





неофіційний переклад

Додатковий інструмент: Впровадження підходу до управління ризиками критичної інфраструктури

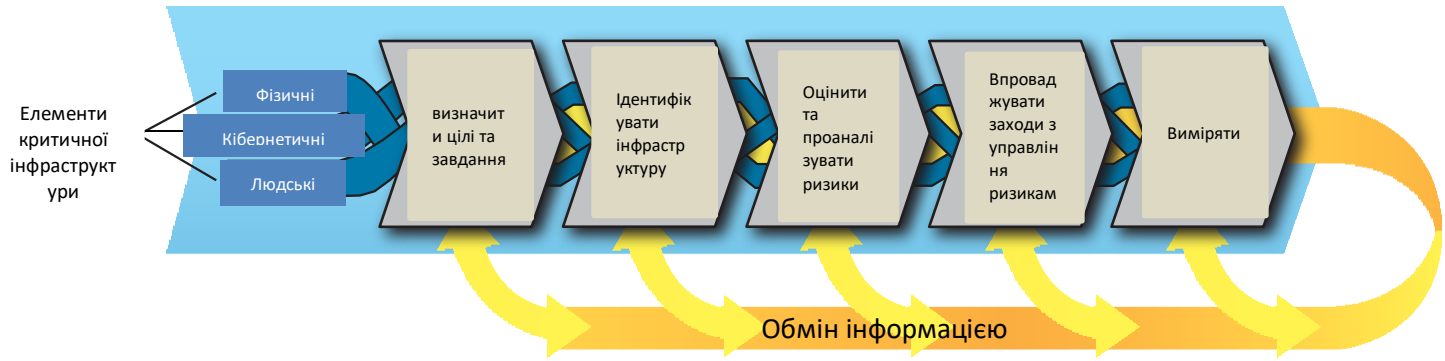
Посилання на офіційний оригінал документа:
https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

Впровадження підходу до управління ризиками критичної інфраструктури

Ризик визначається як потенційна можливість небажаного результату в результаті інциденту, події або явища, що визначається його ймовірністю та пов'язаними з ним наслідками. На нього впливають характер і величина загрози або небезпеки, вразливість до цієї загрози або небезпеки, а також наслідки, які можуть виникнути в результаті. Інформація про ризики дозволяє партнерам, від власників, операторів об'єктів до федеральних агентств, визначати пріоритети в управлінні ризиками.

У цьому Додатковому інструменті описано ефективний підхід до управління ризиками критичної інфраструктури, який підтримує структуру управління ризиками, зображену на Рисунку 1. Ця система дозволяє інтегрувати стратегії, можливості та структури управління для прийняття рішень щодо критично важливої інфраструктури країни з урахуванням ризиків. Підхід до управління ризиками критичної інфраструктури, описаний у цьому Додатковому інструменті, можна застосовувати до всіх загроз і небезпек, включаючи кіберінциденти, стихійні лиха, техногенні загрози безпеці і терористичні акти, хоча для розуміння кожної з них може використовуватися різна інформація і методології.

Рисунок 1: Структура управління ризиками критичної інфраструктури



Крім того, підхід до управління ризиками критичної інфраструктури доповнює і підтримує процес ідентифікації загроз і небезпек та оцінки ризиків (THIRA), що здійснюється регіональними, штатними та міськими органами влади. Процес THIRA передбачає виявлення загроз і небезпек, їх вплив на громаду, а також визначення найкращих способів пом'якшення цих загроз і небезпек, виходячи з поточних можливостей і потреб у ресурсах. Цей процес узгоджується з етапами системи управління ризиками критичної інфраструктури, як описано у відповідних розділах цього Додаткового інструменту. Процес THIRA підтримується Стратегічною національною оцінкою ризиків (Strategic National Risk Assessment (SNRA)), яка аналізує найбільші ризики країни. Взяті разом, THIRA, SNRA та більш спеціалізовані методології оцінки ризиків (такі як оцінки ризиків для окремих секторів та інших об'єктів критичної інфраструктури), надають інтегровану картину національних ризиків, що допомагає досягти Цілі національної готовності - побудувати більш безпечну та стійку державу.

Багато урядових і промислових партнерів використовують інші моделі управління ризиками, які можуть бути більш детальними і пристосовані до конкретних потреб. Система управління ризиками критичної інфраструктури не має на меті замінити моделі чи процеси, що вже використовуються. Вона радше підтримує загальний, об'єднуючий підхід до управління ризиками, який всі партнери у сфері критичної інфраструктури можуть використовувати, співвідносити і узгоджувати зі своїми власними моделями управління ризиками і діяльністю.

