

***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.Ðu1055?осилання на офіційний оригінал документа:***

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf>

Національний міжсекторальний форум

План дій на 2021-2023 роки для критичної інфраструктури

ПОБУДОВА **БЕЗПЕЧНОЇ** ТА **СТІЙКОЇ КАНАДИ**





© Її Величність Королева по праву Канади, в особі Міністра громадської безпеки та готовності до надзвичайних ситуацій, 2021.

Анекс. No: PS4-66/2021E-PDF ISBN: 978-0-660-38395-8

# Зміст

Вступ

Досягнення 2018-2020

Ландшафт ризиків : зміни в дорозі

Залучення спільноти : як ми працюємо разом

Заходи Плану дій на 2021-2023 роки

Побудова партнерських відносин

Обмін інформацією та її захист

Впровадження підходу до управління ризиками всіх небезпек

Додатки

A: Роль та обов'язки

B: Сектори критичної інфраструктури та провідні федеральні департаменти/агентства

C: Секторальні мережі та національний міжсекторальний форум

D: Досягнення в рамках акції

План критичної інфраструктури (2018-2020)

E: План дій на 2021-2023 роки: зведена таблиця

F: Ресурси

# Введення

***Національна стратегія критичної*** інфраструктури ( Національна стратегія) визначає підхід Канади до посилення стійкості критичної інфраструктури. Національна стратегія визначає критично важливу інфраструктуру як процеси, системи, об'єкти, технології, мережі, активи та послуги, необхідні для здоров'я, безпеки, безпеки або економічного добробуту канадців та ефективного функціонування уряд. Канадці щодня покладаються на критично важливу інфраструктуру, від інфраструктури, що підтримує транспорт, до харчового та водного секторів. Національна стратегія визначає три основні цілі для посилення стійкості критично важливої інфраструктури: побудова партнерських відносин, обмін та захист інформації, а також практика підходу до ризиків усіх небезпек. З моменту публікації

Національна стратегія на 2010 рік, три допоміжні плани дій (2010-2013; 2014- 2017 рр.; та 2018-2020) були оприлюднені для окреслення конкретних кроків на шляху досягнення цілей, визначених стратегією.

У період з 2018 по 2020 рік також було проведено експертизу Національної стратегії, щоб визначити, чи існує потреба в оновленні загального підходу Канади до стійкості критичної інфраструктури. Висновки експертизи призвели до рекомендації, яка була надана заступнику міністра громадської безпеки для Департаменту розпочати процес оновлення, який тепер відбуватиметься протягом наступних трьох років (2021-2023).

Щоб продовжувати підтримувати просування цілей Національної стратегії до оприлюднення цього оновленого національного підходу до стійкості критичної інфраструктури, Міністерство громадської безпеки Канади (PS) створило  *Національний міжсекторальний форум* 2021-2023  *План дій для критичних*

*Інфраструктура* (План дій). План дій підтверджує зобов'язання уряду Канади тісно співпрацювати з партнерами в секторі критичної інфраструктури, провінціями та територіями для більш безпечної та стійкої Канади. План дій ґрунтується на прогресі, досягнутому завдяки минулі плани дій, визначає нові заходи, засновані на мінливому середовищі загроз, і підтримуватиме спільний підхід для підвищення безпеки та стійкості критичної інфраструктури Канади. План дій продовжує підтримувати тристратегічні цілі, визначені в Національній стратегії підвищення стійкості критичної інфраструктури в Канаді:

* Побудова партнерських відносин;
* Обмін та захист інформації; і
* Впровадження підходу до управління ризиками всіх небезпек.

# Досягнення 2018-2020 років

В рамках *Плану дій* щодо критичної інфраструктури  *Національного міжсекторального форуму на 2018-2020* роки PS завершило експертизу Національної стратегії та загального підходу Канади до критичної інфраструктури. Це сталося через взаємодію з ключовими національними зацікавленими сторонами критичної інфраструктури, включаючи: Національний міжсекторальний форум (NCSF), провідні федеральні департаменти (LFD), Федеральну / провінційну / територіальну (FPT) робочу групу з критичної інфраструктури та обмежені індивідуальні зустрічі з члени громади з питань критичної інфраструктури, а також наукових кіл.

Протягом цього періоду PS продовжувала проводити оцінку ризиків усіх небезпек через Регіональну програму оцінки стійкості (RRAP). Це включало роботу з провінціями та територіями для визначення пріоритетних місць для оцінки, а також визначення та впровадження заходів для збільшення впливу та охоплення RRAP. У період з 2018 по 2020 рік RRAP продовжив роботу над більш широкими регіональними оцінками всіх небезпек за допомогою третього транскордонного проекту RRAP; підтримував високий рейтинг задоволеності власників інфраструктури / операторів; і створив профілі секторів, аналізуючи сукупні дані з оцінок місця.

