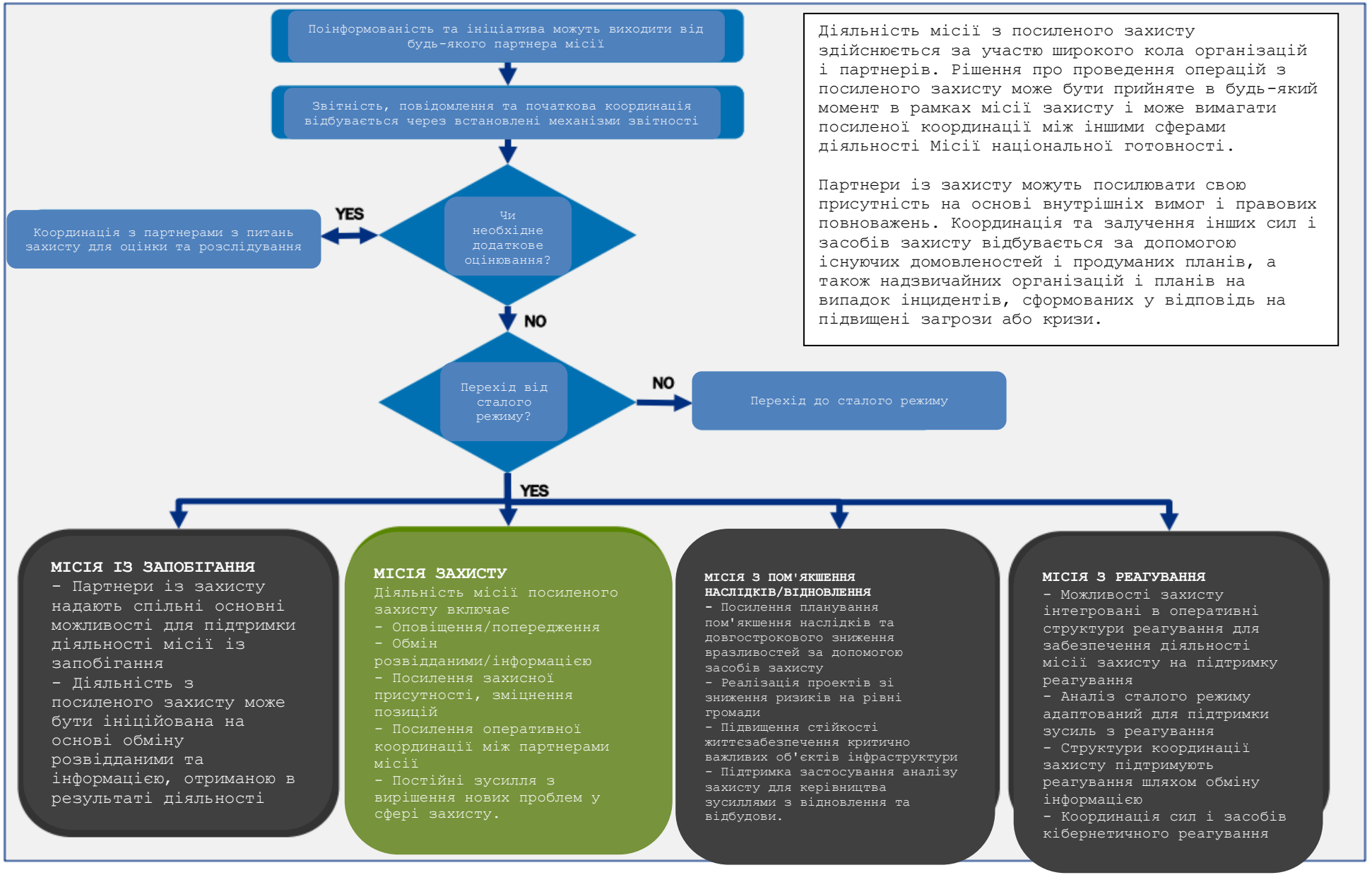


Рисунок 3: Процес прийняття рішення про ескалацію захисту

- **Поінформованість та ініціативність.** Потреба в ескалації заходів із захисту та координації між партнерами може виникнути будь-де в межах діяльності місії із захисту. Рішення про ініціювання дій, які призводять до підвищення рівня активності у сфері захисту та залучення інших партнерів, є результатом лідерства та координації з боку партнерів у сфері захисту в рамках усієї спільноти.