Підхід до управління ризиками критичної інфраструктури може бути адаптований і застосовуватися на рівні активів, систем, мереж або функцій, залежно від характеристик рішень, які він покликаний підтримувати, і характеру інфраструктури. Секторам та організаціям, які в першу чергу залежать від основних активів та фізичних об'єктів, може виявитися найбільш доречним висхідний підхід, що передбачає оцінку ризиків за кожним активом. Для таких секторів, як комунікації, інформаційні технології, харчова промисловість і сільське господарство, з доступними і розподіленими системами, може виявитися більш ефективним низхідний підхід забезпечення безперервності бізнесу, який використовує оцінку ризиків, зосереджену на взаємозалежності мереж і систем.

Описаний нижче підхід до управління ризиками критичної інфраструктури включає наступні заходи:

- **Встановити цілі та завдання:** Визначити конкретні результати, цілі, кінцеві точки або цільові показники ефективності, які в сукупності описують ефективну та бажану позицію управління ризиками.
- **Ідентифікувати інфраструктуру:** Ідентифікувати активи, системи та мережі, які сприяють критично важливим функціям, та зібрати інформацію, необхідну для управління ризиками, включаючи аналіз залежностей і взаємозалежностей.

- **Оцінити та проаналізувати ризики:** Провести оцінку ризиків, беручи до уваги потенційні прямі та непрямі наслідки інциденту, відомі вразливості, а також загальну або конкретну інформацію про загрози.
- **Впровадити заходи з управління ризиками: Прийняти** рішення та впровадити підходи до управління ризиками, щоб контролювати, визначити прийнятними, передавати ризики стороні, яка здатна краще їх контролювати, або уникати ризиків. Підходи можуть включати запобігання, захист, пом'якшення, реагування та відновлення.
- **Вимірювання ефективності:** Використання метрик та інших процедур вимірювання прогресу та оцінки ефективності зусиль, спрямованих на забезпечення та посилення стійкості критичної інфраструктури.

Цей підхід забезпечує інтегрований і безперервний процес із зворотним зв'язком та ітеративними кроками. Він дає змогу особам, відповідальним за прийняття рішень у сфері критичної інфраструктури, відстежувати прогрес і впроваджувати заходи, спрямовані на підвищення безпеки та стійкості критичної інфраструктури з плином часу. Фізичні, кібернетичні та людські елементи критичної інфраструктури повинні розглядатися як частина кожного аспекту підходів до управління ризиками.

1. Встановити цілі та завдання

Цілі та завдання, ймовірно, будуть відрізнятися в різних секторах і організаціях залежно від ландшафту ризиків, операційного середовища та складу конкретної галузі, ресурсу або іншого аспекту критичної інфраструктури. На національному рівні загальною метою управління ризиками критичної інфраструктури є підвищення рівня безпеки та стійкості, що досягається шляхом впровадження цілеспрямованих заходів з управління ризиками в межах і між секторами та рівнями державного управління.

Національний план встановлює наступні цілі для національних зусиль з посилення безпеки та стійкості критичної інфраструктури:

- Оцінювати та аналізувати загрози, вразливості та наслідки для критичної інфраструктури з метою інформування про заходи з управління ризиками;
- Захищати критично важливу інфраструктуру від людських, фізичних та кіберзагроз за допомогою постійних зусиль зі зниження ризиків, враховуючи при цьому витрати та вигоду від інвестицій у безпеку;
- Підвищувати стійкість критичної інфраструктури шляхом мінімізації негативних наслідків інцидентів за допомогою завчасного планування та пом'якшення наслідків, а також ефективного

реагування для порятунку життів і забезпечення швидкого відновлення життєво важливих послуг;

- Обмін практичною та актуальною інформацією серед спільноти критичної інфраструктури для підвищення обізнаності та прийняття рішень з урахуванням ризиків;
- Сприяння навчанню та адаптації під час і після тренувальних вправ та реальних інцидентів. Підхід

до управління ризиками критичної інфраструктури сприяє досягненню наступних цілей:

- Сприяння розробці профілів ризиків на національному рівні, на рівні штатів, регіонів і секторів, які ляжуть в основу Щорічного звіту про безпеку та стійкість національної критичної інфраструктури. Ці профілі ризиків окреслюють найбільші ризики, з якими стикаються різні сектори та географічні регіони та вказують на проблеми, які є спільними для них та є важливими для урядового фокусу на критичній інфраструктурі. Крім того, у цих профілях відображаються можливості для ініціатив на рівні секторів, штатів та регіонів.
- Надання можливості спільноті ОКІ визначати найкращі шляхи дій для зменшення потенційних наслідків, загроз та/або вразливостей, що, в свою чергу, зменшить ризики. Деякі варіанти включають заохочення добровільного впровадження цілеспрямованих стратегій управління ризиками (наприклад, через державно-приватне партнерство), застосування стандартів і найкращих практик, реалізацію політики і програм, пов'язаних з економічним стимулюванням, а також проведення додаткового обміну інформацією, якщо це доцільно.
- Інформування про визначення варіантів управління ризиками та розподілу ресурсів, ніж визначення вимог до власників та операторів критичної інфраструктури.