PS також тісно співпрацювала із зацікавленими сторонами критичної інфраструктури для розширення охоплення своїх механізмів кібер-взаємодії, зокрема через симпозіуми з безпеки Промислової системи управління (ICS). Симпозіуми з безпеки АСУ ТП зібрали власників та операторів критичної інфраструктури Канади для брифінгів щодо останніх загроз, практичного розвитку навичок обробника інцидентів та інформації для підвищення безпеки ICS. PS також запустила серію веб-конференцій, де експерти галузі проводили брифінги на теми, пов'язані з безпекою АСУ ТП. Інавгураційна зустріч досягла потужності і дозволила PS розширити своє охоплення зацікавлених сторін по всій країні.

Міжсекторальні настільні навчання у координації з LFD, провінціями та територіями, муніципалітетами та власниками та операторами критичної інфраструктури також тривали протягом Nexus Vitalis 2019. Ці навчання об'єднали об'єднання об'єктів критичної інфраструктури для моделювання реагування на атаки з усією небезпекою (наприклад, кібератаки), а також для зміцнення нових та існуючих партнерств шляхом обміну інформацією та вирішення спільних проблем. PS завершив серію навчань Nexus Vitalis у трьох різних регіонах (Саскачеван, Британська Колумбія та Атлантична Канада) навесні 2019 року.

Враховуючи , що приватні власники та оператори критичної інфраструктури залежать від важливих подій та стабільної державної інформації, від Уряду

*У 2019 році PS опублікувала книгу «Підвищення стійкості критичної інфраструктури Канади до інсайдерських ризиків». Цей документ надав канадським організаціям критичної інфраструктури рекомендації щодо того, що являє собою інсайдерський ризик та рекомендації щодо моніторингу, реагування та зменшення інсайдерських ризиків.*

Канади був заклик покращити форуми під керівництвом PS (наприклад, засідання NCSF, LFDs, робочої групи FPT для критичної інфраструктури та багатосекторної мережі (MSN) для усунення бар'єрів для інформації, а саме дозволів на безпеку. У відповідь PS та Security Partn почали проводити несекретні панельні дискусії щодо нових загроз та заходів щодо пом'якшення наслідків, які допоможуть покращити загальну ситуаційну обізнаність.

Віртуальний центр аналізу ризиків (VRAC) PS також модифікував розробку та розповсюдження продуктів оцінки впливу для підтримки прийняття рішень та управлінських дій зацікавлених сторін критичної інфраструктури. VRAC надав експертизу та аналіз для виявлення потенційних впливів

руйнівних подій, підтримка покращеного планування, а також швидке реагування та відновлення у разі виникнення інцидентів. Наприклад, під час сезонів повеней та пожеж VRAC підготував звіти, щоб висвітлити, які наслідки може мати кожен сектор та якими можуть бути каскадні наслідки для інших секторів. Ці циклічні продукти були розміщені на інформаційному шлюзі критичної інфраструктури.

І, нарешті, у 2019 році PS опублікувала книгу Enhancing Canada's Critical Infrastructure Resilience to Insider Risk. Цей документ надав канадським організаціям критичної інфраструктури рекомендації щодо того, що являє собою інсайдерський ризик, а також рекомендації щодо моніторингу, реагування та зменшення інсайдерського ризику. Цей посібник допомагає організаціям розробляти свої програми інсайдерських ризиків для захисту від людських і технічних вразливостей, включаючи ті, що пов'язані з їхніми партнерами , постачальниками послуг та партнерами. Документ був високо оцінений як державними, так і приватними партнерами як такий, що містить корисні та обґрунтовані поради у сфері, що викликає зростаючу стурбованість.

Ландшафт ризиків:

# Зміна управління

З нетерпінням чекаємо ще одного десятиліття, світ невизначеності зберігається. Ландшафт ризиків, з якими стикається канадська спільнота критичної інфраструктури, продовжує залишатися складним, включаючи низку екологічних загроз, загроз кібербезпеці, іноземну діяльність, економічний тиск і, перш за все, кризу в галузі охорони здоров'я, яка підкреслила необхідність більшої уваги до готовності та пов'язаних з ними ризиків глобально розподіленими ланцюгами поставок, які підтримують критично важливу інфраструктуру.

Клімат Канади змінюється. Наслідки широкомасштабного потепління очевидні в багатьох частинах Канади і, за прогнозами, посиляться в майбутньому. Ці зрушення все більше впливають на природне значення Канади

навколишнє середовище, економіка та здоров'я канадців. Екстремальна погода Події, такі як повені та пожежі, продовжують загрожувати здатності критичних інфраструктура для надання послуг. Наприклад, сильна хуртовина в 2020 році Викликало Санкт. Івана, Ньюфаундленд і Лабрадор до досвід a Порушення В його Транспорт Системи, Телекомунікації Мереж і просто в- Час поставка Ланцюги.

Цифровізація Системи і процесів, і також здатність дистанційно контролювати операції критичної інфраструктури також продовжують створювати нові виклики Кібербезпека.