- **Звітування та сповіщення.** Уся громада ділиться інформацією про потенційні загрози та небезпеки, використовуючи встановлені канали зв'язку та сповіщення. Залежно від типу загрози або небезпеки, державні, приватні та некомерційні організації зобов'язані або заохочуються повідомляти інформацію про потенційні загрози та небезпеки, використовуючи існуючі механізми та законодавчі вимоги. Приклади включають правоохоронні органи, охорону здоров'я та встановлені партнерські канали комунікації та звітності.

- **Оцінювання.** Уряди на всіх рівнях підтримують операції з ліквідації наслідків надзвичайних ситуацій, а також центри спостереження та реагування для підтримання ситуаційної обізнаності та аналізу потенційних загроз і наслідків. Оцінка нової загрози як вірогідної, а самої загрози як невідкладної означає відхід від сталих режимів функціонування і вимагає дій відповідно до Національної системи реагування, а також посилення сталих заходів із захисту та пом'якшення наслідків. Оцінка нової загрози як потенційної терористичної загрози може вимагати дій відповідно до Національної системи запобігання.

- **Реагування та посилення заходів сталого захисту.** Після оцінки ситуації може виникнути потреба в проведенні заходів із запобігання, пом'якшення наслідків, реагування або відновлення, які потребують підтримки місії із захисту. При виникненні нових проблем може бути необхідно змінити сталі заходи охорони на посилені сталі заходи охорони. Важливість існуючих партнерських структур і каналів обміну інформацією зростає з необхідністю посилення заходів у сталому режимі. Нижче наведені приклади заходів із захисту, що здійснюються під час посиленого сталого режиму:
  - Обмін інформацією про загрози, включаючи випуск попереджень та інших бюлетенів про надзвичайні ситуації. Наприклад, Національна метеорологічна служба видає повідомлення про погоду, щоб попередити громадськість про шторми і суворі погодні умови, що насуваються. На місцевому, штатному, племінному і національному рівнях для моніторингу ризиків для здоров'я регулярно використовується низка систем спостереження за станом здоров'я. Національна система консультування з питань тероризму передає інформацію про терористичні загрози всій громаді.
  - Обмін інформацією та попередженнями про кіберзагрози між федеральним урядом та партнерами з приватного сектору.
  - Підтримка заходів реагування шляхом забезпечення належного захисту громад та осіб, які здійснюють реагування, під час кризи.
  - Координація заходів із запобігання, ліквідації та відновлення шляхом реалізації відповідних повноважень та надання ресурсів.

- **Повернення до сталої діяльності із захисту.** Коли ситуація з посиленим захистом послаблюється, відбувається повернення до сталої діяльності.

Зв'язок з іншими напрямками місії

У цьому розділі описується взаємозв'язок між захистом та іншими сферами діяльності місії. Національна система захисту охоплює сталі та посилені сталі заходи, які потребують координації і здебільшого здійснюються паралельно з процесами, визначеними в програмах з питань запобігання, пом'якшення наслідків, реагування та відновлення.

Зона дії місії «запобігання»

Місії запобігання та захисту тісно пов'язані та інтегровані. Запобігання включає в себе можливості, необхідні для уникнення, запобігання або припинення дії загрози або реального терористичного акту. Для цілей цього документу термін "запобігання" означає запобігання безпосереднім терористичним загрозам. Сфера дії місії "Запобігання" зосереджена на розвідувальних, технічних і правоохоронних заходах, які не дають противнику здійснити напад на території США, з метою запобігання первинному або подальшому терористичному нападу. З іншого боку, діяльність із захисту зосереджена на заходах уряду, приватного сектору і громадян, із виявлення, стримування, перешкоджання діяльності терористів зі збирання інформації, планування, виконання терористичних актів, а також стримання і перешкоджання реалізації інших загроз і небезпек. Всі ці заходи також зосереджені на мінімізації наслідків надзвичайних подій. У деяких випадках ті ж самі сили і засоби, що використовуються для захисту, застосовуються і в операціях із запобігання. Однак, в той час як Національна система запобігання спрямована на безпосередні терористичні акти, Національна система захисту спрямована на усунення всіх загроз і забезпечення постійної безпеки потенційних терористичних цілей. Будь-яка інша діяльність, що традиційно вважається превентивною, наприклад, профілактика захворювань і кібербезпека, підпадає під місію захисту. Крім того, після нападу цілком ймовірно, що операції в зоні дії місії будуть виконуватися одночасно, і що рішення, прийняті в одній зоні місії, можуть мати вплив на інші. Як наслідок, рішення повинні прийматися на основі єдиної інформаційної бази шляхом обміну інформацією та оперативної координації за допомогою оцінки ситуації.