З точки зору сектору або юрисдикції, цілі безпеки та стійкості критичної інфраструктури та їхні допоміжні цілі повинні:

- Розглядати окремі активи, системи, мережі, функції, операційні процеси, бізнес-середовища та підходи до управління ризиками;
- Визначати позицію в управлінні ризиками, яку партнери в сфері критичної інфраструктури прагнуть досягти індивідуально або колективно;
- Висловити цю позицію в термінах цілей і результатів, яких прагнуть досягти.

Взяті разом, ці цілі та завдання є орієнтиром для всіх рівнів влади та приватного сектору при розробці програм та заходів з управління ризиками для задоволення потреб у забезпеченні безпеки та стійкості критичної інфраструктури.

2. Ідентифікувати інфраструктуру

Партнери у сфері критичної інфраструктури розглядають критичність по-різному, виходячи з їхніх унікальних обставин, операційних моделей та пов'язаних з ними ризиків. Партнери - як державні, так і приватні – ідентифікують як об'єкти критичної інфраструктури ті, які вони вважають важливими для своєї діяльності та зусиль, спрямованих на покращення і посилення безпеки та стійкості. Федеральний уряд співпрацює з партнерами, щоб визначити, які активи, системи та мережі мають національне значення, а також визначити ті, які є важливими для їхньої подальшої діяльності. Деякі сектори визначають регіональну, штатну та місцеву критичну інфраструктуру як спільну діяльність між урядом і промисловими партнерами. Власники та оператори приватного сектору можуть визначати додаткову інфраструктуру, яка необхідна для забезпечення функціонування їхнього бізнесу та надання товарів і послуг своїм клієнтам. Аналогічно, штатні, місцеві, племінні та територіальні органи влади (SLTT) можуть визначити ті активи, системи та мережі, які мають вирішальне значення для їхньої безперервної діяльностіз метою забезпечення громадського здоров'я та безпеки і надання основних послуг.

Національна програма пріоритизації критичної інфраструктури (NCIPP) Міністерства національної безпеки США визначає об'єкти критичної інфраструктури національного значення для підтримки прийняття рішень федеральним урядом та його партнерами у сфері критичної інфраструктури з урахуванням ризиків. Критично важливі активи, системи та мережі, визначені в рамках цього процесу, включають в себе ті, які в разі руйнування або порушення роботи можуть спричинити значні людські жертви, значні економічні збитки або широкомасштабні та довгострокові наслідки для національного добробуту. NCIPP ідентифікує, збирає та визначає пріоритетність інформації про критичну інфраструктуру, що надходить від шататів, секторів критичної інфраструктури та інших партнерів у сфері національної безпеки по всій країні. У ньому використовується вдосконалене програмне забезпечення для збору даних про інфраструктуру, який надає можливість вводити дані протягом року.

Дані, зібрані через NCIPP, складають основу Національного реєстру, який включає активи, системи та мережі, що мають національне значення, а також ті, що можуть не мати значення на національному рівні, але, тим не менш, є важливими для безпеки та стійкості критичної інфраструктури на штатному, місцевому чи регіональному рівнях, а також для забезпечення національної готовності до надзвичайних ситуацій. Національний реєстр включає інформацію про стихійні лиха, промислові аварії та інші інциденти. Партнери у сфері критичної інфраструктури працюють разом, щоб забезпечити точність, актуальність і безпеку даних у Національному реєстрі.

Партнери федерального уряду, включаючи секторальні агентства (SSA), працюють з власниками та операторами критично важливої інфраструктури, а також суб'єктами SLTT над створенням та

оновленням існуючих реєстрів на штатному та місцевому рівнях, які мають регіональне та місцеве значення.

Кіберінфраструктура

Національний план розглядає безпеку та стійкість кібер-елементів критичної інфраструктури комплексно, а не як окремий аспект. Під час процесу оцінки ризиків компоненти кіберсистеми повинні бути ідентифіковані окремо або включені як кібер-елемент більшого активу, системи чи мережі, з якими вони пов'язані. Процес ідентифікації повинен включати інформацію про міжнародну кіберінфраструктуру з транскордонними наслідками, взаємозалежностями або міжсекторальними наслідками.