У той час як зростаюче впровадження систем цифрової інфраструктури поряд з традиційною фізичною інфраструктурою покращило загальний зв'язок, зв'язок і надання послуг канадцям, використання систем з доступом до Інтернету збільшує ймовірність і масштаб як навмисних, так і ненавмисних збоїв.

Ритаційна інфраструктура Канади залишається цінною мішенню для іноземного втручання, в тому числі з метою навмисних збоїв у роботі служб та крадіжки інтелектуальної власності. Високий рівень взаємозв'язку в секторах критичної інфраструктури Канади створює мультиплікаційний ефект дестабілізації для одного сектора. Компроміс оператора в одному секторі, наприклад, постачальника електроенергії в секторі енергетики та комунальних послуг, може мати каскадні наслідки для інших секторів.

І не забуваймо, що розробка Плану дій (2021-2023) відбувається за безпрецедентних обставин, пов'язаних із поширенням нового коронавірусу (COVID-19), який було оголошено глобальною пандемією

Клімат Канади змінюється. Наслідки широкомасштабного потепління очевидні в багатьох частинах Канади і, за прогнозами, посиляться в майбутньому.

Критично важлива інфраструктура Канади залишається цінною мішенню для іноземного втручання, в тому числі з метою навмисних збоїв у роботі служб та крадіжки інтелектуальної власності.

у березні 2020 року Всесвітньою організацією охорони здоров'я. З початку пандемії власники та оператори критичної інфраструктури Канади зіткнулися з проблемами, оскільки уряди санкціонували закриття несуттєвих підприємств та обмежили рух людей і товарів, а також зберігався дефіцит медичних товарів, включаючи засоби індивідуального захисту.

Пандемія висвітлила різні вразливості критичної інфраструктури, такі як залежність від глобально розподілених ланцюгів поставок товарів першої необхідності. Наприклад, Канада зараз покладається лише на кілька м'ясопереробних підприємств у Канаді та США для постачання м'яса канадцям. Багато з цих об'єктів були змушені тимчасово закритися і зменшити потужності через ризики для здоров'я, тим самим підриваючи нашу продовольчу безпеку. Інше занепокоєння викликає те, що більшість фармацевтичних препаратів Канади надходять з однієї країни, що залишає мало можливостей у разі збоїв. Усі наші сектори критичної інфраструктури залежать від товарів та послуги, вироблені ланцюгами поставок, що базуються по всьому світу, що виходять за межі компетенції Канади, що може становити певні ризики. Пандемія кинула виклик нормам і повинна формувати підхід Канади до стійкості ще довго після розробки вакцин.

Залучення спільноти :

# Як ми працюємо разом

Окрім розгляду поточних та нових небезпек і загроз критично важливій інфраструктурі, План дій враховує зворотний зв'язок, отриманий під час консультацій та численних заходів із залучення. Зовсім недавно PS об'єднала спільноту критичної інфраструктури під час пандемії COVID-19 за допомогою розширеного NCSF (E-NCSF).

NCSF - це консультаційна та інформаційно-просвітницька організація на національному рівні, яка об'єднує лідерів десяти секторів критичної інфраструктури Канади для визначення пріоритетів та обговорення міжгалузевих питань та ініціатив для підвищення стійкості життєво важливих активів та систем Канади. На початку пандемії COVID-19 засідання NCSF були розширені, щоб включити сотні нових учасників у всіх десяти секторах критичної інфраструктури. Цей форум був перейменований на E-NCSF, щоб відрізнити його діяльність від основного NCSF. Громада критичної інфраструктуривикористовувала цей вихід під час подій, що розгорталися на початку пандемії, як засіб надання та отримання цінної інформації, керівництва та планування для забезпечення стійкості, а засідання E-NCSF продовжують проводитися щомісяця, поки ситуація з пандемією продовжуєрозвиватися. Пандемія підтвердила зустрічі багатосекторної мережі, такі як NCSF та E-NCSF, як основний засіб для ефективної співпраці між спільнотою критичної інфраструктури та федеральним урядом.

У лютому 2020 року PS також провів особисте засідання робочої групи FPT з питань критичної інфраструктури та засідання MSN. Ці заходи включали обговорення Національної стратегії віч-на-віч та уроки, отримані із серії вправ Nexus Vitalis. Ці консультації вказали на важливість посилення комплексне реагування на надзвичайні ситуації, одночасно підвищуючи обізнаність про нові загрози та вразливості.

# План заходів на 2021-2023 роки

Наступний розділ окреслює заходи та дії, які підтримують принципи управління ризиками, визначені стратегічними цілями Національної стратегії. Заходи спрямовані на зміцнення стійкості критичної інфраструктури Канади, допомагаючи запобігати, пом'якшувати, готуватися до реагування, реагувати та відновлюватися після збоїв.