Національні системи захисту та запобігання мають три однакові основні можливості. Процеси, описані в цих Національних системах, розроблені таким чином, щоб діяти одночасно і забезпечувати безперешкодну інтеграцію в разі потреби. Наприклад, у період безпосередньої терористичної загрози діяльність із запобігання може бути зосереджена на обміні інформацією, правоохоронних операціях та інших заходах, спрямованих на запобігання, стримування і попередження тероризму. Захист може оцінювати підвищені ризики і координувати обмін інформацією та інші дії, необхідні для посилення конкретних захисних заходів.

Зона дії місії «пом'якшення наслідків»

Пом'якшення наслідків - це заходи, необхідні для зменшення людських жертв і матеріальних збитків шляхом зменшення впливу і ймовірності того, що певний інцидент призведе до масштабної катастрофи. Діяльність у рамках місій з пом'якшення наслідків та захисту, як правило, здійснюється у сталому режимі або задовго до події. При захисті особлива увага приділяється безпеці і стримуванню загроз, а при пом'якшенні наслідків - досягненню стійкості шляхом зменшення вразливостей. Обидва підходи спрямовані на мінімізацію наслідків і пов'язані з критично важливою інфраструктурою. Забезпечення безпеки цієї інфраструктури належить до місії "Захист", а забезпечення стійкості інфраструктури - до місії "Пом'якшення наслідків". Аналіз ризиків необхідний для ефективної розробки успішних стратегій пом'якшення наслідків і захисту. Інтеграція інформації про ризики, діяльності з планування та координаційних структур зменшує дублювання зусиль і впорядковує дії з управління ризиками в обох сферах діяльності місії.

Зона дії місії «реагування»

Зона дії місії **"Реагування"** включає в себе можливості, необхідні для порятунку життя, захисту майна та навколишнього середовища, а також задоволення основних потреб людини після інциденту. Стихійні лиха та інциденти можуть посилювати вразливості, що вимагає впровадження під час реагування заходів, розроблених у рамках Національної системи захисту. Зусилля із захисту людей і громад, а також життєво важливих об'єктів, систем і ресурсів нерозривно пов'язані із заходами реагування. Учасники реагування підтримують місію захисту і покладаються на організації захисту до, під час і після інцидентів. Ресурси та можливості захисту, необхідні для підтримки операцій з реагування, координуються через структури, визначені в Національній рамці реагування. Національна структура захисту забезпечує структуру для оцінки та усунення підвищеної вразливості та ризиків за межами конкретного району катастрофи, а також для забезпечення того, щоб захисні можливості не були скомпрометовані.

Засоби захисту, розгорнуті для підтримки зусиль з реагування, відповідають та інтегруються в організаційні структури реагування, включаючи Систему управління інцидентами та структури Функції підтримки в надзвичайних ситуаціях.

Аналітичні продукти, розроблені в підтримку заходів захисту під час стабільних умов, також призначені для підтримки планування заходів під час реагування на інцидент.

Оцінка впливу на інфраструктуру та визначення пріоритетів під час реагування також спирається на структури та відносини, що склалися в рамках місії із захисту.

Зона дії місії «Відновлення»

Зона дії місії **"Відновлення"** охоплює можливості, необхідні для надання допомоги громадам, що постраждали від інциденту та їхньому ефективному відновленню. Систематична оцінка загроз і небезпек та реалістичні стратегії, що випливають з оцінки загроз і небезпек через планування на основі оцінки ризиків, є основою дій, що вживаються під час місії відновлення. Координація з планами відновлення до і після стихійного лиха забезпечить стійкий процес відновлення, який враховує питання захисту. Захист і пом'якшення наслідків зосереджені на стійкості економіки та громади, а не лише на швидкому відновленні інфраструктури, будівель та послуг.

Визначення пріоритетів відновлення та забезпечення того, щоб стійкість і управління ризиками були центральними елементами зусиль з відновлення, вимагає від місії із захисту побудови своєї діяльності таким чином, щоб підтримувати зусилля з відновлення.