Елементи кіберсистем, які існують у більшості, якщо не у всіх, секторах, включають бізнес-системи, системи керування, системи контролю доступу та системи попередження та сповіщення. Інтернет був визначений як ключовий ресурс, який складається з національних та міжнародних активів у секторах інформаційних технологій та зв'язку; потреба в доступі до інформації та залежність від неї є загальною для всіх секторів.

Міністерство національної безпеки допомагає секторальним агентствам та іншим партнерам з критичної інфраструктури виявляти кібер-активи, системи та мережі, в тому числі ті, що охоплюють кілька секторів. Кілька секторів розробили функціональний підхід до ідентифікації критично важливої кіберзалежної інфраструктури. Підхід до ідентифікації кіберзалежної інфраструктури[2] базується на трьох етапах, які включають:

- Визначення критеріїв "катастрофічного" впливу в усіх секторах;
- Оцінка попередніх зусиль сектору, щоб визначити, як можна використати критерії "катастрофічного" впливу для виявлення критично важливої кіберзалежної інфраструктури, що перебуває під найбільшим ризиком;
- Застосування функціонального підходу для визначення кіберзалежної інфраструктури та її впливу на сектор.

Крім того, DHS у співпраці з іншими партнерами з критичної інфраструктури надає міжсекторальні кібер-методології, які дозволяють секторам ідентифікувати кібер-активи, системи та мережі, що можуть мати значні наслідки на національному рівні в разі їх знищення, виведення з ладу або несанкціонованого використання. Ці методології також характеризують наскільки сектори залежать від кіберсистем для забезпечення своєї бізнес- та операційної функціональності.

3. Оцінити та проаналізувати ризики

Ризики національній безпеці можна оцінити з точки зору їхньої ймовірності та потенційних наслідків. Узгоджені визначення, сценарії, припущення, метрики та процеси оцінки ризиків

можуть створити єдине розуміння між партнерами щодо оцінки ризиків. Підхід до управління ризиками підтримує стратегію оцінювання, результатом якої є обґрунтовані, засновані на сценаріях оцінки наслідків і вразливостей, а також оцінку ймовірності того, що припущена загроза або небезпека відбудуться.

Як зазначено у вступі до цього Додаткового інструменту, важливо думати про ризик як про такий, що залежить від характеру та масштабу загрози або небезпеки, вразливості до цієї загрози або небезпеки та наслідків, які можуть виникнути в результаті.

- **Загроза:** Природне або техногенне явище, особа, організація або дія, що має або вказує на потенційну можливість завдати шкоди життю, інформації, діяльності, навколишньому середовищу та/або майну. Для оцінки ризику, який пов'язаний з ненавмисною небезпекою, загроза зазвичай оцінюється на основі ймовірності того, що сама небезпека виникне. Навмисна загроза зазвичай оцінюється як ймовірність спроби нападу з боку зловмисника. У випадку навмисно ворожих суб'єктів і дій, як для фізичних, так і для кібернетичних сфер, загроза оцінюється на основі намірів і можливостей зловмисника.
- **Вразливість:** Фізична характеристика або оперативна властивість може зробити об'єкт вразливим до використання або вразливим до певної загрози або небезпеки. При розрахунку ризику навмисної загрози загальним показником вразливості є ймовірність того, що атака буде успішною, за умови, що вона була здійснена.
- **Наслідок:** Ефект події, інциденту або явища. Він відображає рівень, тривалість і характер втрат, спричинених інцидентом. Потенційні наслідки можуть включати впливи на громадське здоров'я та безпеку (тобто, втрата життя та захворюваність), економічні (прямі та непрямі), психологічні та управлінські/місійні впливи.

Оцінка ризиків критичної інфраструктури може враховувати кожен з цих факторів,але не обов'язково у кількісній формі. Аналітики повинні бути дуже обережними під час оцінки ризиків, щоб належним чином врахувати взаємозалежності та будь-які зв'язки між тим, як розраховані загрози та вразливості, щоб забезпечити правильність та обґрунтованість результатів.

Оцінка ризиків критичної інфраструктури

Оцінка ризиків проводиться партнерами у сфері критичної інфраструктури для задоволення власних потреб у прийнятті рішень з використанням широкого спектру методологій. Як правило, перевага надається простим, але надійним методологіям, а не складним методам. Прості методології з більшою ймовірністю відповідають вимогам прозорості та практичності.

Методології оцінки ризиків поділяють на якісні та кількісні, та за умови належної розробки обидва типи оцінок мають потенціал для отримання корисних аналітичних результатів. В

той самий час якісні та кількісні методології можуть бути невиправдано складними або погано розробленими. Методологія, будь то кількісна чи якісна, але яка найкраще відповідає потребам особи, що приймає рішення, зазвичай є найкращим вибором.