Ці заходи покликані сприяти співпраці та обміну інформацією між усіма рівнями уряду, партнерами з приватного сектору та країнами-союзниками з акцентом на реалізації конкретних ініціатив з управління ризиками. Стислий виклад діяльності та пов'язані з ними терміни імплементації можна знайти в Додатку Е.

Визнаючи швидку зміну операційного середовища внаслідок панде-мікрофона COVID-19, заходи та результати Плану дій переглядатимуться щорічно, щоб визначити, чи слід додавати нові види діяльності чи кінцеві результати, чи видаляти існуючі.

ПОБУДОВА ПАРТНЕРСЬКИХ ВІДНОСИН

Зміцнення стійкості критично важливої інфраструктури вимагає спільних зусиль усіх партнерів та зацікавлених сторін. Для побудови ефективних партнерських відносин і досягнення взаємних цілей PS тісно співпрацює з федеральними департаментами і агентствами, провінціями і територіями, приватним сектором і міжнародними партнерами. Наведені нижче заходи та досягнення зосереджені на розбудові, підтримці та посиленні співпраці з усіма партнерами у спільноті критичної інфраструктури, включаючи механізми сприяння співпраці та інформації Шарінг.

## Вирішення міжсекторних питань за допомогою багатосекторних зустрічей

Багатосекторні зустрічі продовжують залишатися ефективним способом обміну інформацією та вирішення міжсекторних питань і проблем. Старші представники з усіх десяти секторів критичної інфраструктури залучаються через NCSF, співголовою якого є заступник міністра PS, і підтримуються обговореннями на оперативному рівні на багатосекторних зустрічах network (MSN), таких як E-NCSF.

На додаток до засідань NCSF та MSN, PS забезпечить керівництво координацією спеціальних міжсекторних зустрічей для вирішення питань, що становлять спільний інтерес.

**Результатів**

* 1. MSN зустрічатися особисто або віртуальноі щорічно. PS забезпечить лідерство В координації додаткових спеціальних Багатосекторних зустрічей

**Хронологія:** Триває

* 1. NCSF зустрічатися особисто або віртуально, а також брати участь у розділі спеціальних телеконференціях. PS координуватиме та організовуватиме всі зустрічі **Хронологія:** Триває
  2. PS для повторної оцінки членства на сайті NCSF та технічного завдання

**Хронологія:** Рік 1

* 1. PS спиратиметься на E-NCSF для зміцнення співпраці між державним та приватним секторами шляхом залучення MSN під час операцій у стані подій та стаціонарних операціях

**Хронологія:** Триває

## Взаємодіяти з провінціями та територіями для зміцнення стійкості критично важливої інфраструктури

PS продовжуватиме співпрацювати з іншими рівнями влади, насамперед через Робочу групу з питань критичної інфраструктури федерального/провінційного/територіального (FPT), займаючись поточнимита новими проблемами, з якими стикаються сектори критичної інфраструктури, включаючи реагування на COVID-19 Зусилля. PS та провінції/території (P/Ts) працюватимуть разом, щоб визначити можливості для P/T використовувати федеральні програми критичної інфраструктури для підтримки юрисдикційних зусиль з підвищення стійкості.

**Результатів**

* 1. PS для координації та головування на засіданнях ФПТ ТАМ ПО.

**Хронологія:** Триває

* 1. РГ ФПТ КІ розробити та впровадити Робочий план для окреслення та спрямування своєї роботи.

**Хронологія:** Триває

* 1. PS взаємодіяти з П/Тс крізь ФПТ ТАМ ВІД для визначення змін, потреб та пріоритетів внаслідок COVID-19

**Хронологія:** Рік 1

* 1. PS для роботи з P/Ts для визначення потреб муніципальних органів влади та визначення можливостей підтримки муніципальних ініціатив

**Хронологія:** Триває

## Продовження співпраці з провідними федеральними департаментами (LFD)

PS продовжуватиме надавати керівництво та підтримку федеральному співтовариству критичної інфраструктури , включаючи його координаційну роль щодо провідної мережі критичної інфраструктури Федерального департаменту (Мережа LFD CI). Ця мережа об'єднує федеральні департаменти / агентства, відповідальні за десять секторів критичної інфраструктури, для підтримки обміну інформацією та співпраці. PS також буде готова тісно співпрацювати з іншими урядовими організаціями, включаючи Канадський центр кібербезпеки (CCCS) та регіональні офіси PS.

**Результатів**

* 1. Мережа LFD CI регулярно зустрічається на рівні директора. PS для головування та координації зустрічей

**Хронологія:** Триває

* 1. PS працюватиме з LFD для зміцнення партнерських відносин у сфері кібербезпеки шляхом продовження підтримки спільноти експертів з кібербезпеки критичної інфраструктури

**Хронологія:** Триває

* 1. PS надасть пряму підтримку міжурядовим зусиллям на підтримку відповіді Канади на COVID-19

**Хронологія:** Триває

* 1. PS для роботи з ЛФД для оновлення профілів секторів та інформаційних листів

**Хронологія:** Триває

## Взаємодіяти з різними міжнародними форумами для вирішення питань критичної інфраструктури

PS продовжить брати участь у ряді міжнародних груп, включаючи «Критичну п'ятірку». Ці міжнародні групи є форумом для обговорення питань стійкості критичної інфраструктури, що становлять взаємний інтерес.