Оперативне планування

Національні системи планування пояснюють роль кожної сфери діяльності місії в забезпеченні національної готовності та надають всеохоплюючу доктрину того, як спільнота розбудовує, підтримує та забезпечує основні спроможності. Концепції, викладені в концептуальних засадах, використовуються для оперативного планування, яке надає додаткову інформацію щодо ролей та обов'язків, визначає найважливіші завдання, які організація виконуватиме для реалізації основних спроможностей, а також визначає потреби в ресурсах, персоналі та джерелах постачання. Оперативне планування здійснюється на рівні всієї спільноти. На федеральному рівні кожна структура підтримується FIOP для конкретної місії. Посібник з комплексної готовності 101 містить додаткову інформацію про різні типи планів і рекомендації щодо основ планування.

У наступних розділах описано, як оперативне планування застосовується в рамках місії захисту на федеральному рівні.

Оперативне планування захисту

Планування всього спектру заходів у сфері захисту є невід'ємним обов'язком кожного рівня влади, приватного та некомерційного сектору. План - це безперервний, еволюціонуючий інструмент передбачуваної або поточної діяльності, який максимізує можливості та спрямовує операції з захисту. Оперативне планування здійснюється в масштабах усієї спільноти. Його метою є визначення пріоритетів, цілей, стратегій, а також придбання і розподіл ресурсів, необхідних для захисту від потенційних загроз, проведення правоохоронних розслідувань або участі в правоохоронних і захисних заходах на основі повноважень. З точки зору федерального рівня, інтегроване планування допомагає пояснити, як федеральні міністерства та відомства, а також інші партнери на національному рівні надають необхідні ресурси в потрібний час для підтримки місцевих, регіональних/міських, штатних, племінних, територіальних, острівних та федеральних операцій.

Оперативні плани на рівні департаментів

Для підтримки Національної системи готовності кожне виконавче міністерство і відомство розробляє і підтримує, за необхідності, оперативні плани на рівні міністерства, щоб забезпечити основні можливості захисту і виконання обов'язків організації, описаних у FIOPs.

Для розробки таких планів міністерства та відомства можуть використовувати існуючі плани, протоколи, стандартні операційні процедури або керівництва. Кожне міністерство або відомство визначає власні вимоги до планування і вирішує, чи потрібно його підрозділам розробляти підпорядковані оперативні плани.

Оперативні плани на рівні міністерств визначають конкретні критичні завдання та обов'язки, в тому числі, як задовольнити потреби в ресурсах та інші конкретні положення, визначені в FIOPs. Оперативні плани на рівні міністерств також використовують інтегруючі фактори для захисту - усунення ризиків, планування та здійснення процедур координації та комунікації, а також розподіл ресурсів, а також використовують основні можливості захисту.

Федеральний міжвідомчий оперативний план з захисту (FIOP)

FIOP описує, як федеральні відомства та агенції працюють разом, щоб забезпечити основні можливості захисту. Державний, приватний і некомерційний сектори зможуть використовувати FIOP з питань захисту для поточного планування, підготовки і навчань у сфері захисту в межах своїх юрисдикцій або організацій. FIOP буде розроблено в рамках спільного процесу, який забезпечить інтеграцію між усіма сферами місії, з особливим акцентом на запобігання та пом'якшення наслідків. Інформація про федеральні можливості дозволить уряду, приватному і некомерційному секторам більш точно зосередитися на місцевих, регіональних/міських, штатних, племінних, територіальних і острівних потребах у ресурсах і можливостях. Зусилля приватного та некомерційного секторів, місцевого, регіонального/міського, штатного, племінного, територіального та острівного рівнів, а також федерального уряду, спрямовані на підтримку Національної системи захисту, повинні бути спрямовані на вирішення наступних завдань:

- Співпраця з усіма зацікавленими сторонами, включаючи організації, що захищають інтереси людей з обмеженими можливостями та функціональними потребами, включаючи людей з інвалідністю, людей з обмеженим знанням англійської мови, а також людей з расово та етнічно різних спільнот.

- Детальна концепція діяльності, яка пояснює, як операції із захисту координуються тавиконуються спільно.[33]

[33] Концепція діяльності - це заява, яка в загальних рисах пояснює, чого організація (або група організацій) має намір досягти. Вона повинна описувати, як організація або група досягне низки цілей, щоб досягти бажаного кінцевого результату.