Загальні принципи аналізу, які були вперше наведені в Національному плані захисту інфраструктури, є широко застосовними до всіх етапів методології управління ризиками. Ці принципи можуть бути використані для вдосконалення існуючих методологій або їх модифікації, щоб інвестиції та експертиза, які вони представляють, могли бути використані для підтримки національної оцінки ризиків, інвестицій, планування реагування на інциденти та приоритезації ресурсів. Визнаючи, що багато методологій оцінки ризиків перебувають на стадії розробки, а інші розвиваються в динамічному середовищі, аналітичні принципи методологій оцінки ризиків слугують орієнтиром для майбутніх адаптацій. Основні аналітичні принципи гарантують, що оцінка ризиків є:

- **Задокументованою:** Методологія та оцінка повинні чітко документувати, яка інформація використовується і як вона синтезується для отримання оцінки ризиків. Будь-які припущення, вагові коефіцієнти та суб'єктивні судження мають бути зрозумілими для людини яка використовує методологію, її аудиторії та інших осіб, які будуть використовувати результати оцінювання. Перед проведенням оцінки ризиків необхідно чітко визначити, для яких рішень або сценаріїв оцінка ризиків призначена, а також часові рамки оцінки (наприклад, поточні умови в порівнянні з майбутніми операціями).
- **Відтворюваною:** Якщо кілька різних аналітиків, або група аналітиків проводять оцінку однієї і тієї ж критичної інфраструктури, то методика повинна забезпечувати однакові результати, щоб можна було проводити порівняння та приймати обґрунтовані рішення на основі цих результатів. Вона повинна мінімізувати кількість і вплив суб'єктивних суджень, залишаючи політичні та ціннісні судження для тих, хто приймає рішення.
- **Обґрунтованою:** Методологія оцінки ризиків повинна логічно інтегрувати свої компоненти, належним чином використовувати професійні дисципліни, що мають відношення до аналізу, а також не містити суттєвих помилок або упущень. Невизначеність, пов'язана з оцінкою наслідків, і впевненість в оцінках вразливостей та загроз повинні бути обговорені.

Ідентифікація сценаріїв ризику

Оцінювання ризиків національній безпеці, як правило, повинно використовувати сценарії, щоб розділити виявлені ризики на частини, які можна оцінити та проаналізувати окремо. Сценарій - це гіпотетична ситуація, що складається з ідентифікованої загрози або небезпеки, суб'єкта, на якого впливає ця небезпека, та пов'язаних з нею умов, включаючи наслідки небезпеки.

Під час розробки можливих сценаріїв для визначення потенційних ризиків, аналітики повинні враховувати всі аспекти проведення оцінки і надавати особі, яка приймає рішення, повну інформацію. Для відносно стаціонарної системи важливо визначити ті компоненти або критичні вузли, де потенційні наслідки будуть найвищими і де потрібно зосередити заходи з забезпечення безпеки та стійкості. Аналітики повинні бути обережними при роботі з результатами. Проведення двох сценаріїв про одну і ту ж саму подію, може призвести до подвійного підрахунку ризику.

Оцінка загроз і небезпек

Федеральний уряд оцінює поточну терористичну загрозу для Сполучених Штатів шляхом ретельного вивчення і розуміння дій терористів і терористичних організацій, і часто це вивчення ґрунтується на аналізі засекреченої інформації. Уряд надає партнерам незасекречені оцінки потенційних терористичних загроз і відповідний доступ до засекречених оцінок, якщо це необхідно і дозволено.
Ці оцінки загроз ґрунтуються на аналізі намірів і можливостей зловмисника та описують те, що відомо про зацікавленість терористів до певних секторів критичної інфраструктури, а також про конкретні методи атак. Оскільки міжнародні терористи постійно демонструють гнучкість і непередбачуваність, федеральний уряд також аналізує відомі терористичні цілі та завдання, а також можливості, що розвиваються, щоб надати власникам і операторам критичної інфраструктури широке уявлення про потенційні загрози і можливі методи терористичних атак. Подібні підходи використовуються для оцінки загроз крадіжок, вандалізму, саботажу, внутрішньої загрози, кіберзагроз, нападу з вогнепальної зброї та інших навмисних дій.

Як національні, так і міжнародні об'єкти критичної інфраструктури є потенційними першочерговими цілями для зловмисників. З огляду на глибоко вкорінений характер цілей зловмисників, об'єкти критичної інфраструктури, ймовірно, залишатимуться дуже привабливими цілями для державних і недержавних суб'єктів та інших осіб зі зловмисними намірами. Оцінка загроз повинна враховувати різні елементи як фізичних, так і кіберзагроз для критичної інфраструктури, залежно від типу атаки і її цілей.