**Результатів**

* 1. PS очолить участь Канади в міжнародних групах для просування спільного підходу до зміцнення стійкості глобально взаємопов'язаних активів і систем та обміну передовим досвідом

**Хронологія:** Триває

* 1. PS для підтримки різних ініціатив Організації економічного співробітництва та розвитку (ОЕСР), пов'язаних з критичною інфраструктурою

**Хронологія:** Триває

## Взаємодіяти із зацікавленими сторонами державного та приватного секторів щодо оновлення стратегії та підходу Канади до критичної інфраструктури

PS використовуватиме існуючі партнерські відносини та створить нові механізми для підтримки оновлення стратегії та підходу Канади до критичної інфраструктури, щоб забезпечити її відображення ширшої критичної ситуації Канади інфраструктурне співтовариство, а також виклики і проблеми , з якими вони зіткнуться в результаті мінливого ландшафту загроз і ризиків.

**Результатів**

5.1 PS створити Робочу групу експертів з критичної інфраструктури (CIEWG), що складатиметься із зацікавлених сторін державного та приватного секторів, науковців та вибраних профільних експертів, які діятимуть як консультативний Орган для процесу оновлення стратегії та підходу Перед критичної інфраструктури

**Хронологія:** Рік 1

ОБМІН ІНФОРМАЦІЄЮ ТА ЇЇ ЗАХИСТ

Обмін та захист інформації є ключовим компонентом зміцнення стійкості спільноти критичної інфраструктури Канади. Своєчасний обмін інформацією всередині та через

Сектори критичної інфраструктури та всі рівні управління необхідні для сприяння ефективному управлінню ризиками. Заходи та результати, описані нижче, підготовлені таким чином, щоб забезпечити зацікавленим сторонам своєчасний доступ до відповідної інформації для підтримки планування та прийняття рішень.

Ці ініціативи мають спільний підхід до оцінки того, який тип інформації виробляється, з ким нею діляться та як нею діляться.

1. **Модернізація та просування інформаційного шлюзу критичної інфраструктури**

PS продовжувати зусилля з модернізації шлюзу CI для задоволення мінливих потреб спільноти критичної інфраструктури, а також сприяти використанню шлюзу CI для збільшення кількості користувачів і відвідувань сайтів.

**Результатів**

* 1. PS модернізує ТАМ Шлюз з метою збільшення функціональності та покращення загального користувацького досвіду **Хронологія:** Триває
  2. P.S. для проведення огляду існуючих публікацій та інструментів для забезпечення їх постійної актуальності

**Хронологія:** Рік 2

* 1. PS буде активно сприяти використанню Шлюз ТАМ для включення більшого регіонального та галузевого представництва

**Хронологія:** Триває

## Розробляти та розповсюджувати продукти оцінки впливу як під час стаціонарного, так і під час подій

PS для надання своєчасної та актуальної інформації партнерам державного та приватного сектору під час стабільних та подійних станів. PS підвищить ситуаційну обізнаність зацікавлених сторін критичної інфраструктури шляхом розробки аналізу стійкості, орієнтованої на критичну інфраструктуру, шляхом розподілу: оцінки загроз та впливу; відповідної інформації про управління надзвичайними ситуаціями та безперервність бізнесу; аналіз залежностей та взаємозалежностей критичної інфраструктури; геопросторові продукти; як мибудемо використовувати відповідну статистичну інформацію.

**Результатів**

* 1. PS для розробки та обміну аналітичними матеріалами та інформаційними продуктами для підтримки дій зацікавлених сторін критичної інфраструктури з управління ризиками

**Хронологія:** Триває

* 1. PS продовжуватиме використовувати дані оцінки RRAP та інші джерела даних для створення звітів про тенденції, оглядів секторів та інших аналітичних продуктів для підтримки партнерів критичної інфраструктури **Хронологія:** Триває
  2. PS співпрацюватиме із зацікавленими сторонами державного та приватного секторів для розширення охоплення надійних інформаційних продуктів для партнерів критичної інфраструктури та громад у Канаді **Хронологія:** триває

ВПРОВАДЖЕННЯ ПІДХОДУ ДО УПРАВЛІННЯ РИЗИКАМИ ВСІХ НЕБЕЗПЕК

Найкращий спосіб мінімізувати вплив на критично важливу інфраструктуру, громадян, економічне процвітання та безпеку – це запровадити підхід до всіх небезпек для усунення ризиків та взаємозалежностей критичної інфраструктури. Національна стратегія сприяє застосуванню ризик-менеджменту та обґрунтованого планування безперервності бізнесу для посилення стійкості критично важливої інфраструктури. Застосовуючи ризик-орієнтований підхід, уряди та промисловість можуть оцінити