- Опис критичних завдань.
- Опис ролей та обов'язків.
- Ресурсні та кадрові потреби.
- Конкретні положення щодо швидкої інтеграції ресурсів та особового складу для посилення операцій у сталому режимі.
- Як плани захисту можуть виконуватися одночасно з іншими планами.
- Як план передбачає заходи та стратегії для вирішення численних, географічно розподілених загроз та небезпек.
- Як план задовольняє потреби людей з гострими захворюваннями.
- Як план передбачає безперервність виконання основних функцій, які є необхідними для забезпечення основних можливостей, які підтримують місії.
- Дотримання положень, що стосуються прав осіб, захищених законами про громадянські права, в тому числі осіб з інвалідністю, расових та етнічних меншин, а також осіб з обмеженим рівнем володіння англійською мовою.

Міністр національної безпеки координує розробку FIOP у співпраці з усіма федеральними міністерствами та відомствами, які відіграють певну роль у реалізації основних можливостей місії "Захист". У розділі "Ролі та обов'язки" визначено федеральні міністерства та відомства, які мають переважні повноваження або обов'язки в рамках місії "Захист". Визначені міністерства і відомства несуть основну відповідальність за участь у процесах планування щодо національної готовності та залучення інших федеральних міністерств і відомств, а також інших осіб, які мають відповідні обов'язки. Міністр національної безпеки відповідає за поточне управління та підтримку FIOP. Міністр очолює процес перегляду та оновлення Плану щонайменше кожні три роки або після проведення великих навчань, після реальних інцидентів чи після перегляду відповідних повноважень або доктрин.

Припущення щодо планування

При розробці операційних планів ми виходитимемо з наступних припущень:

- Спроможності всієї громади відіграють вирішальну роль у захисті.
- Діяльність в рамках місії захисту відбувається безперервно і може здійснюватися паралельно із запобіганням, пом'якшенням наслідків, реагуванням та відновленням.
- Національна система захисту зосереджується на сталому режимі та посиленому сталому режимі функціонування.
- Ресурси на захист купуються, виділяються та розподіляються через звичайні бюджетні та програмні процеси.
- Відповідальність за захист децентралізована, а повноваження та можливості контролю розподілені між усією спільнотою осіб, організацій, міністерств та відомств, що займаються захистом.

Застосування Національної системи захисту

Урядові, приватні та некомерційні партнери можуть використовувати Національну систему захисту для інформування та узгодження відповідного планування, підготовки, навчань та інших заходів, спрямованих на посилення безпеки всієї громади. Процеси захисту та керівні принципи,що містяться в цій Національній системі, забезпечують структурований підхід, який є гнучким і може бути адаптований до конкретних вимог місії із захисту. Зосередження планування, тренувань і навчань на основних силах і засобах захисту підвищує готовність.

Інтеграція

Інтеграція між п'ятьма зонами дій місії призводить до синхронізації та оперативної сумісності всієї спільноти. Інтеграція досягається між сферами дій місії та всередині них через процеси планування оперативної координації з використанням координаційних структур, описаних у відповідних програмах та пов'язаних з ними планах.

Планування. Суб'єкти захисту координують діяльність з планування в межах усієї громади, щоб забезпечити наявність і доступність необхідних ресурсів у разі потреби, особливо якщо ці ресурси можуть бути використані для відвернення загрози або небезпеки. Під час планування партнери у сфері захисту повинні враховувати наступне:

- Оцінка наявних ресурсів всієї громади об'єднує зусилля та збільшує ефективність, а також зменшує витрати та час надання допомоги. У багатьох юрисдикціях приватні та некомерційні організації укладають угоди про взаємодопомогу.

- Координація та аналіз вимог з використанням загальних припущень щодо планування, оцінок ризиків або сценаріїв допомагає визначити, які інвестиції в сили і засоби найбільш ефективно протистоять загрозі або небезпеці і використовують ресурси найбільш раціонально.

- Врахування темпів виснаження ресурсів в попередніх інцидентах дозволяє визначити потенційні прогалини в ресурсах з плином часу.

Оперативна координація. Створення та підтримка уніфікованих оперативних структур і процесів забезпечує архітектуру для належної інтеграції діяльності, коли це необхідно для одночасного забезпечення основних сил і засобів для запобігання, захисту, пом'якшення наслідків, реагування та відновлення. Спільні тренування та навчання сприяють інтеграції та підтримують єдність зусиль, дозволяючи підрозділу з питань захисту та іншим партнерам у зоні діяльності місії узгодити структури координації та комунікації.