Оцінки небезпеки спираються на історичну інформацію та майбутні прогнози щодо природних

загроз, щоб оцінити ймовірність або частоту різних небезпек. Це сфера, де різні органи федерального уряду працюють з власниками та операторами інфраструктури в секторах для проведення оцінок перед будь-якою конкретною небезпекою, а також після виявлення загрози, що насувається (наприклад, урагану, який ще не досягнув берега). Оцінки небезпек все частіше враховують такі фактори, як зношування інфраструктури та зміни клімату та їх вплив на загальну безпеку та стійкість. Загрози та небезпеки критично важливої інфраструктури включені до переліку загроз та небезпек, визначених в рамках процесу THIRA.

Оцінка вразливостей

Вразливості можуть бути пов'язані з фізичними (наприклад, відсутність бар'єрів або сигналізації), кібернетичними (наприклад, відсутність брандмауера) або людськими (наприклад, непідготовлені охоронці) факторами. Оцінка вразливостей може бути окремим процесом або складовою частиною оцінки ризиків і включає оцінку конкретних загроз для активів, систем або мереж з метою виявлення слабких місць, які можуть призвести до негативних наслідків.

У багатьох секторальних планах описуються різні методології оцінки вразливостей, що застосовуються в конкретних секторах критичної інфраструктури. У них також може міститися детальна інформація про різні способи проведення оцінювання (наприклад, ким і як часто).

Оцінка наслідків

Категорії наслідків можуть включати:

- **Громадське здоров'я та безпека:** Вплив на життя та фізичне здоров'я людини (наприклад, смертельні випадки, травми/захворювання).
- **Економічні:** Прямі та непрямі економічні втрати (наприклад, витрати на відновлення активів, витрати на реагування та відновлення після атаки, витрати на переробку, пов'язані з перебоями в постачанні продукції або послуг, довгострокові витрати через шкоду, завдану навколишньому середовищу).
- **Психологічні:** Вплив на суспільну мораль і довіру до національних економічних і політичних інститутів. Сюди відносяться зміни у сприйнятті, що виникають після значного інциденту, які впливають на відчуття безпеки і благополуччя громадськості і можуть проявлятися у відхиленнях у поведінці.
- **Вплив на управління/місії:** Вплив на здатність уряду або промисловості підтримувати порядок, надавати основні державні послуги, забезпечувати охорону здоров'я та безпеку населення, а також виконувати місії, пов'язані з національною безпекою.

В ідеалі аналіз наслідків повинен враховувати як прямі, так і непрямі наслідки. Функціонування багатьох активів, систем і мереж залежить від зв'язків з іншими об'єктами критичної інфраструктури. Наприклад, майже всі сектори покладаються на сектор енергетики, зв'язку,

транспорту та водопостачання. У багатьох випадках вихід з ладу одного об'єкта або системи вплине на здатність взаємопов'язаних об'єктів або систем у тому ж чи іншому секторі виконувати свої функції. Крім того, кібернетична взаємозалежність створює унікальні виклики для всіх секторів через безмежну природу кіберпростору. Взаємозалежності мають подвійну природу. Наприклад, енергетичний сектор покладається на комп'ютерні системи управління для управління електромережою, в той час як ті ж самі системи управління потребують електроенергію для роботи. Як наслідок, повний аналіз наслідків розглядає усі взаємозв'язки критичної інфраструктури з метою оцінки ризиків.

Найскладніші моделі оцінки ризиків та симуляцій, можуть бути недоцільним та непотрібними для всіх активів, систем або мереж. За таких обставин спрощений аналіз залежностей і взаємозалежностей, заснований на експертних оцінках, може надати достатньо інформації для своєчасного прийняття обґрунтованих рішень з управління ризиками.

В оцінках наслідків також присутній елемент невизначеності. Навіть коли сценарій з обґрунтованими найгіршими умовами чітко сформульований і послідовно застосовується, існує цілий ряд інших результатів, які можуть відбутися. Для деяких інцидентів діапазон наслідків невеликий, і не складна оцінка наслідків може надати достатньо інформації для прийняття рішень. Якщо діапазон наслідків великий, сценарій може вимагати більшої конкретизації умов для отримання відповідних оцінок наслідків. Однак, якщо сценарій розбитий на частини з достатнім рівнем деталізації, але все одно залишається значна невизначеність, оцінка наслідків повинна супроводжуватися діапазоном невизначеностей для підтримки прийняття більш обґрунтованих рішень. Найкращий спосіб передачі інформації про можливість появи невизначеностей буде залежати від факторів, які роблять результат невизначеним, а також від обсягу і типу наявної інформації.

4. Впровадження заходів з управління ризиками

Результати оцінок ризиків критичної інфраструктури допомагають обирати і впроваджувати заходи зі зниження ризиків та визначати пріоритети управління ризиками для власників і операторів критичної інфраструктури. Аналогічним чином, результати THIRA, які можуть включати оцінку ризиків критичної інфраструктури, можуть бути використані для вибору варіантів управління ризиками та пріоритетів у сфері основних можливостей для цілих громад. Вибір і впровадження відповідних заходів з управління ризиками допомагає сфокусувати планування, покращити координацію та підтримати ефективний розподіл ресурсів і прийняття рішень щодо управління інцидентами. Порівняння та визначення пріоритетності ризиків, з якими стикаються різні організації, допомагає визначити, де зниження ризиків є найбільш необхідним, а також визначити та обґрунтувати вибір найбільш економічно ефективних варіантів управління ризиками. Це підтримує рішення щодо розподілу ресурсів (наприклад, де слід запровадити програми управління ризиками), спрямовує інвестиції в ці

програми і виділяє заходи, заходи, які найбільше вигідні з точки зору досягнення результатів після інвестування.

Процес оцінки та вибору ефективних заходів з управління ризиками генерує інформацію, яка може бути використана під час реагування на інциденти та для прийняття рішень щодо відновлення критично важливої інфраструктури. Він також забезпечує основу для розуміння потенційних переваг зменшення ризиків, що може бути використано для планування та прийняття рішень щодо розподілу ресурсів.

Партнери у сфері критичної інфраструктури покладаються на різні підходи до вибору заходів з управління ризиками відповідно до їхніх конкретних повноважень, потреб сектору, ландшафту ризиків, підходів до безпеки та бізнес-середовища. Наприклад, власники та оператори, федеральні міністерства та відомства, штатні та місцеві органи влади мають різні можливості для зменшення ризиків. Підходи, спрямовані на захист активів, можуть бути доречними для об'єктів критичної інфраструктури, ризики яких переважно пов'язані з фізичними об'єктами та інфраструктурою. Функціонально-орієнтовані підходи можуть бути більш ефективними для забезпечення безперервності роботи під час і після інциденту в секторах, де стійкість критичної інфраструктури може бути важливішою, ніж фізичний захист і зміцнення критичної інфраструктури. Підходи, спрямовані на зниження ризиків критичної інфраструктури, мають ан увазі вкладення коштів у захист фізичних активів або забезпечення стійкості віртуальних систем, залежно від того, який варіант краще дозволяє ефективно управляти ризиками критичної інфраструктури з мінімальними витратами.

Власники та оператори об'єктів критичної інфраструктури визначають пріоритети та впроваджують заходи зі зниження ризиків, виходячи з їхньої економічної ефективності, доцільності та потенціалу для зниження ризиків. Оцінюючи ризики та варіанти управління ними, як процес THIRA, так і підхід до управління ризиками критичної інфраструктури допомагають виявити прогалини в спроможностях і визначити можливості, які необхідно розвивати або посилювати.

Дії з управління ризиками включають заходи, спрямовані на стримування, запобігання та підготовку до загроз і небезпек, зменшення вразливостей до інциденту; пом'якшення наслідків після нього, забезпечення своєчасного, ефективного реагування та відновлення після інциденту, будь то терористичний напад, стихійне лихо або інше. Підхід до управління ризиками зосереджує увагу на тих заходах із запобігання, захисту, пом'якшення наслідків, реагування та відновлення, які приносять найбільшу віддачу від інвестицій, а не просто на зменшенні вразливостей. Заходи з безпеки та стійкості відрізняються в різних секторах та юрисдикціях і охоплюють широкий спектр дій, спрямованих на забезпечення безпеки та посилення стійкості критичної інфраструктури.

Діяльність з управління ризиками також може включати засоби для зменшення наслідків атаки або інциденту. Ці заходи спрямовані на пом'якшення наслідків, реагування та/або відновлення. Часто економічно ефективніше вбудувати системи забезпечення безпеки та

стійкості в активи, системи та мережі, ніж модернізувати ці системи вже після розгортання. Відповідно, партнери у сфері критичної інфраструктури повинні розглянути, як управління ризиками стійкість та відповідні заходи з посилення фізичної та кібербезпеки можуть бути інтегровані в процес проектування і будівництва нової критичної інфраструктури, а також в перепроектування або ремонт вже існуючої інфраструктури. У ситуаціях, коли надійність і стійкість є ключовими для управління ризиками критичної інфраструктури, більш ефективним і дієвим може бути впровадження програм на системному рівні а не на рівні окремих активів. Наприклад, може бути економічно неефективно забезпечувати стійкість кожної лікарні в мегаполісі, але було б розумно переконатися, що географічно або іншим чином пов'язані лікарні є стійкими як група або система, щоб одна з них могла підмінити іншу в разі настання катастрофи.

Оцінюючи варіанти управління ризиками, організації повинні враховувати галузеві стандарти та найкращі практики, заходи, які ефективно застосовуються в інших умовах, а також уроки, винесені з реальних подій та навчань. Варіанти управління ризиками повинні бути описані досить детально, щоб визначити, якою мірою вони зменшать ризики, а також оцінити усі витрати (наприклад, початкові інвестиції або запуск, експлуатація та технічне обслуговування, а для фізичних активів - знесення та утилізація). Важливо проаналізувати можливі варіанти синергії (наприклад, випадки, коли варіанти зниження ризику, розроблені для одного сценарію, впливають на збільшення чи зменшення ризиків інших сценаріїв). Використання позитивних синергій та уникнення негативних дозволяє суб'єктам господарювання обирати економічно ефективні варіанти зниження ризиків). Використання позитивних синергій та уникнення негативних дозволяє організаціям обирати економічно ефективні варіанти зниження ризиків.

Ефективна діяльність з управління ризиками є комплексною, скоординованою та економічно ефективною. Рішення з управління ризиками повинні прийматися на основі аналізу витрат та інших наслідків, а також прогнозованих вигод від прийнятих способів дій, включаючи дії пов’язані з бездіяльністю, коли вважається, що ризик вже ефективно управляється. Важливо зазначити, що заходи з управління ризиками варто оцінювати на основі їхнього потенціалу щодо управління ризиками в сукупності за різними сценаріями, а також їхньої здатності управляти ризиками, пов'язаними з окремим сценарієм; ці два варіанти мають вирішальне значення для визначення найбільш ефективних дій.

5. Вимірювання ефективності

Використання показників ефективності є важливим кроком у процесі управління ризиками критичної інфраструктури, що дозволяє оцінити покращення у сфері безпеки та стійкості критичної інфраструктури.

Показники ефективності дозволяють партнерам відстежувати прогрес у досягненні поставлених цілей і завдань. Ці показники є основою для спільноти критичної інфраструктури, що дозволяє їй створювати систему звітності, документувати фактичні показники, сприяти ефективному управлінню та забезпечувати механізм зворотного зв'язку для прийняття рішень.

Національні цілі, які зосереджені на управлінні ризиками, ситуаційній обізнаності та національній готовності, матимуть центральне значення для ефективної оцінки ефективності, забезпечуючи спільне розуміння бажаного "кінцевого результату", над досягненням якого колективно працює партнерство. Додатковий набір національних пріоритетів, розроблений за участі широкого кола партнерів у сфері критичної інфраструктури, ілюструватиме напрямки дій, необхідні для досягнення національних цілей.

Спільнота критичної інфраструктури буде розробляти високорівневі результати, які пов'язані з цілями та пріоритетами національного рівня, щоб допомогти вимірювати прогрес щодо досягнення кінцевого результату, а саме - забезпечення безпеки та стійкості критичної інфраструктури, який було визначено в PPD-21.

Маючи спільне розуміння, спільнота критичної інфраструктури може продемонструвати прогрес у досягненні національних цілей, використовуючи наявні дані та інформацію. Коли буде досягнуто значний прогрес в досягненні національних цілей і пріоритетів (в міру розвитку середовища ризиків, політичного ландшафту і сфери практичної діяльності) спільнота перегляне і оновить ці цілі і пріоритети. Сектори та регіональні партнерства повинні визначити цілі, що доповнюють національні цілі, але адаптовані до конкретного сектору або географічної області.

Використання метрик та вимірювання ефективності для безперервного вдосконалення

Використовуючи метрики для оцінки ефективності зусиль партнерства, спрямованих на досягнення національних і секторальних пріоритетів, партнери у сфері критичної інфраструктури можуть коригувати та адаптувати свої підходи до забезпечення безпеки та стійкості з урахуванням досягнутого прогресу, а також змін у загрозах та іншого. Показники використовуються для того, щоб зосередити увагу на сферах безпеки та стійкості, які потребують додаткових ресурсів або змін, шляхом аналізу викликів і пріоритетів на національному, секторальному рівнях та на рівні власника/оператора.

Показники також слугують механізмом зворотного зв'язку для інших аспектів управління ризиками критичної інфраструктури. Вони можуть інформувати про прогрес у досягненні національних і секторальних цілей і надавати аналітикам інформацію для коригування їхніх оцінок ризиків. Наприклад, метрики вказують на ефективність заходів з безпеки та стійкості, а також на те, наскільки ці заходи зменшують ризики. Нарешті, показники можуть допомогти у визначенні пріоритетів і виборі найбільш ефективних та економічно вигідних способів управління ризиками