ймовірність і вплив потенційного порушення і розподіл ресурсів на основі їх толерантності до ризику. Маючи це на увазі, PS та інші федеральні департаменти та агентства тісно співпрацюють з іншими рівнями уряду та зацікавленими сторонами критичної інфраструктури, щоб отримати більш глибоке розуміння цих ризиків. Заходи та результати, перелічені нижче, спрямовані на те, щоб забезпечити спільноту критичної інфраструктури Канади інструментами та інформацією, необхідними для прийняття значних ризиків Управлінські дії з точки зору всіх небезпек.

## Підтримка секторальних та міжсекторальних навчань з метою посилення готовності та спроможностей реагування критично важливої інфраструктури Канади

Вправи є ефективним засобом тестування, оцінки та покращення управління подіями у спільноті критичної інфраструктури . PS продовжує працювати у співпраці з LFD, P/Ts, власниками та операторами критичної інфраструктури для підтримки секторальних та міжсекторальних навчань з метою посилення здатності зацікавлених сторін пом'якшувати наслідки руйнівних подій.

**Результатів**

* 1. PS продовжуватиме надавати підтримку секторальним і міжсекторальним навчанням, орієнтованим на фізичну та кібернетичну сферу, у співпраці з LFD, P/Ts та компаніями критичної інфраструктури та Операторів

**Хронологія:** Триває

* 1. PS для обміну спостереженнями та найкращими Практики навчань та заходів

**Хронологія:** Триває

* 1. PS вивчить можливості для різних Моделі і Платформ Доставка вправ

**Хронологія:** Триває

## Використовуйте існуючі інструменти оцінки для оцінки стійкості критичної інфраструктури

PS працюватиме з відповідними зацікавленими сторонами критичної інфраструктури, включаючи P/Ts, місцеву владу та інших партнерів, з метою оцінки стійкості критичної інфраструктури Канади. Ця робота в першу чергу буде вестися через РРПД.

PS у співпраці з CCCS надає Канадський інструмент кібербезпеки для організацій для самооцінки своєї організаційної стійкості і захисту кіберсектору. Інструмент надає поради та вказівки, орієнтовані на кібер, і представляє результати як порівняльний огляд стану кібербезпеки організації. Це допоможе PS та CCCS у розробці наступного покоління продуктів та послуг для задоволення потреб кібербезпеки спільноти критичної інфраструктури Канади.

**Результатів**

* 1. PS продовжить використовувати інструмент стійкості критичної інфраструктури (CIRT) та мультимедійний інструмент критичної інфраструктури (CIMT ) для проведення оцінок РПД по всій Канаді

**Хронологія:** Триває

* 1. PS продовжить проводити Канадський огляд кіберстійкості (CCRR) по всій Канаді, включаючи використання інструменту аналізу стійкості мережевої безпеки (NSRA)

**Хронологія:** Триває

* 1. PS для проведення досліджень додаткових інструментів оцінки та методів проведення

**Хронологія:** Рік 2

* 1. PS Доставити канадський інструмент кібербезпеки спільноті критичної інфраструктури

**Хронологія:** Триває

## Підвищити безпеку систем промислового контролю для спільноти критичної інфраструктури Канади

Для усунення ризиків, пов'язаних з конвергенцією систем фізичної та кіберкритично важливої інфраструктури, PS продовжуватиме проводити тренінги з питань захисту АСУ ТП та об'єднувати зацікавлені сторони для обміну своїми знаннями та досвідом щодо пом'якшення кіберзагроз. PS буде тісно співпрацювати з LFD та власниками та операторами критичної інфраструктури, щоб розширити своє охоплення в десяти секторах критичної інфраструктури.

**Результатів**

* 1. PS проводити щорічні симпозіуми з безпеки АСУ ТП особисто або віртуально

**Хронологія:** Триває

* 1. PS Провели технічні семінари з безпеки АСУ ТП для спільноти критичної інфраструктури

**Хронологія:** Триває

* 1. PS для проведення вебінарів з безпеки ICS для розширення охоплення та кількості осіб, які можуть взяти участь

**Хронологія:** Триває

## Оновити стратегію та підхід Канади до стійкості критичної інфраструктури

PS здійснить проект з оновлення стратегії та підходу Канади до критичної інфраструктури, який включатиме широкі дослідження, аналіз та консультації в ширшій спільноті критичної інфраструктури. Цей проект оновлення буде шукатифундаментальні визначення та концепції; ролі та обов'язки; законодавчі органи та нормативні акти, а також загальне виконання програми. Результатом стане стратегія та підхід до спрямування зусиль щодо стійкості критично важливої інфраструктури у швидко мінливому середовищі загроз та ризиків.