Мережева інтеграція

Мережева інтеграція - це координація та реалізація основних можливостей в рамках місії захисту між різними секторами. На відміну від ієрархічної або командно-адміністративної моделі реалізації діяльності місії, децентралізований характер юрисдикцій, що перетинаються, вимагає мережевої моделі координації. Наприклад, штати інтегрують свою діяльність з місцевими, племінними, територіальними та острівними територіями, а також з федеральними відомствами, які підтримують їх в операціях із захисту. Так само федеральні міністерства і відомства мають власні повноваження щодо захисту, але вони також прагнуть співпрацювати та координуватися з іншими партнерами. Відповідні регіональні організації також включені як важливі елементи мережевої інтеграції; вони можуть забезпечити зв'язок між національним і місцевим рівнями.[34] Крім того, органи влади всіх рівнів беруть участь у спільних навчаннях із захисту для забезпечення інтеграції своєї діяльності.

Партнери у сфері захисту здійснюють інтеграцію наступними способами:

- **Інтеграція через партнерства та обмін інформацією.** Основні можливості захисту координуються між функціональними органами, такими як поліція, пожежна охорона, служби екстреної медичної допомоги, системи охорони здоров'я, громадські роботи, а також підприємства, що займаються питаннями тваринництва та сільського господарства. Основні сили і засоби також координуються на регіональному рівні з сусідніми юрисдикціями, які можуть мати спільний профіль ризиків, ресурси або інформацію і підтримувати один одного в наданні основних сил і засобів захисту. Така інтеграція відбувається між державними установами та елементами приватного сектору, громадськими групами, релігійними організаціями та NGOs на всіх рівнях через партнерство та обмін інформацією.

[34] Прикладами регіональних організацій є згадане вище Партнерство PNWER та Консорціум "Всі небезпеки" (All Hazards Consortium). Консорціум "Всі небезпеки" сприяє регіональній інтеграції між урядами та приватними власниками і операторами інфраструктури, насамперед у середньо атлантичному регіоні Сполучених Штатів.

- **Інтеграція за допомогою фреймворків та планів.** На федеральному рівні інтеграція досягається між п'ятьма зонами діяльності місії шляхом розробки концептуальних засад, FIOP та оперативних планів на рівні міністерств. Зокрема, концептуальні засади усіх зон місії координуються між собою, зосереджуючи увагу на інтеграційних факторах, таких як основні спроможності і час проведення заходів, що перетинаються. Ці фактори також застосовуються при розробці та підтримці оперативних планів FIOP та оперативних планів на рівні федеральних відомств. Використання цих інтегруючих факторів дозволяє партнерам у сфері захисту зрозуміти взаємозв'язки, такі як взаємозалежність і можливості між п'ятьма сферами місії.

Інтеграція науки і технологій

Науково-технічний потенціал та інвестиції мають важливе значення для забезпечення та постійного вдосконалення національної готовності. Уся спільнота повинна розробляти, проводити і вдосконалювати діяльність, спираючись на найкращі наукові дані, методи і науково обґрунтовані дослідження. Співробітництво та інвестиції, що забезпечують світове лідерство в галузі науки і техніки, дадуть змогу отримати передові технології та наукові знання,якими можна буде керуватися в заходах з національної готовності. Крім того, координація зусиль усієї спільноти, в тому числі наукових дослідників, забезпечить відповідність наукових зусиль національній готовності.

Багато основних спроможностей в рамках місії із захисту спираються на надійну, науково обґрунтовану оцінку вразливостей, на стандарти, що враховують ризики, і сучасні інструменти для виявлення та ідентифікації потенційних загроз. Захист критичної інфраструктури, кібербезпека, захист сільського господарства і продовольства, охорона здоров'я, морська безпека і безпека транспорту - всі ці сфери отримують значну користь від науково-технічного прогресу. Наприклад, науково-технічні інвестиції, спрямовані на поглиблення розуміння явищ природної небезпеки, сприяють вдосконаленню стандартів інфраструктури і протоколів морської безпеки. Ці науково-технічні інвестиції включають дослідження з моделювання прибережних і річкових повеней для більш точного прогнозування масштабів і місця виникнення повеней, сильних вітрів і небезпечних морських умов.

Забезпечення довгострокових інвестицій в науку і технології сприяє підвищенню здатності моніторингу і захисту від нових вразливостей. Координація між тими, хто відповідає за місію захисту, і науково-технічними спільнотами та установами США буде необхідною для того, щоб наукові зусилля, освіта і інвестиції були актуальними.

Допоміжні ресурси

Існує ціла низка ресурсів для підтримки місії "Захист". Ці ресурси включають тренінги, навчання та сайти в Інтернеті - такі як CitizenCorps.gov, USA.gov та Ready.gov - які доступні як для державних, так і для недержавних партнерів.

Крім того, існує низка документів і керівних принципів, які підтримують розробку міжвідомчих та інших оперативних планів. Приклади включають, але не обмежуються наступними: Національний план захисту інфраструктури та відповідні галузеві плани; Указ Президента № 13636: Посилення кібербезпеки об'єктів критичної інфраструктури; Указ Президента № 13691: Сприяння кібербезпеці інформації приватного сектору; PPD-21: Безпека та стійкість критичної інфраструктури; HSPD 9: Захист сільського господарства та продовольства США; Президентська директива 46 про національну безпеку: Політика і стратегія США у війні з тероризмом; HSPD 5: Управління внутрішніми інцидентами; Національна стратегія безпеки глобального ланцюга постачання; Федеральна міжвідомча геопросторова концепція операцій; Федеральні директиви щодо безперервності 1 і 2; Циркуляр з питань безперервності 1 і 2; PPD-22: Національні події особливого характеру; Директива Президента США з питань національної безпеки 51/Директива Президента США з питань національної безпеки 20: Національна політика безперервності; і Закон про обмін інформацією з кібербезпеки від 2015 року.

Висновок

Національна система захисту покликана сприяти координації діяльності місії захисту перед обличчям все більш динамічних і мінливих ризиків. Спільна відповідальність за місію захисту поширюється від

індивідуального рівня та рівня громади до місцевих урядів, урядів штатів, племен, територій та острівних територій, а також федерального уряду. Децентралізація та адаптивність діяльності місії захисту відповідає характеру ризиків, а забезпечення національного потенціалу захисту спирається на мережу координаційних структур, що охоплює всю країну.

Впроваджуючи Національну систему захисту з метою підвищення національної готовності,партнери виробляють спільне розуміння ризиків, одночасно нарощуючи майбутній потенціал і можливості. Об'єднуючі принципи і доктрини, що містяться в цій Національній системі, будуть регулярно переглядатися з метою оцінки відповідності існуючим і новим політикам, умовам, що змінюються, і досвіду, отриманого в результаті її використання. Наступні огляди будуть проводитися з метою оцінки ефективності цієї Національної системи на чотирирічній основі.

Міністерство національної безпеки координує і контролює процес перегляду і підтримки Національної системи захисту. Процес перегляду включає розробку або оновлення будь-яких документів, необхідних для реалізації можливостей. Суттєві оновлення цього документу будуть перевірятися в рамках міжвідомчого процесу перегляду на федеральному рівні на рівні вищого керівництва. Ця Національна система буде переглянута з метою досягнення наступних цілей:

- Оцінювати та оновлювати інформацію про основні сили і засоби на підтримку цілей і завдань захисту.
- Переконатись, що вона адекватно відображає організацію відповідальних осіб.
- Переконатись, що вона узгоджується з іншими чотирма сферами місії.
- Оновлення процесів на основі змін у національному середовищі загроз/небезпек.
- Враховувати отримані уроки та ефективні практики з повсякденних операцій, навчань, а також реальних інцидентів.
- Відображати прогрес у виконанні країною основних завдань місії захисту, необхідність виконання нових законів, указів і директив Президента, а також стратегічні зміни в національних пріоритетах і керівних принципах, критично важливих завданнях або національних силах і засобах.

Робота над безпекою та стійкістю в Америці триває, і вона повинна розвиватися та адаптуватися до мінливих загроз і небезпек, щоб забезпечити стійкість. Хоча країна стала безпечнішою, сильнішою та краще підготовленою, ніж десять років тому, прагнення суспільства захистити країну від найбільших ризиків, з якими вона стикається зараз і на десятиліття вперед, залишається рішучим. Об'єднавши зараз усю громаду для підтримки колективних та інтегрованих дій, необхідних для задоволення спільних майбутніх потреб, країна продовжить покращувати свою готовність до будь-яких викликів, що постануть перед нею.