**Результатів**

11.1 PS тісно співпрацювати з P/T, федеральним співтовариством та Приватний Сектор для розробки нової стратегії та підходу Перед стійкості критичної інфраструктури

**Хронологія:** Рік 3

## Використовувати механізм відстеження для оцінки прогресу виконання заходів у Плані дій

PS відстежуватиме хід виконання заходів, зазначених у цьому Плані дій. Він відкоригує елементи, якщо це необхідно, щоб забезпечити їх досягнення своєї основної мети. З цією метою PS розробить інструмент відстеження, який буде оновлюватися і щорічно звітуватися вищому керівництву NCSF і PS.

**Результатів**

12.1 PS розробити механізм забезпечення відстеження прогресу виконання пунктів дій та регулярного звітування про досягнення цілей

**Хронологія:** рік 1 (і триває)

Додаток А:

# Ролі та обов'язки

|  |  |  |
| --- | --- | --- |
| **Актор** | **Роль** | **Обов'язки** |
| Федеральний уряд | Вести федеральну діяльність | * Просувати спільний федеральний, провінційний та територіальний підхід до зміцнення стійкості критично важливої інфраструктури * Співпрацювати з провінційними та територіальними урядами для досягнення цілей Стратегії * Співпрацюйте з національними асоціаціями * Співпрацювати з власниками та операторами критичної інфраструктури в рамках федерального мандату в консультації з провінціями та територіями |
| Провінційні / територіальні уряди | Керувати провінційними / територіальними заходами | * Просувати спільний федеральний, провінційний та територіальний підхід до зміцнення стійкості критично важливої інфраструктури * Співпрацювати з федеральними, провінційними та територіальними урядами для досягнення цілей Стратегії * Координація діяльності зі своїми зацікавленими сторонами, включаючи муніципалітети або органи місцевого самоврядування , де це застосовується, асоціаціями та власниками та операторами критичної інфраструктури |
| Власники/оператори критичної інфраструктури | Спільне управління ризиками, пов'язаними з їх критично важливою інфраструктурою | * Управляти ризиками для власної критичної інфраструктури * Брати участь у заходах з ідентифікації, оцінки, запобігання, пом'якшення наслідків, готовності, реагування та відновлення критичної інфраструктури |

Джерело: *План дій щодо критичної інфраструктури* (2010)

Додаток Б:

# Сектори критичної інфраструктури

**та провідні федеральні департаменти / агентства**

|  |  |
| --- | --- |
| **Сектор** | **Галузевий федеральний департамент/агентство** |
| Енергетика та комунальні послуги | Природні ресурси Канади |
| Інформаційно-комунікаційні технології | Інновації, наука та економічний розвиток Канади |
| Фінанси | Фінанси Канади |
| Здоров’я | Агентство охорони здоров'я Канади |
| Харчування | Сільське господарство та агропродовольча Канада |
| Вода | Навколишнє середовище та зміна клімату Канади |
| Транспорт | Транспорт Канади |
| Безпеки | Громадська безпека Канади |
| Уряд | Громадська безпека Канади |
| Виробництва | Міністерство інновацій, науки та економічного розвитку Канади, Міністерство національної оборони |

Джерело: *План дій щодо критичної інфраструктури* (2010)

Додаток С:

# Секторальні мережі та Національний міжсекторальний форум

Виробництва

Уряд

Безпеки

Транспорт

Вода

Харчування

Здоров’я

Фінанси

Енергетика та комунальні послуги

**Національний міжсекторальний Форум**

Членство: приватний сектор, уряди (федеральні, провінційні, територіальні)

Інформаційно-комунікаційні технології

Джерело: *Національна стратегія критичної інфраструктури* (2010)

Ця діаграма окреслює членство в NCSF, яке включає представництво від приватного сектору та федеральних, провінційних та територіальних урядів. Він показує десять секторів: енергетика та комунальні послуги, фінанси, продовольство, транспорт, уряд, інформаційні та комунікаційні технології, охорона здоров'я, вода, безпека та виробництво.

Додаток D:

# Досягнення в рамках Плану дій Національного міжсекторального форуму з розвитку критичної інфраструктури (2018-2020)

ПОБУДОВА ТА ЗМІЦНЕННЯ ПАРТНЕРСЬКИХ ВІДНОСИН

|  |  |
| --- | --- |
| **Кінцевий результат** | **Поточний статус** |
| Вирішення міжсекторних питань за допомогою багатосекторних зустрічей | Завершено (і триває) |
| Взаємодіяти з провінціями та територіями для зміцнення стійкості критично важливої інфраструктури | Завершено (і триває) |
| Постійна співпраця з провідними федеральними департаментами | Завершено (і триває) |
| Розширення регіонального охоплення програм критичної інфраструктури | Завершено (і триває) |
| Взаємодіяти з різними міжнародними форумами для вирішення питань критичної інфраструктури | Завершено (і триває) |

ОБМІН ІНФОРМАЦІЄЮ ТА ЗАХИСТ ЇЇ

|  |  |
| --- | --- |
| **Кінцевий результат** | **Поточний статус** |
| Модернізація та просування інформаційного шлюзу критичної інфраструктури | Завершено (і триває) |
| Проведіть екологічне сканування щодо обміну інформацією | Поточні |
| Розробка та розповсюдження інформації про ризики під час стаціонарного стану та під час руйнівних подій | Завершено (і триває) |
| Підтримка отримання дозволів на безпеку серед зацікавлених сторін приватного сектору | Завершено (і триває) |

ВПРОВАДЖУВАТИ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ ВСІХ НЕБЕЗПЕК

|  |  |
| --- | --- |
| **Кінцевий результат** | **Поточний статус** |
| Підвищення впливу оцінок стійкості | Завершено (і триває) |
| Впровадження ризик-орієнтованого підходу для визначення ключових активів та інфраструктури , що мають важливе значення | Завершено (і триває) |
| Визначення шляхів підтримки спільноти критичної інфраструктури у вжитті заходів для усунення ризиків | Поточні |
| Проведення міжсекторальних навчань для посилення готовності та реагування | Завершено (і триває) |
| Оцініть стан десяти мереж сектору критичної інфраструктури | Завершено (і триває) |
| Підтримка спільноти у вирішенні ризиків, пов'язаних із конвергенцією систем фізичної та кіберкритичної інфраструктури | Завершено (і триває) |
| Вивчити Національну стратегію критичної інфраструктури (2010), щоб визначити, чи є потреба в оновленні загального підходу Канади до стійкості критичної інфраструктури | Завершено |
| Розробити механізм відстеження для оцінки прогресу виконання заходів у Плані дій | Завершено |

Додаток Е:

# План дій на 2021-2023 роки: зведена таблиця

ПОБУДОВА ТА ЗМІЦНЕННЯ ПАРТНЕРСЬКИХ ВІДНОСИН

|  |  |
| --- | --- |
| **Кінцевий результат** | **Життєпис** |
| Вирішення міжсекторних питань за допомогою багатосекторних зустрічей | Поточні |
| Взаємодіяти з провінціями та територіями для зміцнення стійкості критично важливої інфраструктури | Поточні |
| Продовження співпраці з провідними федеральними департаментами (LFD) | Поточні |
| Взаємодіяти з різними міжнародними форумами для вирішення питань критичної інфраструктури | Поточні |
| Взаємодіяти із зацікавленими сторонами державного та приватного секторів щодо оновлення стратегії та підходу Канади до критичної інфраструктури | Поточні |

ОБМІН ІНФОРМАЦІЄЮ ТА ЗАХИСТ ЇЇ

|  |  |
| --- | --- |
| **Кінцевий результат** | **Життєпис** |
| Модернізація та просування інформаційного шлюзу критичної інфраструктури (CI Gateway) | Поточні |
| Розробляти та розповсюджувати продукти оцінки впливу як під час стаціонарного, так і під час подій | Поточні |

ВПРОВАДЖЕННЯ ПІДХОДУ ДО УПРАВЛІННЯ РИЗИКАМИ ВСІХ НЕБЕЗПЕК

**Терміни** кінцевих результатів

Підтримка секторальних та міжсекторальних навчань з метою посилення готовності та спроможностей реагування критично важливої інфраструктури Канади

Поточні

Використовуйте існуючі інструменти оцінки для оцінки стійкості критичної інфраструктури Триває

Підвищити безпеку систем промислового контролю для спільноти критичної інфраструктури Канади

Поточні

Оновити стратегію та підхід Канади Перед стійкості критичної інфраструктури Рік 3

Використовувати механізм відстеження для оцінки прогресу виконання заходів у Плані дій , що триває

Додаток F:

# Ресурси

Наступні веб-сайти містять корисну інформацію щодо стійкості критичної інфраструктури Канади :

### Національна стратегія критичної інфраструктури

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>

### Громадська безпека Канади/Критична інфраструктура

<https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx>

### Канадський інформаційний шлюз критичної інфраструктури

<https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx>

### Підвищення стійкості критичної інфраструктури Канади до інсайдерських ризиків

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx>

### Королівська канадська кінна поліція

<https://www.rcmp-grc.gc.ca/en>

### Канадська служба безпеки розвідки

<https://www.canada.ca/en/security-intelligence-service.html>

### Канадський центр кібербезпеки

<https://cyber.gc.ca/en/>

### Національна стратегія кібербезпеки

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx>

### Підвищення стійкості до тероризму: антитерористична стратегія Канади

<https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-trrrsm-strtg-en.aspx>

### Канадська база даних катастроф

<https://www.publicsafety.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-en.aspx>

### Стратегія управління надзвичайними ситуаціями для Канади

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx>