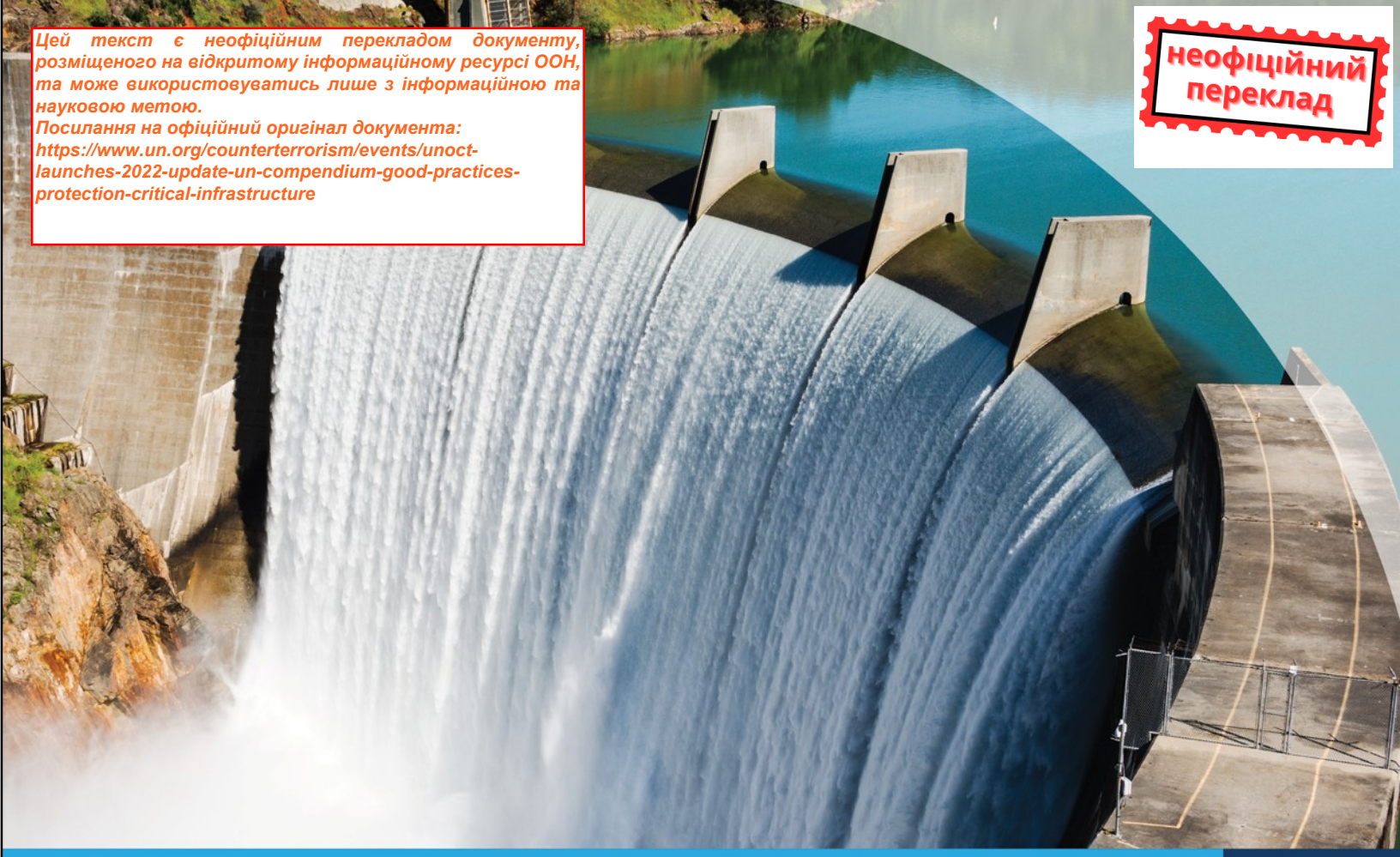

The Protection of Critical Infrastructure Against Terrorist Attacks

COMPENDIUM OF GOOD PRACTICES

2022 UPDATE

Захист критичної інфраструктури від терористичних атак

Збірник передових практик 2022

Вступ

Терористи все частіше використовують вразливі місця в державних і приватних комунальних підприємствах майже в усіх секторах, включаючи транспорт і енергетику, а також водну інфраструктуру та ядерні об'єкти. Критична інфраструктура стала основною метою терористичних атак по всьому світу. Взаємозалежність і взаємопов'язаний характер критичної інфраструктури, розташованої через кордони, викликають додаткові занепокоєння та вимагають двосторонніх або регіональних заходів. Мета терористів добре відома: зруйнувати наш спосіб життя, розірвати структуру наших суспільств і посіяти розкол.

Хоча великомасштабних терористичних атак на критично важливу інфраструктуру зі значними каскадними наслідками ще не відбулося, загроза, яку створює такий сценарій, залишається постійною та вимагає від країн вжиття відповідних заходів запобігання, реагування та стійкості.

Збірник належної практики щодо захисту критичної інфраструктури від терористичних атак, вперше опублікований у 2018 році та оновлений у 2022 році, був розроблений, щоб надати державам-членам, практикам, громадянському суспільству, міжнародним і регіональним організаціям, академічним колам, приватному сектору та всім відповідним зацікавленим сторонам з відповідними передовими практиками, інструментами та тематичними дослідженнями з усього світу для підтримки зусиль держав-членів щодо захисту їх критичної інфраструктури.

Генеральна Асамблея і Рада Безпеки протягом багатьох років приділяють пильну увагу цій темі. У Глобальній контртерористичній стратегії Організації Об'єднаних Націй, у рамках Другої частини щодо заходів боротьби з тероризмом і запобігання йому, держави-члени вирішили «активізувати всі зусилля для покращення безпеки та захисту особливо вразливих цілей, таких як інфраструктура та громадські місця, а також як реакція на терористичні напади та інші лиха, зокрема у сфері цивільного захисту, визнаючи, що держави можуть потребувати допомоги з цією метою».

На додаток до більш загальних закликів до запобігання цій загрозі, включених до резолюцій 1373 (2001) і 1566 (2004), Рада Безпеки ухвалила резолюцію 2341 (2017), яка була першим глобальним документом, повністю присвяченим важливості захисту критично важливої інфраструктури від терористичних атак. Зокрема, у резолюції Рада нагадала про своє рішення в резолюції 1373 (2001)

про те, що всі держави повинні визнати терористичні акти серйозними кримінальними злочинами у національних законах і постановах, і закликала всі держави-члени забезпечити встановлення кримінальної відповідальності за терористичні напади, призначені для знищення або виведення з ладу критичної інфраструктури, а також планування, навчання, фінансування та матеріально-технічна підтримка таких атак.

У резолюції 2396 (2017) Рада Безпеки визнала, що Ісламська держава в Іраку та Леванті (ІДІЛ), закликала своїх прихильників і філії, особливо терористів, які залишають зони збройних конфліктів, планувати та здійснювати напади на громадські місця та комунальні послуги. У цій резолюції Рада підкреслила необхідність для держав встановити або зміцнити національне, регіональне та міжнародне партнерство із зацікавленими сторонами, як державними, так і приватними, для обміну інформацією та досвідом з метою запобігання, захисту, пом'якшення, розслідування, реагування та відновлення шкоди від терористичних атак проти «м'яких» цілей.

З моменту першої публікації цього Збірнику Організація Об'єднаних Націй та її держави-члени продовжують свою роботу зі зміцнення міжнародного співробітництва у протидії тероризму та протидії терористичним загрозам критичної інфраструктури.

Що стосується Ради Безпеки, то в 2018 році Контртерористичний комітет опублікував додаток до Мадридських керівних принципів 2015 року, в якому підкреслюється важливість захисту вразливих цілей, як це передбачено в принципах 50 і 51. Крім того, Резолюція 2617 (2021) Ради Безпеки, прийнята в грудні 2021 року, також включає конкретні положення щодо захисту критичної інфраструктури та так званих «м'яких» цілей як частину нового мандату Виконавчого директорату Контртерористичного комітету та визнає вирішальну важливість співпраці з Управлінням по боротьбі з тероризмом у цій сфері.

У червні 2021 року під час сьомого перегляду Глобальної контртерористичної стратегії ООН держави-члени консенсусом погодилися, що захист уразливих цілей має бути пріоритетом у наших спільних діях проти тероризму. Резолюція 75/291 Генеральної Асамблеї містила два параграфи преамбули та чотири пункти резолюції на цю тему, наголошуючи на необхідності об'єднати всі відповідні зацікавлені сторони — держави-члени, міжнародні та регіональні організації, приватний

сектор, громадянське суспільство та наукові кола — для ефективної боротьби з безпрецедентною загрозою. через терористичні атаки на критичну інфраструктуру та легкі цілі.

Протягом останніх чотирьох років держави-члени також дуже активно адаптували свої правові, інституційні та операційні рамки для захисту критичної інфраструктури. Цей Збірник продемонструє читачам швидкість, з якою змінюється ландшафт захисту критичної інфраструктури.

Глобальна програма з протидії терористичним загрозам проти вразливих цілей, яку спільно впроваджують Контртерористичний офіс, Виконавчий директорат Контртерористичного комітету, Міжрегіональний науково-дослідний інститут ООН у сфері злочинності та правосуддя (UNICRI) та Альянс цивілізацій ООН у Співпраця з Міжнародною організацією кримінальної поліції (ІНТЕРПОЛ) з 2021 року підтримує держави-члени у розбудові їхнього потенціалу, розвитку зв'язків між експертами та визначенні передових практик для захисту критичної інфраструктури.

Ми впевнені, що цей оновлений Збірник, який став можливим завдяки щедрому фінансуванню Глобальної програми з боку Держави Катар, стане основоположним інструментом у цій сфері на користь всіх держав-членів та їхніх громадян.

Володимир Воронков

Управління по боротьбі
з тероризмом

Виконуючий обов'язки
директора Виконавчої
дирекції
Контртерористичного
комітету

Передмова

Нам щодня нагадують про загрозу, яку становлять терористи для міжнародної спільноти та нашого спільного процвітання та безпеки. Здатність цих суб'єктів завдавати шкоди зростає в геометричній прогресії, коли їхня діяльність спрямована на критичну інфраструктуру (KI), таку як розміщення хімічних, біологічних, радіологічних і ядерних (CBRN) матеріалів, або вразливі цілі, такі як громадські місця, комунальні послуги та Інтернет.

Міжнародна організація кримінальної поліції (ІНТЕРПОЛ) і світове співтовариство правоохоронних органів у співпраці з усіма партнерами, зібраними в рамках Глобального договору про координацію боротьби з тероризмом ООН, віддані визначенню пріоритетних терористичних загроз для наших країн і прямій протидії їм. Боротьба з тероризмом має бути колективною та спільною діяльністю, і світовій спільноті, як ніколи, необхідно працювати в партнерстві, щоб використовувати свої відповідні мандати та досвід.

Зважаючи на це, Робоча група з нових загроз і захисту критичної інфраструктури під головуванням Інтерполу внесла свій внесок у початковий випуск цього збірника передових практик захисту KI від терористичних атак, а тепер і в його оновлення 2022 року.

Збірник, який щедро спонсорує Управління по боротьбі з тероризмом і постійно підтримується Виконавчим директоратом Контртерористичного комітету, надає розробникам політики, а також регіональним і національним органам влади рекомендації щодо належної практики захисту KI. Збірник зосереджений на індикаторах, стандартах, заходах оцінки ризиків і відповідних рекомендаціях, а також надає країнам довідковий матеріал для розробки проактивних стратегій зниження ризиків, пов'язаних з тероризмом, для KI.

Протидія тероризму вимагає підходу всього суспільства. Разом ми продовжуємо виявляти та реагувати на зміни в ландшафті терористичної загрози. Відповідно, ті з нас, хто бере участь у спільному підході до підготовки цього Компендіуму, сподіваються, що цей документ допоможе вам у боротьбі з поточними та майбутніми загрозами KI. Давайте разом докладати постійних колективних зусиль для виявлення, стримування та припинення терору в його джерелі.

Стівен Кавана

Виконавчий директор поліцейської

служби ІНТЕРПОЛу

Зміст

Вміст

Тематичні дослідження

Інструменти

Таблиці

Абревіатури та акроніми

ABC	автоматизовані системи прикордонного контролю (ICAO)
AFS	аеронавігаційна фіксована служба
AIS	автоматизований обмін індикаторами (CISA)
API	попереднє інформування пасажирів (ICAO)
ASEAN	Асоціація держав Південно-Східної Азії
ASIO	Австралійська організація розвідки безпеки
BCN	біологічні, хімічні та ядерні
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (Положення про ідентифікацію критичної інфраструктури)
CBRN	хімічні, біологічні, радіологічні та ядерні
CBRNE	хімічні, біологічні, радіологічні, ядерні та вибухові речовини
CI	Критична інфраструктура
CICT	Інтегрований центр інформації та розвідки по боротьбі з тероризмом – Колумбія
CII	критична інформаційна інфраструктура
CIIP	захист критичної інформаційної інфраструктури
CISA	Агентство з кібербезпеки та безпеки інфраструктури (Сполучені Штати)
CNI	критична національна інфраструктура
CNPIC	Національний центр захисту інфраструктури та кібербезпеки (Іспанія)
COVID-19	коронавірусна хвороба
CPNI	Центр захисту національної інфраструктури (Великобританія)
CTEPs	Настільні пакети вправ CISA (Сполучені Штати)
CTITF	Оперативна група Організації Об'єднаних Націй з реалізації заходів боротьби з тероризмом
CTPN	Мережа підготовки до протидії тероризму
DoS attacks	атаки на відмову в обслуговуванні
DTC	цифрові облікові дані для подорожей (ICAO)
ECOWAS	Економічне співтовариство держав Західної Африки
EFTA	Європейська Асоціація Вільної Торгівлі
Europol	Агенство Європейського Союзу з питань співробітництва правоохоронних органів
FBI	Федеральне бюро розслідувань (Сполучені Штати)
GFCE	Глобальний форум кіберекспертизи
GHS	Глобальна гармонізована система класифікації та маркування хімічних речовин

IAEA	Міжнародне агентство з атомної енергії
ICAO	Міжнародна організація цивільної авіації
ICT	інформаційні та комунікаційні технології
IED	саморобний вибуховий пристрій
INTERPOL	Міжнародна організація кримінальної поліції

IOM	Міжнародна організація з міграції
ISO	Міжнародна організація стандартизації
ISIL	Ісламська держава в Іраку та Леванті
ISPS Code	Міжнародний кодекс охорони суден і портових засобів
ITU	Міжнародний союз електрозв'язку
NIS	мережеві та інформаційні системи
OAS	Організація Американських Штатів
OECD	Організація економічного співробітництва та розвитку
OPCW	Організація із заборони хімічної зброї
OSCE	Організація з безпеки та співробітництва в Європі
PKD	Директорія відкритих ключів (ICAO)
PPPs	державно–приватне партнерство
SARPs	Стандарти та рекомендовані практики (ICAO)
SOLAS Convention	Конвенція з безпеки життя на морі
TETRA	наземний транкінговий радіозв'язок
UAS	безпілотна літальна система
UNICRI	Міжрегіональний дослідницький інститут злочинності та правосуддя ООН
USAID	Агентство США з міжнародного розвитку
WHO	Всесвітня організація охорони здоров'я
WMD	зброя масового ураження

Вступ: контекст, цілі та методологія

У цьому Збірнику розглядається тема, яка значною мірою все ще перебуває в зародковому стані. Швидкість, з якою сучасна економіка стала нерозривно взаємопов'язаною протягом останніх двох десятиліть, особливо завдяки великим успіхам, досягнутим інформаційно-комунікаційними технологіями (ІКТ), наразила наше суспільство набору безпрецедентних загроз і вразливостей. Багато з них походять від терористичних груп, які прагнуть дестабілізувати громади та створити широку паніку, підриваючи самі активи та процеси, від яких залежить виживання наших суспільств. Ці активи та процеси є центральними вузлами, відомими як «критична інфраструктура» (КІ).

Однак зростаюче усвідомлення того, що ми зараз стикаємося з новим типом середовища безпеки, не відповідає відповідним рівням готовності. Тим не менш, нещодавні атаки на транспортні системи, неодноразові диверсійні акти проти дамб, нафтопроводів, телекомунікаційних мереж та інших об'єктів є новим нагадуванням про гострий інтерес терористичних груп різної приналежності до об'єктів інфраструктури, за допомогою яких надається низка основних послуг.

Саме в цьому контексті Рада Безпеки прийняла свою резолюцію 2341 (2017) як перший в історії глобальний інструмент, повністю присвячений захисту КІ від терористичних атак. Його положення відображають рішучість міжнародного співтовариства розробити та вдосконалити механізми, необхідні для мінімізації ризиків для КІ, спричинених терористичними атаками, а також для забезпечення адекватної відповіді на такі атаки та відновлення після них.

З огляду на відновлення інтересу до захисту та стійкості КІ та гострої необхідності для держав-членів імплементувати резолюцію 2341 (2017), у 2018 році Антитерористичне управління та Виконавчий директорат Контртерористичного комітету розробили перше видання Збірнику передових практик захисту критичної інфраструктури від терористичних атак[1]. Збірник було задумано як практичний інструмент для підтримки широкого кола суб'єктів (від політиків до правоохоронних органів і зацікавлених сторін у приватному секторі) з різним ступенем відповідальність за розробку та впровадження політики та заходів, необхідних для виконання резолюції

2341 (2017). Після випуску Збірник використовувався як провідне джерело інформації та передового досвіду, а також як інструмент для скерування дискусій на кількох регіональних зустрічах експертів у різних частинах світу[2].

Ця публікація являє собою оновлену та розширену версію Збірнику, яка враховує події, що відбулися з 2018 року та сприяють ширшому розумінню загроз, що виникають, нових правових і політичних інструментів, а також нових кроків, які вживаються країнами для вирішення проблеми. Вся інформація, включена у видання 2018 року, була подвійно перевірена на актуальність. Нові матеріали (політичні та стратегічні документи, правові інструменти, тематичні дослідження та інструменти) були додані завдяки новому раунду кабінетних досліджень та обміну експертами через платформу Connect and Learn Глобальної мережі експертів ООН із захисту вразливих цілей від Терористичних атак. Більше того, ряд держав-членів надали інформацію у відповідь на вербальну ноту, надіслану державам-членам 2 березня 2022 року, з проханням «поділитися своїм передовим досвідом із захисту критичної інфраструктури», включаючи «національний і регіональний передовий досвід, стратегії, плани дії, рамки, інструменти, тематичні дослідження, посібники та інструкції з акцентом на захист критичної інфраструктури».

---

[1] Перше (2018) видання Збірнику було розроблено в рамках робочої групи під головуванням Інтерполу Цільової групи з реалізації заходів з боротьби з тероризмом щодо «захисту критичної інфраструктури, включаючи вразливі цілі. У 2019 році Оперативну групу було включено до Глобального договору ООН про координацію боротьби з тероризмом. Згідно з цією новою структурою робочі групи Цільової групи із захисту критичної інфраструктури, включаючи Інтернет, уразливі об'єкти та безпеку туризму, а також із запобігання та реагування на терористичні атаки зі зброєю масового знищення були об'єднані для створення робочої групи Договору щодо нових загроз та захист критичної інфраструктури (робоча група ETCIP). Нове (2022) видання Компендіуму було розроблено під егідою робочої групи ETCIP.

[2] Касабланка, Марокко (листопад 2018), Туніс (квітень 2019), Сінгапур (січень 2019) і Йоганнесбург, Південна Африка (листопад 2019).

Відповідно до версії 2018 року, нове видання Збірнику організоване за тематичними блоками, які загалом відповідають структурі резолюції 2341 (2017). Кожен розділ розпочинається одним або кількома пунктами постановляючої частини, взятими з відповідних інструментів, і містить аналіз питань, що розглядаються. Було вжито заходів для того, щоб не припускати, що читач має попередні знання про концепції, пов'язані з КІ. Цей підхід випливає з визнання того, що поняття «захист критичної інфраструктури» є відносно новим доповненням до дискурсу глобальної державної політики.

Основні практичні та правові виклики, з якими стикаються держави, розглядаються з точки зору поточних і потенційних рішень, прийнятих окремими урядами, міжнародними установами, організаціями приватного сектора та організаціями громадянського суспільства. Прагматичний підхід, якого дотримується Збірник, ілюструється великою кількістю тематичних досліджень, які містять конкретні приклади та варіанти впровадження. Було додано низку таблиць, щоб дати можливість країнам швидко порівняти заходи, які вживають інші країни, і зрештою допомогти їм сформувати відповіді, які найкраще відповідають їхньому інституційному контексту.

Новинкою нової редакції Збірнику є те, що вона об'єднує низку спеціалізованих тематичних модулів – як доповнення – зосередження уваги на захисті так званих «м'яких цілей»[3]. Таким чином Збірник прагне розширити розуміння заходів із захисту критичної інфраструктури шляхом визначення точок контакту з певним типом уразливих сайтів (м'яких цілей) та заохочення країн до розвитку синергії між політикою та оперативними заходами в обох сферах[4].

Хоча Збірник зосереджується на захисті КІ від терористичних атак, він визнає, що ряд держав-членів вирішили прийняти широкі стратегії, які враховують необхідність підвищення стійкості КІ до всіх небезпек, створених людиною чи природою. У світлі цього визнання Збірник надає концептуальні інструменти, які дозволять державам-членам прийняти, якщо вони того бажають, всеохоплюючі стратегії, приділяючи особливу увагу терористичній загрозі та відповідним механізмам оцінки та пом'якшення.

Відповідно до резолюції 2341 (2017), у Збірнику йдеться про КІ, не зосереджуючись на конкретному типі інфраструктури. Цей наскрізний підхід має на меті висвітлити загальні принципи, процеси та методології, які держави-члени заохочуються перетворити на реальні стратегії, плани дій та заходи. У той же час у документі наводяться приклади заходів пом'якшення, характерних для окремих галузей. Крім того, у розділі 9 подано огляд основних ініціатив, вжитих провідними міжнародними агентствами у вибраних секторах.

Нарешті, надаючи вказівки для держав-членів, Збірник підтримує принцип, згідно з яким правам людини та гендерним питанням слід приділяти належну увагу та ефективно включати їх у всі заходи захисту КІ та відповідні стратегії

[3] Чотири галузеві модулі вводяться загальним модулем і стосуються захисту релігійних і туристичних місць, міських центрів і загроз, створених безпілотними літальними системами..

[4] Збірник і відповідні модулі дотримуються термінологічного підходу, прийнятого Генеральною Асамблеєю під час сьомого перегляду Глобальної контртерористичної стратегії ООН. Резолюція 75/291, зокрема, розглядає «м'які цілі» як одну з двох підмножин вразливих цілей, іншу — «критичну інфраструктуру».

1. Усвідомлення проблеми

Резолюція Ради Безпеки 2341 (2017)

Рада безпеки

...

1. *Заохочує всі державни докладати узгоджених і скоординованих зусиль, у тому числі шляхом міжнародного співробітництва, для підвищення обізнаності, розширення знань і розуміння викликів, пов'язаних з терористичними нападами, з метою покращення готовності до таких нападів на критичну інфраструктуру*

Додаток до керівних принципів щодо іноземних бойовиків-терористів (Мадридські керівні принципи)

1.1 Тероризм як особлива загроза КІ

Незважаючи на те, що КІ завжди зазнавала численних небезпек, включаючи природні явища, людські помилки, технічні збої та злочинні дії в широкому сенсі, поява захисту КІ як особливої сфери політики стала прямим наслідком подій 11 вересня 2001 року. .

Протягом останніх кількох десятиліть терористи регулярно виявляли інтерес до КІ як мішеней для досягнення своїх цілей. Ще в 2002 році вже були чіткі ознаки того, що Аль-Каїда намагалася використати вразливі місця в державних і приватних комунальних службах Сполучених Штатів. Виявлення в Афганістані комп'ютера, що містить програми структурного аналізу гребель, спонукало Національний центр захисту інфраструктури Сполучених Штатів випустити інформаційний бюлетень із попередженням про небезпеку.[5]

Важливо те, що навряд чи жоден сектор уникнув терористичної діяльності або принаймні постійної уваги з боку терористичних груп. У ряді випадків КІ переслідували з конкретною метою перервати надання основних послуг і таким чином спричинити негативний вплив на місцеві чи глобальні спільноти.[6] *Прикладів безліч.*

Енергетичний сектор є свідком постійної терористичної діяльності через напади, здійснені Аль-

Каїдою та її філіями на об'єкти та персонал нафтових компаній в Алжирі, Іраку, Кувейті, Пакистані, Саудівській Аравії та Ємені. Як показує приклад 1, дедалі частіші терористичні атаки на енергетичну інфраструктуру, зареєстровані між 1970 і 2011 роками, виявилися однією з головних причин перебоїв в енергетиці з наслідками для всіх країн у всьому ланцюгу енергопостачання.

---

5 Перегляньте http://lists.jamed.com/crime/2002/01/0055.html.

6 В інших випадках терористичні атаки або плани за участю КІ здійснювалися не з конкретною метою перешкоджання самим операціям КІ, а скоріше для максимізації жертв серед цивільного населення шляхом використання присутності великих натовпів людей усередині чи навколо КІ. Транспортний сектор особливо постраждав від такого типу терористичної діяльності, починаючи з атаки із застосуванням зарину в токійському метро в 1995 році. Іншим прикладом є одночасні атаки на аеропорт Брюсселя та метро в 2016 році, здійснені двома групами бойовиків ДАІШ. Загалом загинули 32 людини, близько 300 отримали поранення.

Вміст 1

Терористичні загрозита КІ: природа та вплив на енергетичний сектор

Дослідження терористичних атак, скоєних у всьому світі проти енергетичної загрози 1970-2011[7], *прийшло до висновку, що*:

- Зростання частоти терористичних атак на енергетичну інфраструктуру в період, що розглядається, стало однією з головних причин перебоїв в енергетиці з наслідками для всіх країн у всьому ланцюгу енергопостачання.
- У сучасному глобалізованому світі всі країни, включаючи країни-виробники, стали взаємозалежними з точки зору їх енергетичної безпеки. Терористи можуть досягти глобального впливу з мінімальними зусиллями. З цієї причини будь-яке переривання вищезазначених систем або інфраструктурної мережі потенційно може вплинути на весь ланцюг енергопостачання.
- Перебої в електропостачанні можуть бути спричинені не лише атаками на масштабні об'єкти енергетичної інфраструктури, такі як нафтові термінали, нафтопереробні заводи та трубопроводи, які часто перебувають у центрі уваги ЗМІ, але й атаками на незначні цілі, такі як електричні трансформатори або високовольтні лінії.
- Десять країн, які зазнали найбільшої кількості атак на енергетичну інфраструктуру в період, що розглядається, це Ангола, Чилі, Колумбія, Сальвадор, Ірак, Пакистан, Перу, Філіппіни, Південна Африка та Іспанія. Ці країни стали жертвами 3801 із 4653 інцидентів атак на енергетичну інфраструктуру, що сталися в усьому світі, що становить 82 відсотки всіх зареєстрованих атак.
- Терористичні атаки спрямовані не лише на енергетичні об'єкти в таких країнах-виробниках, як Ангола, Колумбія та Ірак, а й у транзитних країнах, таких як Афганістан, Пакистан і Туреччина, а також у країнах-споживачах, таких як Сальвадор, Перу та Іспанія. Скрізь, де виникають повстання, політичні заворушення чи громадянська війна, енергетична інфраструктура виглядає важливою ціллю через безпосередній вплив таких атак. Тому для урядів життєво важливо включити це питання у свою енергетичну політику, особливо в стратегії управління ризиками.
- Існує загальна тенденція в усіх країнах, коли терористичні організації віддають перевагу атакам із застосуванням бомб або вибухівки, що відповідає за 4177, або 90 відсотків, із 4653 атак. Це демонструє дуже сильну перевагу цього методу атаки на енергетичну інфраструктуру.

Зовсім нещодавно Управління розвідки та аналізу Міністерства внутрішньої безпеки США опублікувало попередження для сектору електроенергетики після запитів від енергетичних компаній підрахувати зростання загроз з боку домашніх насильницьких екстремістів («DVE») у 2020 і 2021 роках. За даними Департаменту внутрішньої безпеки, «DVE розробили надійні, конкретні плани нападу на електричну інфраструктуру принаймні з 2020 року, визначаючи електричну мережу як особливо привабливу ціль, враховуючи її взаємозалежність з іншими секторами інфраструктури».[8]

Загрози для енергетичної інфраструктури також матеріалізувалися у формі безпілотних літальних систем («UAS»). Згідно зі спільним розвідувальним бюлетенем Міністерства внутрішньої безпеки, Федерального бюро розслідувань (ФБР) і Національного антитерористичного центру, 16 липня 2020 року невеликий готовий безпілотник із 4 роторами був виявлений на вершині будівля біля підстанції. Нейлонові мотузки з дрона звисали на двофутовому вигнутому шматку мідного дроту, і аналіз пристрою показав, що це, ймовірно, було призначено для короткого замикання підстанції, у першому відомому випадку модифікованої системи безпілотного літального апарату, очевидно, використовуваної в Сполучені Штати спеціально спрямовані на енергетичну інфраструктуру. Оператор дрона досі не ідентифікований; Камера системи, карта пам'яті та всі ідентифікаційні позначки були видалені, що вказувало на те, що оператор намагався уникнути ідентифікації, а також, цілком ймовірно, знаходився в межах прямої видимості наміченої цілі під час польоту безпілотника.[9]

Основна водна інфраструктура була об'єктом особливої уваги з боку ДАІШ. У період з 2013 по 2015 роки ДАІШ здійснив близько 20 великих атак на сирійські та іракські цілі. Окрім руйнування труб, каналізаційних станцій і мостів, ДАІШ стратегічно використовувала водну інфраструктуру, наприклад, закриваючи дамби та перекриваючи водопостачання.[10]

---

[7] *Мехмет Біресселіоглу та Ісік Юмуртачі, «Оцінка характеру терористичних атак на енергетичну інфраструктуру: періодичне*

дослідження за 1970-2011 роки», Міжнародний журнал технологій нафти, газу та вугілля, вип. 10, № 3, С. 325–341 У дослідженні розглядається ширше коло подій, у тому числі незначних. Основна причина полягає в тому, що незначні атаки однаково ймовірно призведуть до перебоїв у постачанні електроенергії та, таким чином, підірвуть наявність і доступність існуючих енергетичних послуг, безпосередньо впливаючи на домашнє використання та промислову продуктивність. Дані для дослідження були отримані з цільового типу утиліт з Глобальної бази даних тероризму, бази даних з відкритим кодом, якою керує Університет Меріленда та містить інформацію про терористичні події по всьому світу. Дослідження доступне за адресою www.researchgate.net/publication/282446687_Evaluating_the_nature_of_terrorist_attacks_on_the_energy_infrastructure_The_periodical_study_for_1970-2011.

[8] Продивіться https://www.thedailybeast.com/dhs-warns-that-right-wing-extremists-could-attack-power-grid.

[9] Продивіться https://www.hstoday.us/featured/physical-attacks-on-electricity-infrastructure-extremist-messaging-plots-and-action/.

[10] Продивіться https://worldview.stratfor.com/article/water-wars-waged-islamic-state.

У лютому 2021 року невідомий комп'ютерний хакер намагався дистанційно отруїти водопостачання міста у Флориді, дистанційно збільшивши кількість гідроксиду натрію.

Сектор телекомунікацій також став мішенню. Наприклад, у 2012 році «Боко Харам» здійснила скоординовану дводенну атаку на телекомунікаційну інфраструктуру, що належить кільком операторам у п'яти містах на півночі Нігерії. Цей приклад цікавий, оскільки Боко Харам, схоже, черпав натхнення для цього нападу з подібних актів, вчинених терористичними групами в Афганістані кількома роками раніше, що свідчить про те, що в сфері КІ терористичні групи, які діють у різних частинах світу, готові наслідувати один одного з точки зору обраних ними цілей і методології атаки.

У деяких випадках терористичні атаки були здійснені на інфраструктуру, що містить небезпечні матеріали. 26 червня 2015 року людина врізалася автомобілем у територію хімічного заводу поблизу Ліона та розбила газові балончики, спровокувавши вибух. У 2016 році дві атомні електростанції в Бельгії були заблоковані за підозрою в спробі ДАІШ атакувати, проникнути або саботувати об'єкти для отримання ядерних і радіоактивних матеріалів.

Незважаючи на те, що на сьогоднішній день не було жодних масових атак на КІ із значними каскадними наслідками або збоями, загроза, яку створює цей тип сценарію, все ще дуже присутня та змушує країни створювати адекватні плани профілактики та дій у надзвичайних ситуаціях. Дійсно, терористичні дії, вчинені досі, виявили внутрішню вразливість ряду КІ. Цілком імовірно також, що нові покоління терористів все більше знайомитимуться з ІКТ. Хоча кібератаки з масовими втратами, які можна кваліфікувати як «кібертерористичні атаки», ще не відбулися, зростаючий рівень ноу-хау ІКТ, можливо, зробить їх більш ймовірними. За даними Групи урядових експертів з розробок у сфері інформації та телекомунікацій у контексті міжнародної безпеки, «використання ІКТ у терористичних цілях, окрім вербування, фінансування, навчання та підбурювання, у тому числі для терористичних атак проти ІКТ або ІКТ- залежна інфраструктура є зростаючою ймовірністю, яка, якщо її не розглянути, може загрожувати міжнародному миру та безпеці».[11]

[11] Продивіться https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/227/92/PDF/N1522792.pdf?OpenElement.

Терористичні загрози авіаційній КІ

Хоча загрози для КІ, пов'язані з цивільною авіацією, не зазнали суттєвих змін за останні кілька років, наразі можна спостерігати зростання в деяких векторах загроз, таких як загроза, яку становлять кібератаки, атаки, здійснені на відстані, і внутрішні атаки.

Загалом аеропорти та інші критично важливі об'єкти, пов'язані з авіацією, залишаються привабливою мішенню для злочинної діяльності. Серед зареєстрованих нападів на авіаційні об'єкти багато можна віднести до категорії крадіжок зі зломом, збройних пограбувань або крадіжок, вчинених правопорушниками, які прагнуть отримати цінні товари чи готівку, які зазвичай зберігаються у вантажних приміщеннях чи на складах у зоні аеропорту або перевозяться на комерційних літаках. Хоча жодна з цих подій не стосується осіб, пов'язаних з терористичними групами, вони демонструють, наскільки вразливими можуть бути певні райони аеропортів і наскільки важко їх охоронять. Крім того, з середини 2010-х було зареєстровано низку подій, пов'язаних із несанкціонованими транспортними засобами або особами, які примусово проникли в зону польоту та злітно-посадкові смуги аеропортів.

Ризик, пов'язаний із саморобними вибуховими пристроями, залишається на найвищому рівні та стає все більш географічно розподіленим. Авіаційна змова, розкрита в Австралії в липні 2017, показала, що за допомогою авіаційної системи для розповсюдження матеріалів та Інтернету для розповсюдження знань можна здійснювати складні атаки з місць, де присутня лише невелика кількість мотивованих осіб. Так звані атаки «самотнього вовка» також стають все більш поширеними, і хоча вони в основному наразі мають низький рівень складності, це явище, яке іноді називають «тероризмом замовлень поштою», може збільшити витонченість і вплив таких атак в майбутньому.

У березні 2019 поліція в Лондоні перехопила саморобні вибухові пристрої в підозрілих поштових посилках, імовірно в рамках операції терористичної групи. Один із цих пристроїв було знайдено поблизу аеропорту Хітроу та успішно дезактивовано. Подібним чином у квітні 2019 влада Кувейту виявила саморобний вибуховий пристрій, захований у видовбаній книзі всередині вантажної посилки, після того, як авіаперевізники ідентифікували об'єкт як підозрілий.

Окрім саморобних вибухових пристроїв, кібератаки (розглянуто в розділі 1.2.1) залишаються серйозною проблемою для цивільної авіації. Хоча у 2021 не надходило повідомлень про кібератаки, які безпосередньо загрожували авіаційній безпеці, кількість таких атак на інфраструктуру цивільної авіації щороку постійно зростала. Основні типи кібератак, які спостерігалися у 2021, включали використання шахрайських веб-сайтів (наприклад, видавання себе за авіаційні організації, щоб спонукати користувачів надати інформацію чи оплату), викрадення даних (наприклад, особистої інформації пасажирів або співробітників), фішинг і програми-вимагачі..

Загроза атак на відстані, яка включає ракетні атаки та озброєння безпілотних літальних апаратів, як і раніше викликає занепокоєння для авіаційних операцій як усередині, так і за межами зон конфлікту. У той час як більшість терористичних інцидентів проти цивільної авіації в усьому світі, як і раніше, стосуються аеропортів у зонах конфлікту, атаки на аеропорти за межами зон конфлікту все ж відбуваються і, як правило, спрямовані на об'єкти подвійного призначення, які використовуються як цивільною, так і військовою авіацією. У більшості атак на аеропорти використовується зброя протистояння, включно з такими ракетами, як міномети та реактивні снаряди, а також озброєння безпілотних літальних апаратів, які дозволяють здійснювати атаки дистанційно.

Спостереження БПЛА навколо аеропортів і над злітно-посадковими смугами також викликають зростаюче занепокоєння, оскільки вони ставлять під загрозу безпеку та безпеку людей та інфраструктури, не кажучи вже про ризик для літаків, що наближаються, і часто неминучу зупинку операцій на час усунення загрози.

Іншим значним типом загрози, що впливає на цивільну авіацію, є загроза, яку створюють інсайдери (додаткову інформацію див. у вмісті 4).

Джерело: представник ICAO.

1.2. Характер терористичних загроз KI

Загрози KI, пов'язані з тероризмом, мають кілька вимірів. У наступних розділах такі загрози розподіляються залежно від їх природи (фізична чи кібернетична), походження (інсайдерська чи зовнішня) та контексту, у якому вони виникають (ізольована чи кілька цілей). Розуміння типів загроз, яким піддається KI, є першим кроком у процесі розробки адекватних стратегій захисту, як обговорюється в розділі 2.

1.2.1. Фізичні загрози проти кіберзагроз

Фізичні загрози KI можуть мати різні форми. Їхньою спільною характеристикою є те, що вони спрямовані на руйнування інфраструктури, її ослаблення або виведення з ладу повністю або частково через порушення її фізичної структури, механічних компонентів та інших атрибутів.

Найбільш інтуїтивно зрозумілі фізичні загрози KI передбачають використання саморобних вибухових речовин або запальних пристроїв, транспортних засобів, ракет, переносних систем протиповітряної оборони, гранат і навіть простих інструментів (таких як сірники або запальнички, при підпалах) і так далі, щоб досягти повного або часткового руйнування або руйнування об'єкта. Атаки також можуть передбачати навмисну модифікацію або маніпулювання системами та процесами KI (наприклад, увімкнення та вимкнення засобів, ініціювання або звільнення закриття в системах трубопроводів, придушення сигналів процесу, сигналів несправності або тривоги).

Розгортання хімічної, біологічної, радіологічної або ядерної зброї або речовин є ще одним типом загрози для KI. Такі атаки можуть здійснюватися шляхом розповсюдження інфекційних патогенів у ланцюгах постачання продуктів харчування,12 водопроводів, використання отруйного газу на ключових транспортних розв'язках і перехрестях тощо. Атака на критично важливий об'єкт, що містить такі матеріали, також може призвести до того, що сам об'єкт випустить такі матеріали.

Хоча кіберзагрози за своєю природою відрізняються від фізичних, кінцевий результат може бути однаковим. Кіберзагрози відрізняються, але можуть включати, наприклад, атаки, які призводять до:

- Маніпулювання системами даних – наприклад, зловмисне програмне забезпечення, яке використовує вразливості в комп'ютерному програмному забезпеченні та апаратних компонентах, необхідних для роботи KI
- Вимкнення критично важливих систем, таких як атаки на відмову в обслуговуванні (також називаються «DoS»)[13]
- Обмеження доступу до критично важливих систем або інформації – наприклад, через атаки програм-вимагачіві[14]

Як показано в розділі 2.4.2, у той час як взаємопов'язані та інтегровані комп'ютеризовані системи управління значно оптимізували спосіб роботи KI та створили ринкову ефективність, розширене підключення може також збільшити поверхню атаки і, отже, наражати KI на високий ризик маніпулювання. .

Відповідно до опитування 200 керівників галузі, які працюють на критично важливих об'єктах для електроенергетики в 14 країнах, проведеному в приватному секторі, «[у 2010 році] майже половина респондентів сказали, що вони ніколи не стикалися з широкомасштабними атаками типу «відмова в обслуговуванні» або мережевими проникненнями. До [2011] ці цифри різко змінилися; 80 відсотків зіткнулися з широкомасштабною атакою відмови в обслуговуванні, а 85 відсотків зазнали проникнення в мережу».[15]

---

[12] У 1984 році салатні бари десяти ресторанів в Орегоні, США, були заражені сальмонелою. Напад організувала група людей, які прагнули вплинути на місцеві вибори. Інцидент ілюструє відносну легкість, з якою біотерористична атака може бути здійснена в критично важливому секторі, такому як ланцюг постачання продовольства.

[13] Нещодавнім прикладом атаки на відмову в обслуговуванні, яка безпосередньо вплинула на KI, була атака, здійснена проти датської системи бронювання залізничних квитків 14 травня 2018 року..

[14] SecurityWeek повідомляє, що в період з листопада 2013 року по 31 січня 2022 року було загалом 1137 атак програм-вимагачів на організації КІ, згідно з останньою версією бази даних атак програм-вимагачів Університету Темпл. Дослідники виявили, що охорона здоров'я, уряд та освіта були секторами, на які найбільше націлили протягом останніх чотирьох років. Для отримання додаткової інформації,Продивіться https://www.scmagazine.com/brief/ransomware/more-than-1k-ransomware-attacks-reported- against-critical-infrastructure.

[15] Макафі, «У темряві: критичні галузі протистоять кібератакам. Другий щорічний звіт McAfee про критичну інфраструктуру», 18 липня 2011 р., с. 6.Доступ https://www. publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx.

Вміст 3

Кіберзагрози критичній інформаційній інфраструктурі: висновки робочої групи відкритого складу щодо розробок у сфері інформації та телекомунікацій у контексті міжнародної безпеки

Створена відповідно до резолюції 73/27 Генеральної Асамблеї, робоча група відкритого складу з розробок у сфері інформації та телекомунікацій у контексті міжнародної безпеки забезпечує прозору та інклюзивну платформу для всіх держав-членів, щоб висловити свої погляди та розширити співпрацю про міжнародний аспект безпеки ІКТ.

З 2003 року шість разів створювалися групи державних експертів для вивчення існуючих і потенційних загроз у сфері інформаційної безпеки та можливих спільних заходів щодо їх подолання. За допомогою трьох консенсусних звітів, підготовлених у 2010, 2013 та 2015 роках, ці групи рекомендували 11 добровільних норм відповідальної поведінки держави та визнали, що з часом можуть бути розроблені додаткові норми. Грунтуючись на цьому фундаменті, робоча група відкритого складу шукала точки дотику та взаєморозуміння між державами-членами ООН щодо питання глобального значення. Щодо загроз для КІІ, робоча група відкритого складу дійшла наступних висновків:

- Існують потенційно руйнівні наслідки для безпеки, економічні, соціальні та гуманітарні наслідки зловмисних дій ІКТ для КІ та КІІ, що підтримують основні послуги для населення. Зловмисна діяльність ІКТ проти КІ та КІІ, яка підриває довіру до політичних і виборчих процесів, державних установ або впливає на загальну доступність чи цілісність Інтернету, також викликає справжнє та зростаюче занепокоєння.
- Діяльність у сфері ІКТ, що суперечить зобов'язанням згідно з міжнародним правом, яка навмисно пошкоджує критичну інфраструктуру або іншим чином погіршує використання та роботу критичної інфраструктури для надання послуг населенню, може становити загрозу не лише безпеці, але й державному суверенітету, а також економічному розвитку і засоби до існування, і, зрештою, безпека та добробут людей.
- Оскільки всі держави все більше покладаються на цифрові технології, відсутність обізнаності та відповідних можливостей для виявлення, захисту або реагування на зловмисну діяльність ІКТ може зробити їх більш уразливими. Як засвідчило поточна глобальна надзвичайна ситуація у сфері охорони здоров'я, існуюча вразливість може посилитися під час кризи.
- Держави можуть відчувати загрози по-різному залежно від рівня цифровізації, потенціалу, безпеки та стійкості ІКТ, інфраструктури та розвитку. Загрози також можуть мати різний вплив на різні групи та суб'єкти, зокрема на молодь, людей похилого віку, жінок і чоловіків, людей, які є вразливими, певних професій, малі та середні підприємства та інших..

Джерело: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Таблиця 1
Топ-10 загроз промисловим системам управління (ICS)

No.	Загроза	Пояснення
1	Несанкціоноване використання точок доступу віддаленого обслуговування	Точки доступу для обслуговування є навмисно створеними зовнішніми входами до мережі ICS і часто недостатньо захищені.
2	Онлайн-атаки через офісні або корпоративні мережі	Офісні інформаційні технології (IT) зазвичай підключаються до мережі кількома способами. У більшості випадків також існують мережеві підключення від офісів до мережі ICS, тому зловмисники можуть отримати доступ через цей маршрут.
3	Атаки на стандартні компоненти, що використовуються в мережі ICS	Стандартні IT-компоненти (комерційні готові), такі як системне програмне забезпечення, сервери додатків або бази даних, часто містять недоліки або вразливості, якими можуть скористатися зловмисники. Якщо ці стандартні компоненти також використовуються в мережі ICS, ризик успішної атаки на мережу ICS зростає.
4	DoS-атаки	(Розподілені) атаки типу «відмова в обслуговуванні» можуть порушити мережеві з'єднання та важливі ресурси та спричинити збій систем, наприклад, щоб порушити роботу ICS.

5	Людська помилка та саботаж	Навмисні дії – внутрішніх чи зовнішніх злочинців – становлять серйозну загрозу для всіх цілей захисту. Недбалість і людські помилки також є великою загрозою, особливо щодо конфіденційності та доступності цілей захисту.
6	Запровадження шкідливого програмного забезпечення через знімні носії та зовнішнє обладнання	Використання знімних носіїв і мобільних IT-компонентів сторонніх співробітників завжди тягне за собою великий ризик зараження шкідливим програмним забезпеченням.
7	Читання та запис новин в мережі ICS	Більшість компонентів керування наразі використовують протоколи відкритого тексту, тому зв'язок є незахищеним. Це робить його відносно легким для читання та введення команд керування.

8	Несанкціонований доступ до ресурсів	Внутрішнім зловмисникам і подальшим атакам, що відбуваються після початкового зовнішнього проникнення, особливо легко, якщо служби та компоненти в мережі процесів не використовують методи автентифікації та авторизації або якщо методи небезпечні.
9	Атаки на компоненти мережі	Зловмисники можуть маніпулювати мережевими компонентами, щоб, наприклад, здійснювати атаки типу "людина посередині" або полегшувати пошук.
10	Технічні несправності або форс-мажорні обставини	Збої в роботі внаслідок екстремальних погодних умов або технічних збоїв можуть виникнути в будь-який час - лише в таких випадках ризик і потенційну шкоду можна мінімізувати.

Джерело: ОБСЄ, Посібник із належної практики щодо захисту неядерної критичної енергетичної інфраструктури (NNCEIP) від терористичних атак із зосередженням на загрозах, що виходять із кіберпростору, Відень, 2013 р., с. 34. Доступ www.osce.org/files/f/docu-ments/4/b/103500.pdf

1.2.2. Внутрішні загрози проти зовнішніх загроз

У той час як захист KI від зовнішніх атак користується значною кількістю вказівок національних і міжнародних регуляторних органів, внутрішнім загрозам приділяється порівняно мало уваги. У порівнянні із зовнішніми суб'єктами, які можуть отримати доступ до KI лише за допомогою насильницьких дій або хитрощів, люди, що діють, так би мовити, зсередини, мають відмітні переваги. Часто це співробітники компанії або постачальники. Вони можуть бути головними змовниками або діяти як спільники (наприклад, інформатори) зовнішніх агентів. Вони часто мають можливість спостерігати за процесами протягом певного періоду часу. Їхні знання (або легкість, з якою вони можуть отримати знання) про відповідний об'єкт можна легко використати у злочинних цілях.

У розділі 2.6.2.2 наведено кілька прикладів заходів захисту KI від такого типу загрози. У цій сфері ключову превентивну роль можуть відігравати оператори KI, починаючи від впровадження ефективних процедур відбору та перевірки персоналу.

Вміст 4
Динаміка інсайдерської загрози в секторі цивільної авіації

Загроза, яку представляють інсайдери, залишається серйозною проблемою для сектору цивільної авіації, що посилюється обставинами, спричиненими пандемією коронавірусної хвороби (COVID-19). Незважаючи на те, що це не нова загроза, пандемія напружила багато авіаційних ресурсів і порушила нормальний спосіб життя, що, можливо, підвищило ймовірність матеріалізації цього конкретного типу загрози. Події внутрішньої загрози, зареєстровані на сьогоднішній день, такі як злочинна діяльність, якій сприяють співробітники авіації, зростають, про що свідчить виявлення зброї, захованої в багажі співробітниками авіакомпанії, або схема відмивання грошей, пов'язана з наркотиками, якій сприяв персонал аеропорту. Крім того, деяким зі збройних пограбувань та інших подібних злочинів, згаданих вище, могли сприяти інсайдери та особи з привілейованим доступом. Особи, пов'язані з терористичними групами, намагалися працевлаштуватися в аеропорту, а також в інших частинах транспортної системи, пов'язаної з авіацією. Ця тактика контрастує з більш поширеним

1.2.3. Ізольовані цілі проти кількох цілей

Загрози проти КІ можуть бути як ізольованими та спорадичними діями, так і частиною ширшого плану атаки на інфраструктуру в тому самому секторі (наприклад, енергетика, транспорт, телекомунікації), що належить одному власнику чи оператору або розташована в тій самій географічній зоні. Дії, вмотивовані тероризмом, спрямовані проти КІ, можуть сприйматися приблизно так само, як випадки промислового шпигунства, коли кібератаки часто запускаються як кампанії або серійні атаки. Наприклад, у 2011 році так звана атака зловмисного програмного забезпечення «Lurid» була націлена, серед іншого, на ІКТ-системи низки дипломатичних представництв та державних установ, пов'язаних з космосом. Інші атаки можуть охоплювати інфраструктуру, розташовану в кількох країнах і належати до різних критичних секторів. Наймасштабніша атака з будь-коли організованих на сьогоднішній день, як з точки зору її географічного охоплення, так і викликаних збоїв, – це атака крипто-хробака WannaCry, яка в травні 2017 року вивела з ладу залізничні системи в Німеччині та Російській Федерації, заблокувала лікарні у Великобританії втрутилася в телекомунікаційні мережі в Португалії та Іспанії та зашкодила нафтохімічним компаніям у Бразилії та Китаї.

Ідентифікація закономірностей у подібних складних сценаріях вимагає потужних аналітичних інструментів і обробки інформації з величезних і різнорідних джерел. Що ще більше ускладнює ситуацію, як підкреслила Організація з безпеки та співробітництва в Європі (ОБСЄ), посилаючись на енергетичний сектор, більшість кібератак не розголошується, оскільки відповідні оператори не бажають повідомляти про ці інциденти. У той же час здатність якомога раніше розпізнавати динаміку та методи, що лежать в основі, є ключовою для того, щоб органи влади могли ділитися актуальною інформацією. Це зміцнює здатність ефективніше реагувати на поточні атаки та запобігати неминучим атакам на ймовірних жертв.[16]

У деяких випадках те, що виглядає як ізольована атака, спрямована на відносно неважливі цілі, може насправді бути частиною більш амбітної та поступової злочинної стратегії[17]. Дуже важливо мати можливість якомога раніше визначити, чи є атака спорадичний акт проти однієї частини інфраструктури або є частиною серії запланованих атак на іншу інфраструктуру. Розвиток таких попередніх знань є важливим для профілактичних цілей.

1.3 Терористичні мотиви для нападу на КІ

Гетерогенна природа КІ разом із різними географічними та інституційними контекстами, в яких вона розташована та діє, робить надзвичайно складним зробити загальні висновки щодо того, що спонукає терористів здійснювати напади на КІ, на відміну від некритичних цілей. Однак аналіз терористичних мотивів все ще може надати корисні вказівки як частину ширшої оцінки загрози, необхідної відповідно до національних стратегій захисту критичної інфраструктури.

З обмежених емпіричних досліджень, проведених у цій галузі, випливає, що КІ є привабливим з різних причин. По-перше, деякі критичні об'єкти можуть бути привабливою ціллю через їхню стратегічну цінність для суспільства, зокрема у високоіндустріальних країнах Заходу. Втручання в їх функціонування, в ідеалі з можливістю створення каскадних ефектів, дозволить терористам максимізувати шкоду та вплив своїх дій одним пострілом і вселити страх на рівнях, яких було б не так легко досягти, атакуючи менш критичні цілі. Саме з цією метою, наприклад, як повідомляється, оперативники Аль-Каїди приділяли значну кількість часу стеженню за штаб-квартирами різних фінансових фірм і міжнародних організацій, розташованих у Сполучених Штатах. Можливо, ця ретельна діяльність була розпочата у відповідь на указ Усами бін Ладена 2001 року, який закликав його філії «зосередитися на завданні удару по економіці Сполучених Штатів усіма можливими засобами».[18]

Інші критично важливі об'єкти можуть стати мішенню для демонстрації безсилля державних інституцій. Наприклад, терористичні організації можуть вирішити атакувати об'єкти, що виробляють електроенергію, нафтопроводи та інші подібні установки, щоб припинити постачання основних послуг і виявити крихкість державних органів і відповідної державної політики.

---

16 ОБСЄ, Посібник із належної практики щодо захисту критично важливої неядерної енергетичної інфраструктури (NNCEIP) від терористичних атак із зосередженням на загрозах, що виходять із кіберпростору, Відень, 2013 р. Доступ https://www.osce.org/files/f/documents/4/b/103500.pdf.

17 У спільному звіті Міністерства внутрішньої безпеки та ФБР, опублікованому в 2017, зазначено, що певні урядові мережі США в енергетичному, ядерному, водному, авіаційному та критично важливих виробничих секторах були під загрозою цілеспрямованих передових постійних загроз. Департамент оцінив цю діяльність як «багатоетапну кампанію вторгнення суб'єктів загрози, націлену на низький рівень безпеки та невеликі мережі, щоб отримати доступ і перейти до мереж великих власників цінних активів в енергетичному секторі». Згідно зі звітом, «актори загрози [активно переслідували свої кінцеві цілі протягом довгострокової кампанії», а компанії, такі як сторонні постачальники, спочатку були об'єктами постановки. (Див.: Міністерство національної безпеки, «Розширена постійна загроза, спрямована на енергетику та інші сектори критичної інфраструктури», 20 жовтня 2017

р., Доступ www.us-cert.gov/ncas/alerts/TA17-293A. Див. також Коннер Форрест, «DHS, FBI попереджають про кібератаки, спрямовані на енергетичну інфраструктуру та державні установи», TechRepublic, 23 жовтня 2017 р. Доступ https://www.techrepublic.com/article/dhs-fbi-warn-of- cyberattacks-targeting-energy-infrastructure-government-entities/.

18 Гері Акерман та інші, Оцінка терористичних мотивів для нападу на критичну інфраструктуру, Центр досліджень нерозповсюдження, Монтерейський інститут міжнародних досліджень, 2007 р. Доступ https://digital.library.unt.edu/ark:/67531/metadc887957/m2/1/high_res_d/902328.pdf.

Третя можлива мотивація, пов'язана з двома попередніми, – це бажання отримати більший ступінь публічності, ніж
було б можливим, зосередившись на цілях нижчого профілю.
Як не парадоксально, але терористи можуть шукати контролю над КІ не для того, щоб завдати шкоди чи залякати, а з протилежної причини: з метою встановлення власної легітимності та соціальної прийнятності. Як було зазначено, хоча більшість операцій, проведених ДАІШ з використанням інфраструктури, пов'язаної з водою, були спрямовані на переривання пересування військ і боротьбу з військовими, «такі зусилля також часто [мали] додаткову користь у вигляді посилення зусиль вербування; дозволяючи воді текти в міста, які симпатизують справі Ісламської держави, або навіть просто покращуючи роботу з надання необхідних послуг, група [може] залучити більше чоловіків і жінок до своїх лав».[19]
У багатьох випадках, ймовірно, існує комбінація факторів, які спонукають терористичні групи вчиняти напади за участю КІ. Ці стимули також повинні бути збалансовані низкою обмежень. Остаточне рішення щодо того, яку інфраструктуру нанести удар, і спосіб роботи, який буде використано, залежатиме від таких факторів, як характеристики цільового сектора та вразливість окремої інфраструктури. Це також залежатиме від оперативних і фінансових можливостей терористичної групи здійснити конкретну атаку. Надійність заходів фізичного захисту, які діють на певному критичному об'єкті, природно впливатиме на таке рішення. Подібним чином, надійність процедур, які застосовуються керівництвом інфраструктури для пом'якшення внутрішньої загрози, також відіграватиме свою роль. Це не означає, що терористичні групи атакуватимуть КІ лише тоді, коли вони впевнені, що зможуть втрутитися в її операції. Проста спроба, навіть невдала або така, що завдає дуже обмеженої шкоди, може забезпечити бажаний рівень медіа-резонансу, зокрема, коли ціль вибрано через її символічну цінність.

1.4 Протидія терористичним загрозам КІ за допомогою підходу, який відповідає вимогам прав людини та гендерним аспектам

Тероризм становить серйозну загрозу не лише міжнародному миру та безпеці, але й самим принципам верховенства права та захисту прав людини. Держави-члени вживають заходів для ефективної протидії та запобігання тероризму в рамках своїх зобов'язань згідно з міжнародним правом прав людини. Це зобов'язання має особливе значення з огляду на потенційний вплив, який атаки

на КІ можуть мати на населення, враховуючи роль, яку така інфраструктура часто відіграє у виконанні життєво важливих соціальних функцій. Пошкодження, порушення або знищення критичної інфраструктури може призвести до далекосяжного впливу на широкий спектр прав людини, від права на життя та особисту безпеку до права на здоров'я та здорове довкілля, права на освіту, а також право на воду, санітарію та інші передумови належного рівня життя.

Обов'язок держав захищати права людини передбачає зобов'язання вживати необхідних і адекватних заходів для запобігання, боротьби та судового переслідування діяльності, яка загрожує цим правам, наприклад, загроз національній безпеці або насильницьких злочинів, включаючи тероризм. У цьому відношенні держави повинні керуватися, серед іншого, Глобальною контртерористичною стратегією ООН, яка підкреслює, що ефективна боротьба з тероризмом і забезпечення поваги до прав людини є не конкуруючими, а доповнювальними та взаємодоповнювальними цілями. Хоча заохочення та захист прав людини можуть становити незалежну основу Стратегії, вони також є важливими для успішного виконання всіх чотирьох її компонентів.

Рада Безпеки також послідовно й неодноразово підтверджувала, що держави повинні забезпечити відповідність будь-яких заходів, спрямованих на протидію тероризму, усім їхнім зобов'язанням згідно з міжнародним правом, зокрема міжнародним правом прав людини, міжнародним правом щодо біженців і міжнародним гуманітарним правом. Крім того, у своїй резолюції 2178 (2014) Рада Безпеки заявила, що невиконання цих та інших міжнародних зобов'язань, у тому числі відповідно до Статуту Організації Об'єднаних Націй, створює відчуття безкарності та є одним із факторів, що сприяють зростанню радикалізації.

---

19 Амбіка Вішванатх, «Водні війни, які веде Ісламська держава», Stratfor, 2015 р. Доступ https://worldview.stratfor.com/article/water-wars-waged-islamic-state.

Стратегії боротьби з тероризмом, у тому числі ті, що застосовуються для захисту КІ, повинні також враховувати гендерні та вікові особливості, найкращі інтереси дитини та різний вплив тероризму та насильницького екстремізму, що сприяє тероризму, на права людини жінок і дівчат..[20]

В інтересах протидії терористичним загрозам КІ органи державної влади можуть тимчасово вживати заходів, які призводять до обмеження певних прав, за умови, що ці обмеження відповідають умовам, викладеним у міжнародному праві прав людини. Заходи, вжиті в цьому відношенні, повинні бути справжньою відповіддю на наявну загрозу, що вимагається гостротою ситуації, мати чітку правову основу та бути пропорційними досягненню законних цілей. Держави повинні забезпечити встановлення задовільних гарантій для захисту від свавільного та непропорційного втручання в права людини в цьому контексті.

Для суттєвого дотримання цих зобов'язань держави повинні проводити регулярні оцінки прав людини щодо заходів, вжитих для боротьби з терористичною загрозою для КІ, і переконатися, що такі заходи базуються на фактах і, отже, є ефективними, не посилюють відчуження, упередження чи упередження, а також не перешкоджають доступ або використання простору певними групами чи населенням. Подібним чином інтеграція ґендерних аспектів у CIP є невід'ємною частиною ефективних та дієвих стратегій зменшення ризиків, оскільки враховує не лише ґендерно-специфічні потреби безпеки жінок, чоловіків, хлопчиків та дівчат, а й те, як лежать в основі гендерні стосунки, стереотипи. і динаміка впливає на моделі безпеки та вразливості.

[20] Доповнення до Мадридських керівних принципів (S/2018/1177).

2. Розробка національних стратегій КІІ проти терористичних атак

Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки

...

2. Закликає держави-члени розглянути можливість розробки або подальшого вдосконалення своїх стратегій зменшення ризиків для критичної інфраструктури від терористичних атак, які повинні включати, серед іншого, оцінку та підвищення обізнаності щодо відповідних ризиків, вжиття заходів готовності, включаючи ефективну відповідь на такі атаки, а також просування кращої сумісності в сфері безпеки та управління наслідками, а також сприяння ефективній взаємодії всіх зацікавлених сторін

Додаток до Мадридських керівних принципів

Керівний принцип 50

2.1 Чому національна стратегія?

Більшість держав-членів забезпечили заходи безпеки для своїх КІ задовго до того, як КІІ затвердилася як окрема сфера політики. Захисні заходи здебільшого ухвалювалися поетапно та по частинах у формі нормативних актів, що охоплювали конкретні сектори чи загрози, або зосереджувалися на певних частинах процесів управління ризиками та кризами. У деяких випадках державна політика досягла значного рівня складності та відповідає найвищим міжнародним стандартам.

Як наслідок, можна запитати, чому держави-члени повинні розробляти загальні загальнонаціональні стратегії CIP, коли вони вже мають детальні правила, політику та

практику, що охоплюють більшість, якщо не всі, критичні сектори. Найбільш вагомою причиною є те, що в сучасних суспільствах захист KI стає все більш наскрізним і міждисциплінарним завданням. Взаємозалежність між секторами з можливістю каскадних ефектів у разі аварій (природного походження чи антропогенних) вимагає здатності бачити загальну картину, так би мовити, як умови для ефективної координації запобігання , заходи реагування та відновлення в різних секторах. Крім того, спираючись на суто галузеву – або так звану «вертикаль» – підходи можуть надмірно збільшити кількість залучених установ, спричинити дублювання зусиль і марну витрату ресурсів. Таким чином, комплексна стратегія CIP спрямована на раціоналізацію робочих процесів, економію масштабу та кращий розподіл фінансових і людських ресурсів навколо набору заздалегідь визначених цілей.

Це не означає, що загальнонаціональні стратегії CIP повинні замінити існуючі заходи захисту в окремих галузях, зокрема, якщо ці заходи виявилися успішними або відповідають міжнародним нормативним рамкам або визнаним найкращим практикам. Однак державам-членам необхідно об'єднати різні частинки мозаїки та зробити їх частиною узгодженої системи управління. Стратегії CIP мають бути розроблені відповідно до конкретних потреб і підходів окремих країн.

Як показано в розділі 2.5, держави-члени прийняли різноманітні інституційні моделі, що відображають не лише їхні специфічні правові традиції, але й відносини між урядом, громадянами та приватним сектором. Країни мають значний простір для маневру у визначенні способів захисту своїх KI. Проте всі вони повинні мати концептуальні будівельні блоки (стратегію), щоб з'єднати точки та забезпечити плавні робочі відносини між усіма зацікавленими сторонами. Зважаючи на це, основними цілями загальнонаціональної міжгалузевої стратегії мають бути:

- Визначити сектори, які слід розглядати як критичні, і розробити методологію визначення конкретних активів і процесівяк критичний (див. розділ 2.4.1)
- Визначити та надати повноваження державній установі, відповідальній за координацію та управління зусиллями щодо захисту на національному рівні, що включає сприяння та підтримку реалізації стратегії різними залученими зацікавленими сторонами (див. розділ 2.5).
- Розподілити інституційні обов'язки на рівні кожного критичного сектору та різних рівнів управління (місцевий, державний, федеральний) (див. розділ 5)
- Визначити методології для запобігання та реагування на терористичні атаки проти KI після ризику та кризи підхід до управління (див. розділ 2.6)
- Окреслити форми, канали та процедури постійного обміну інформацією та координації

між компетентними державними установами та приватним сектором, зокрема власниками та операторами КІ (див. розділ 2.5.2)

Інструмент 1
Рекомендації ОБСЄ щодо управління критичними ризиками

www.oecd.org/gov/risk/recommendation-on-governance-of-critical-risks.htm

Прийнята Радою Організації економічного співробітництва та розвитку (ОБСЄ) у 2014 році, Рекомендація пропонує фундаментальний перехід в управлінні ризиками до зусиль усього суспільства. Вводячи поняття «критичного ризику», він пропонує набір дій, які уряди можуть вживати на всіх рівнях управління, у співпраці з приватним сектором і один з одним, щоб краще оцінювати, запобігати, реагувати на наслідки та відновлюватися після них. екстремальних подій (як природних, так і антропогенних), а також вжити заходів для підвищення стійкості до відновлення після непередбачених подій.

У Рекомендації визначено чотири головні міркування, які уряди повинні взяти до уваги, щоб зробити суспільство більш стійким до критичних ризиків:

- Ідентифікація та оцінка ризиків повинні враховувати взаємозв'язки та додаткові ефекти. Це допомагає встановити пріоритети та інформовано розподілити ресурси.
- Слід робити більше інвестицій у запобігання та пом'якшення ризиків - наприклад, інвестиції в захисну інфраструктуру - а також у неструктурні політики, такі як планування землекористування.
- Слід розвивати гнучкі можливості для готовності, реагування та відновлення, щоб допомогти впоратися з непередбаченими та новими типами криз.

Інструмент 2

ОБСЄ, Належне врядування для стійкості КІ, огляд ОБСЄ політики управління ризиками, 2019

www.oecd.org/gov/risk/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm

Визнаючи глобальне збільшення інвестицій в інфраструктуру та цифрову трансформацію інфраструктурних послуг, у цьому звіті аналізується мінливий контекст і розглядаються варіанти політики та моделі управління для здійснення початкових інвестицій у стійкість. На основі міжнародного опитування він аналізує поступовий перехід політики КІ від захисту активів до стійкості системи.

Системний підхід розуміється як підхід, за якого уряди та оператори інфраструктури вирішують взаємозалежність активів і визначають пріоритетність заходів стійкості для критичних концентраторів і

Інструмент 3

Агентство з кібербезпеки та безпеки інфраструктури (CISA), Сполучені Штати: посібник із безпеки та стійкості критичної інфраструктури

www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Посібник містить огляд підходу до безпеки та стійкості критичної інфраструктури, прийнятого в Сполучених Штатах. Замість того, щоб просувати конкретні підходи, мета полягає в тому, щоб поділитися основною інформацією та уроками, отриманими за останні 15 років. Інформація може стосуватися інших країн, зокрема

2.2 Підходи, що стосуються всіх небезпек і специфічних ризиків

Загрози, з якими стикається КІ, є поліморфними за своєю природою. Вони можуть бути природними: так, 11 березня 2011 року землетрус з наступним цунамі спровокував велику ядерну аварію у Фукусімі, Японія. Вони можуть походити від недбалої поведінки людини. У 2006 році відключення електроенергії торкнулося 10 мільйонів людей по всій Європі після дій оператора електропередачі, який вимкнув кабель живлення через річку Емс, щоб дозволити пройти круїзному лайнеру.

Інші загрози можуть бути прямим результатом людської поведінки, спрямованої на досягнення пов'язаних з тероризмом чи інших кримінальних цілей. Кібератаки з метою отримання викупу є все більш поширеним прикладом прибуткової діяльності, яка може серйозно вплинути на КІ через шифрування даних користувачів і вимагання оплати в обмін на розблокування даних. Загрози КІ також можуть бути пов'язані зі злочинною поведінкою більш тонкими та непрямими способами. У Європі французька будівельна асоціація Fédération française du bâtiment неодноразово застерігала

від причетності злочинних мереж до торгівлі контрафактними та неякісними будівельними матеріалами. Повідомляється, що багато компаній у будівельному секторі придбали невідповідні, низькоякісні матеріали, що ставить під загрозу надійність критично важливих активів і піддає їх підвищеному ризику руйнування.

Оскільки держави-члени покликані захищати КІ від багатьох типів ризиків, ключовим питанням є: чи повинні уряди прийняти єдиний план, що охоплює всі можливі загрози, чи радше передбачити прийняття стратегій щодо небезпеки чи ризику? В принципі, будь-який підхід узгоджується з міжнародно-правовою базою, включаючи резолюцію 2341 (2017).

Серед держав-членів, які прийняли стратегії КІІ, більшість дотримується підходу, що враховує всі небезпеки[21]. Це означає, що стратегічні цілі та організаційні структури сформовані таким чином, щоб враховувати випадкові, навмисні та природні загрози для КІ в цілісній системі. спосіб. Підхід до всіх небезпек часто розглядається як передумова найкращого використання обмежених доступних ресурсів і уникнення непотрібного дублювання. Основне обґрунтування полягає в тому, що однакові процеси управління ризиками та співробітництва, а також механізми реагування на кризи можуть широко використовуватися для невиразної реакції на всі типи загроз. Підходи, що враховують усі небезпеки, впроваджені такими країнами, як Канада та Велика Британія.

Інші країни використовують змішаний підхід. Австралія, наприклад, розробила спеціальні вказівки щодо захисту КІ від терористичних атак[22]. Вказівки доповнюють загальну стратегію країни щодо КІІ, яка поширює її охоплення на інші небезпеки. В Іспанії інституційна архітектура КІІ викладена в Законі 8/2011, який встановлює заходи для захисту КІ. На відміну від інших країн, іспанське законодавство зосереджено на протидії терористичній загрозі, хоча воно стосується інших – невизначених – ризиків.

Резолюція 2341 (2017) зобов'язує всебічно відобразити терористичну загрозу в підготовці стратегічних планів урядів щодо захисту КІ. Маючи це на увазі, кожну державу-члена заохочують визначити, як питання національної політики, найбільш ефективні форми та способи захисту КІ від терористичних актів у середовищі з багатьма загрозами.

2.3 Стратегії КІІ у порівнянні з іншими національними політиками

Більшість держав-членів, у тому числі ті, які не запровадили спеціальні стратегії КІІ, вирішують проблеми, пов'язані з КІІ, на практиці за допомогою різноманітних політичних інструментів, розроблених різними урядовими установами. Ці документи, як правило, мають форму стратегій національної безпеки (включаючи кібербезпеку), політик щодо боротьби з тероризмом і захисту легких цілей. Хоча ці різні політики могли бути прийняті в різний час і кількома урядовими установами, життєво важливо, щоб їхні компоненти, пов'язані з КІІ, були частиною узгодженого повідомлення та стратегії. Це вимагає, зокрема, від держав-членів визначення:

- Взаємодія між існуючими політиками (щодо боротьби з тероризмом, національної безпеки та інших подібних питань) і спеціальною стратегією КІІ
- Ступінь, до якого існуюча політика та стратегія CIP повинні бути скориговані та

оптимізовані, щоб уникнути суперечливі результати, які ускладнять або унеможливлять реалізацію

Коли розробляється національна стратегія щодо КІІ, важливо зробити перелік усіх національних політик, які можуть впливати на питання КІІ або перетинатися з ними. Якщо вони по суті зачіпають питання, пов'язані з КІ, їх слід ретельно перевірити з метою забезпечення їх сумісності та доповнення до нещодавно розроблених національних стратегій КІІ.

2.3.1. Політика щодо м'яких цілей

Як добре показано спеціалізованими тематичними модулями, які доповнюють цей Збірник, м'якими цілями є типи вразливих об'єктів (таких як релігійні, туристичні та міські об'єкти, музеї, кінотеатри, торгові центри, наземні та громадські зони аеропорту, спортивні споруди тощо), чий відкритий характер і високий ступінь доступності роблять їх особливо вразливими для терористичних атак. Часто легкі цілі пропонують терористам ідеальний майданчик для удару з невеликими зусиллями планування, водночас спричиняючи масові втрати.[23]

---

21 У контексті авіації ICAO використовує слово «небезпеки» для позначення питань, пов'язаних з безпекою. Події, пов'язані з безпекою, точніше визначити як «інциденти».

22 Див. Національні рекомендації щодо захисту критичної інфраструктури від тероризму, доступні за адресою www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf.

Спеціалізовані тематичні модулі забезпечують широкий аналіз особливостей і характеристик м'яких цілей, а також вказівки та передову практику щодо політики та оперативних дій для усунення їх вразливості та підвищення їх стійкості перед лицем терористичних актів.

Поняття «м'яких цілей» концептуально відрізняється від поняття KI, яке в широкому сенсі стосується активів, систем і процесів, життєво важливих для надання основних послуг і порушення яких може спричинити значні негативні наслідки для безпеки, соціального та економічного добробуту. - буття спільноти.

Таким чином, ключовим елементом відмінності між м'якими цілями та KI є їх ступінь «критичності». М'які цілі самі по собі не є критичними для надання основних соціальних послуг. Крім того, м'яка ціль зазвичай є фізичним місцем, тоді як критична інфраструктура також може бути процесом, включаючи інформаційні системи та мережі (див. розділ 2.4.2). Крім того, на відміну від м'яких цілей, помітною особливістю KI є здатність генерувати так звані «каскадні ефекти», за допомогою яких збої в одному секторі мають потенційний ефект доміно, вражаючи інші сектори та призводячи до паралічу всієї системи (див. розділ 2.4). Критерії, які використовують країни для визначення інфраструктури, яка заслуговує на особливий рівень захисту – засновані на моделях прогнозування серйозності, тривалості, географічного масштабу та економічних наслідків руйнівних подій – навряд чи підходять для визначення того, що є м'якою ціллю.

Основним наслідком цих відмінностей є те, що політика та структура держав-членів щодо м'яких цілей не задовольняє автоматично умови та вимоги щодо захисту KI. Однак це не означає, що дві зони потрібно обробляти в силосах. Навпаки, логіка та досвід показують, що країнам доцільно уникати розділеного підходу та натомість розвивати синергію як частину своєї загальної політики захисту від терористичних актів. Пам'ятаючи про відмінності в концептуальних і нормативних структурах, застосовних до м'яких цілей і KI, слід систематично досліджувати потенціал взаємодоповнюваності. Обґрунтування скоординованого підходу випливає з низки міркувань, зокрема наступних:

- Одні й ті самі державні установи часто несуть інституційні та операційні обов'язки в обох сферах.
- Успішні заходи, розроблені та впроваджені в галузі KII, також можуть бути застосовані для захисту м'яких цілей і навпаки. Наприклад, різні заходи, прийняті для забезпечення фізичної безпеки KI, також зазвичай використовуються для контролю доступу до м'яких цілей (таких як охоронні пости, огорожі, металошукачі тощо).
- Уроки, засвоєні в одній сфері, можуть бути легко – хоча і не автоматично – перенесені в іншу, в тому числі щодо досягнень і невдач, спостережених у зменшенні ризиків та

управлінні кризою.

- Як критична інфраструктура, так і «м'які цілі» зазвичай належать і управляються приватними організаціями, що робить розвиток державно-приватного партнерства (PPP) центральною рисою заходів щодо готовності та захисту обох..

Вміст 5

Порушення КІ та м'яких цілей: взаємодія

КІ часто має вирішальне значення для функціонування м'яких цілей. Наприклад, для проведення спортивної події необхідне безперебійне електропостачання. У той же час, збій у наданні основних послуг, таких як електрика, може не просто залишити присутніх у концертному залі в темряві та перервати виступ, але може бути частиною стратегії ускладнення евакуації під час теракт. У той же час успішна терористична атака на багатолюдний туристичний або релігійний об'єкт може призвести до краху КІ - і навіть цілого критичного сектору. Наприклад, лікарні можуть швидко переповнюватися, а комунікаційні мережі перестають працювати, оскільки вони переповнені запитами користувачів. Атаки на легкі цілі можуть мати особливо серйозні наслідки для СІ, коли вони відбуваються в міських районах, де вони співіснують і взаємодіють у складних і густонаселених просторах, що лежить в основі необхідності підходу, який розглядає обидва як частину єдиної багатогранної системи.

Наведені вище приклади показують, що зусилля із захисту КІ та м'яких цілей потребують тісної політичної,

ВИВЧЕННЯ ПРОБЛЕМИ 1
Інтеграція KI та систем захисту м'яких цілей: Бельгія та Німеччина

«Федеральні пам'ятки» Бельгії

Бельгійський Закон про захист критичної інфраструктури від 1 липня 2011 року містить поняття «федеральні об'єкти інтересу» («points d'intérêt fédéral»). Вони визначаються як «місця, не призначені як критична інфраструктура, але становлять особливий інтерес для громадського порядку, для спеціального захисту людей і майна, для управління надзвичайними ситуаціями або для військових інтересів, і які можуть вимагати захисних заходів, вжитих під час кризи. Головне управління Центру».

Бельгійський закон пропонує приклад єдиної нормативної бази, що враховує як КІ, так і м'які цілі. Незважаючи на те, що так звані «федеральні об'єкти інтересу» не відповідають умовам, щоб вважатися КІ, вони все одно вважаються гідними особливої уваги та захисту.

Системна проти символічної критичності в Німеччині

Німецька національна стратегія захисту критичної інфраструктури розрізняє критичність системного характеру та критичність, яка є просто символічною. Вважається, що інфраструктура є «системно критичною», коли - завдяки своєму структурному, функціональному та технічному положенню в загальній системі секторів інфраструктури - вона є дуже актуальною з огляду на її взаємозалежність. Прикладами є електрика та IT-інфраструктура, які, зважаючи на розмір і щільність мережі, можуть спричинити серйозні збої в житті та процесах громади щоразу, коли відбувається широкомасштабне та тривале відключення. Навпаки, інфраструктура може бути «символічної критичності», якщо її втрата через її культурне значення чи важливу роль у створенні почуття ідентичності може мати емоційний вплив і тривалий і психологічний вплив на суспільство.

Sources: www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf;jsessionid=C71D9BB-5FA7E4A7115D27E77116449A3.1_cid287?__blob=publicationFile&v= and www.nbb.be/doc/cp/fr/2018/20180925_loi_du_1juillet2011.pdf

2.3.2. Політика національної безпеки

Національна безпека – це мінливе поняття. Держави-члени перетворюють цю концепцію на різні підпункти та підходи залежно від ряду факторів і уявлень, що ґрунтуються на їхній конкретній історії, географічному положенні чи геополітичному контексті. У більшості випадків національна безпека охоплює принципи, політику, процедури та функції, спрямовані на гарантування незалежності, суверенітету та цілісності країни, а також прав її громадян.

Деякі країни прямо включають KII серед своїх пріоритетів національної безпеки. Тісний зв'язок KII зі сферою цілей національної безпеки може допомогти забезпечити посилену політичну підтримку для подальшої розробки спеціальних стратегій KII та сприяти їх реалізації.

ВИВЧЕННЯ ПРОБЛЕМИ 2
Інтеграція КІІ у стратегії національної безпеки: Польща та Іспанія

Польща

Стратегія національної безпеки до 2020 року містить чітке посилання на КІІ у своїй частині, яка стосується «Стійкості держави та спільної громадянської оборони». Розділ 2.8 Стратегії передбачає впровадження «моделі захисту критичної інфраструктури, забезпечення її безперервного функціонування та безперебійного надання послуг». Стратегія також містить керівні принципи щодо КІІ у конкретних секторах, таких як охорона здоров'я, економічна та енергетична безпека.

Іспанія

Стратегія національної безпеки до 2021 *року визначає* КІ *як вісь, на якій сформульовано фізичну стійкість країни. Стратегія зосереджена на необхідності сприяння профілактичному аспекту національної системи* КІІ*, з особливим наголосом на захисті комп'ютерних систем* КІ *та операторів основних послуг від кіберзагроз.*

2.3.3 Політика боротьби з тероризмом

Хоча в більшості стратегій боротьби з тероризмом КІ конкретно не згадується, низка цілей та інституційних заходів, викладених у цих стратегіях, відіграють важливу роль у збереженні цілісності КІ та життєво важливих соціальних функцій, які вона виконує. Наприклад, стратегії боротьби з тероризмом неявно стосуються питань КІІ, коли вони встановлюють процедури загального управління кризою після терористичної атаки. Крім того, стратегії боротьби з тероризмом часто встановлюють широкі рамки для запобігання скоєнню терористичних злочинів (наприклад, шляхом розгляду підготовчих дій, створення синергії між розвідувальними та правоохоронними спільнотами та іншими подібними заходами).

Стратегії КІІ повинні інтегрувати концепції та процедури, викладені в рамках політики боротьби з тероризмом, адаптуючи їх до конкретних потреб і контексту КІІ.

ВИВЧЕННЯ ПРОБЛЕМИ 3
Захист КІ через законодавство про боротьбу з тероризмом: Республіка Молдова та Португалія

Республіка Молдова

Положення про захист критичної інфраструктури від тероризму (постанова Уряду № 701) встановлює процес планування, організації та реалізації заходів з протидії терористичному захисту об'єктів КІ шляхом раціоналізації використання наявних людських, фінансових і матеріальних ресурсів та врахування враховувати конкретні вразливості КІ.

Постанову прийнято в рамках Закону № 120 «Про запобігання та боротьбу з тероризмом», який забезпечує нормативну та організаційну основу для координації правоохоронних заходів компетентними органами. Також встановлюються обов'язки тих, хто бере безпосередню участь в антитерористичних операціях, і окреслюються права жертв терористичних атак.

Португалія

Захист КІ є частиною Національної стратегії боротьби з тероризмом країни, яка базується на п'яти стовпах: «виявлення, запобігання, захист, переслідування та реагування». Метою компонента «захист» є зміцнення безпеки пріоритетних цілей, і в цьому відношенні захист приймає форму підвищення безпеки людей, кордонів, руху капіталу, товарів, транспорту, енергії та критичної інфраструктури, як національний і європейський.

У Національній антитерористичній стратегії йдеться про розробку плану дій щодо захисту КІ та підвищення її стійкості. За підготовку планів безпеки відповідають окремі оператори КІ, тоді як зовнішні плани безпеки підпадають під повноваження збройних сил, служб безпеки та Національного управління цивільного захисту.

Крім того, у 2016 році під егідою Системи внутрішньої безпеки країни була створена робоча група із захисту КІ. Таким чином, стало можливим гармонізувати процедури аналізу компоненту безпеки планів безпеки операторів. Робоча група періодично збирається та виконує свій мандат, забезпечуючи захист критичної інфраструктури в енергетичному та транспортному секторах.

Джерело: Інформація надана постійними представництвами Республіки Молдова та Португалії при ООН.

2.3.4. Політика кібербезпеки

Глобальний форум кіберекспертизи (GFCE) визначає кібербезпеку як «сукупність інструментів, політик, концепцій безпеки, заходів безпеки, інструкцій, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можна використовувати для захисту кіберсередовище, організація та активи користувачів»[24]. Політики кібербезпеки займають центральне місце в захисті КІ, оскільки вони забезпечують основу, за якою країни визначають цілі та засоби для захисту критично важливих інформаційних інфраструктур (КІ). Далі ця концепція розглядається в розділі 2.4.2.

Ряд регіональних документів прямо пов'язує концепції кібербезпеки з КІ. Наприклад, Конвенція Африканського Союзу про кібербезпеку та захист персональних даних (2014) вимагає від держав-учасниць «зобов'язатися

[24] Global Forum on Cyber Expertise (GFCE) Foundation, *GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy- Makers*, GFCE-Meridian, 2016. Available at https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

розробити у співпраці із зацікавленими сторонами національну політику кібербезпеки, яка визнає важливість критичної інформаційної інфраструктури (CII) для нації, визначає ризики, з якими стикається нація під час використання підходу, що охоплює всі небезпеки, і описує, як мають бути досягнуті цілі такої політики» (ст. 24, «Національна структура кібербезпеки»).

Зважаючи на це, не всі національні стратегії кібербезпеки надають KI однакове місце та вагу, і між країнами існують значні відмінності. Як зазначено в GFCE-Meridian Good Practice Guide, «деякі стратегії були написані з точки зору лише кіберзлочинності або лише з точки зору Інтернету. Вони, як правило, не помічають (національний) зрив і управління кризою для KII, а також міжсекторальний вплив. Стратегії, написані з точки зору кібербезпеки на основі національної оцінки ризиків, сприйматимуть ширшу перспективу, яка дасть можливість для KII» (с. 8).

Вміст 6

Підхід Європейського Союзу до кібербезпеки

Європейський Союз побудував свою політику кібербезпеки навколо трьох основних стовпів, які безпосередньо стосуються захисту KI: стратегія кібербезпеки; законодавча база; і режим санкцій проти кібератак.

Стратегія кібербезпеки

У грудні 2020 року Європейська комісія та Європейська служба зовнішніх дій представили нову стратегію кібербезпеки Європейського Союзу. У документі містяться пропозиції щодо впровадження нових регуляторних, інвестиційних та політичних інструментів. 22 березня 2021 року Європейська рада прийняла висновки щодо стратегії кібербезпеки, встановивши ключовою метою досягнення стратегічної автономії при збереженні відкритої економіки. Це включає посилення здатності приймати автономні рішення у сфері кібербезпеки з метою зміцнення цифрового лідерства та стратегічного потенціалу Європейського Союзу.

Законодавча база: Закон про кібербезпеку

Закон Європейського Союзу про кібербезпеку, який набув чинності в червні 2018 року, запровадив наступне:

- Загальноєвропейська схема сертифікації: цю схему було створено з огляду на той факт, що різні схеми сертифікації безпеки, які зараз використовуються різними державами-членами Європейського Союзу, створюють фрагментацію ринку та регуляторні бар'єри. Очікується, що загальноєвропейська схема сертифікації відіграватиме вирішальну роль у забезпеченні високих стандартів кібербезпеки для продуктів, послуг і процесів ІКТ.
- Новий і посилений мандат Агентства Європейського Союзу з кібербезпеки: Спираючись на структури свого попередника, Агентства Європейського Союзу з мережевої та інформаційної безпеки, Агентство підтримує держави-члени, інституції Європейського Союзу та інші зацікавлені сторони у боротьбі з кібератаками.

Законодавча база: Директива про мережеві та інформаційні системи (NIS)

Директива NIS була запроваджена в 2016 році як перший в історії Європейський Союз законодавчий захід з метою зміцнення співпраці між державами-членами щодо кібербезпеки. Він встановив зобов'язання щодо безпеки для операторів основних послуг (у таких критичних секторах, як енергетика, транспорт, охорона здоров'я та фінанси) і для постачальників цифрових послуг (онлайн-ринки, пошукові системи та хмарні сервіси). У грудні 2020 року Європейська комісія запропонувала переглянуту директиву NIS (NIS2) на заміну директиві 2016 року. Нова пропозиція відповідає мінливому ландшафту загроз і враховує цифрову трансформацію, яку прискорила криза COVID-19.

Нові правила, для яких Рада розробила загальний підхід у грудні 2021 року, спрямовані, серед інших цілей, на посилення зобов'язань безпеки для підприємств і ланцюгів постачання, запровадження більш суворих заходів нагляду для національних органів влади та розширення обміну інформацією та співпраці

Режим санкцій проти кібератак

У травні 2019 року Рада встановила рамки, що дозволяють Європейському Союзу вперше накладати санкції на осіб або організації, відповідальних за кібератаки або спроби кібератак, які надають фінансову, технічну чи матеріальну підтримку для таких атак або які причетні іншим чином. . Обмежувальні заходи включають заборону на в'їзд осіб до Європейського Союзу та замороження активів фізичних та юридичних осіб. Перші санкції за кібератаки були введені 30 липня 2020 року.

Джерело: https://www.consilium.europa.eu/en/policies/cybersecurity/.

2.4 Яка інфраструктура є критичною?

Додаток до Мадридських керівних принципів

Керівний принцип 50

У своїх зусиллях щодо розробки та впровадження заходів для захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевими органами влади, повинні:

Резолюція Ради Безпеки 2341 (2017) чітко визнає у своїй преамбулі, що «кожна держава визначає, що є її критичною інфраструктурою». Однак у ньому не зазначено, які конкретні критерії мають використовувати держави-члени для вибору певних активів і процесів серед безлічі активів, розташованих на їхніх територіях. Інші міжнародні документи також не містять вказівок щодо цього.[25]

Таким чином, держави-члени мають значну свободу вибору критеріїв для визначення того, яка інфраструктура, що працює на їхній території, задовольняє порогу «критичності». Завдання не є тривіальним: виділення інфраструктури, яка має набути «критичного» статусу, є ключовим для того, щоб мати можливість визначити пріоритетність обмежених ресурсів для захисту кількох активів, систем і процесів. З одного боку, включення занадто великої кількості об'єктів до категорії «критичних» може стати некерованим (крім того, що це буде фінансово нежиттєздатним). З іншого боку, занадто обмежувальний підхід створює ризик залишити ряд ключових активів і процесів незахищеними з потенційно катастрофічними наслідками в разі аварії. Як було зазначено, уряди мають тенденцію розширювати, а не звужувати свої національні списки KI. Це відбувається тому, що, як зазначає Департамент міжнародної безпеки Chatham House Великобританії, «занадто мало осіб, які приймають рішення, готові прийняти політичний ризик, який може виникнути з видаленням пункту зі «критичного» списку, і виникає спокуса постійно розширювати коло речей, які вважаються критичними. Такий рівень неоднозначності є марнотратним, оскільки ресурси не спрямовуються туди, де вони можуть мати найбільший вплив».[26]

Держави-члени, які планують прийняти політику або нормативну базу для ідентифікації власних KI, можуть черпати натхнення з методологій, які використовують інші держави-члени. У наступних підрозділах наведено посилання на деякі широко використовувані методології та ілюстровано три основні кроки, які уряди повинні розглянути.

[25] Конвенція Африканського Союзу про кібербезпеку, наприклад, обмежується вимогою, щоб «кожна держава-учасниця ухвалила такі законодавчі та/або регулятивні заходи, які вона вважає необхідними для визначення секторів, які вважаються чутливими для їх національної безпеки та добробуту економіки». , а також системи інформаційно-комунікаційних технологій, призначені для функціонування в цих секторах як елементи критичної інформаційної інфраструктури» (ст. 25 «Правові заходи», п. 4 «Захист критичної інфраструктури»).''

[26] Дейв Клементе, Кібербезпека та глобальна взаємозалежність: що критично? Chatham House, Лондон, 2013, с. ix. Доступний на https://www.brookings.edu/book/ cyber-security-and-global-interdependence-what-is-critical/.

2.4.1. Визначення «критичності»

Крок 2: Визначення певних секторів як критичних»

Першим основним кроком у процесі ідентифікації КІ є визначення того, що мається на увазі під КІ загалом. Це корисно для визначення арени, на якій будуть створюватися подальші політичні та нормативні рамки[27]. Як правило, національні визначення поєднують два елементи: вони підкреслюють остаточність або мету інфраструктури (пов'язуючи критичність із виконанням основних соціальних функцій) та підкреслити наслідки збою або руйнування (іншими словами, зв'язування критичності з очікуваними наслідками переривання обслуговування).[28]

КІ можна визначити, беручи до уваги роль, яку вона відіграє у сприянні та захисті прав людини (наприклад, інфраструктура, життєво важлива для функціонування систем надання медичної допомоги, систем екстреної допомоги, систем водопостачання та каналізації, та інші), а також вплив на права людини, який, ймовірно, спричинить порушення або руйнування інфраструктури (наприклад, нездатність надати адекватні або навіть життєво необхідні медичні послуги; екологічна шкода, яка може призвести до втрати життя; вимушене переміщення з негативним впливом на право на здоров'я та інші). Такий підхід відображено в різних існуючих визначеннях, у тому числі у визначенні Європейського Союзу, наведеному нижче. У тому ж ключі право збройних конфліктів надає особливий захист інфраструктурі, яка є необхідною для виживання цивільного населення або знищення якої може спричинити серйозні втрати чи завдати шкоди здоров'ю та виживанню населення (Перший додатковий протокол до 1949 р. Женевські конвенції, статті 54–56).

Вміст 7
Визначення критичної інфраструктури Європейського Союзу

Європейський Союз визначає «критичну інфраструктуру» як «актив, систему або її частину», яка є «необхідною для підтримки життєво важливих соціальних функцій, здоров'я, безпеки, безпеки, економічного чи соціального добробуту людей», а також порушення або знищення якого мало б значний вплив «внаслідок нездатності підтримувати ці функції».

Джерело: Council Directive 2008/114/EC, art. 2.

Таблиця 2
Національні визначення КІ

Аргентина	КІ - це те, що є необхідним для належного функціонування основних служб суспільства, охорони здоров'я, безпеки, оборони, соціального забезпечення, економіки та ефективного функціонування держави, знищення чи порушення якого, повністю чи частково, впливає на та/або суттєво впливає на них (резолюція 1523/2019, додаток 1).
Австрія	Інфраструктура або її частини, які мають вирішальне значення для забезпечення важливих соціальних функцій і збій або руйнування яких має серйозні наслідки для здоров'я, безпеки або економічного та соціального добробуту населення або функціонування державних установ (Стратегія кібербезпеки) 2013)

Бельгія	Об'єкт, система або їх частина, що становлять федеральний інтерес і мають важливе значення для підтримки життєво важливих функцій суспільства, здоров'я, безпеки та економічного чи соціального добробуту громадян, і переривання експлуатації чи знищення яких призведе до значної вплив через збій цих функцій (Закон 2011 року про безпеку та захист критичної інфраструктури)
Канада	КІ стосується процесів, систем, засобів, технологій, мереж, активів і послуг, необхідних для здоров'я, безпеки, економічного добробуту канадців і ефективного функціонування уряду (Громадська безпека Канади)

27 The Міжнародне право збройних конфліктів надає особливий захист інфраструктурі, яка є необхідною для або знищення якої може спричинити серйозні втрати чи завдати здоров'ю та виживанню населення (Перший додатковий протокол до женевських конвенцій 1949 р., статті 54-56)

28 Рекомендації також можна знайти в результаті роботи, проведеної деякими міжнародними організаціями та договорами. Наприклад, хоча в документах ICAO не визначено «критичну інфраструктуру» як таку, Керівництво ICAO з авіаційної безпеки посилається на поняття «вразлива точка» як «будь-який об'єкт в аеропорту або пов'язаний з ним, який у разі пошкодження або знищення може завдати серйозної шкоди погіршити роботу аеропорту. Диспетчерські вежі, засоби зв'язку, радіонавігаційні засоби, силові трансформатори, первинні та вторинні джерела живлення та паливні установки, як в аеропорту, так і за його межами, слід вважати вразливими точками. Комунікаційні та радіонавігаційні засоби, які можуть бути підроблені, повинні мати вищий рівень безпеки» (Керівництво з авіаційної безпеки (Doc 8973 – Restricted), пункт 11.2.4.9).

Китай	КІІ стосується важливої мережевої інфраструктури, інформаційних систем та інших об'єктів у важливих галузях і секторах, таких як публічні телекомунікації та інформаційні послуги, енергетика, транспорт, водопостачання, фінанси, державні послуги, електронний уряд, національна оборона, наука, технології та промисловість, а також у випадках, коли їх знищення, втрата функціональності або витік даних може завдати серйозної шкоди національній безпеці, національній економіці та засобам існування людей або суспільним інтересам (Положення про безпеку критичної інформаційної інфраструктури , 2021)
Франція	Життєво важливою інфраструктурою є будь-яка установа, об'єкт або структура, для якої пошкодження, недоступність або руйнування в результаті зловмисних дій, диверсій або терористичних дій можуть прямо чи опосередковано: якщо їх діяльність важко замінити або замінити, серйозно обтяжити військовий потенціал або економічний потенціал, національна безпека чи виживання нації, або серйозно вплинути на здоров'я чи життя населення (Загальна міжміністерська інструкція щодо безпеки життєдіяльності, Генеральний секретаріат з питань оборони та національної безпеки, 2014 р.)
Німеччина	КІ відноситься до організаційних і фізичних структур і об'єктів, які мають таке життєво важливе значення для суспільства та економіки країни, що їх вихід з ладу або деградація призведе до тривалого дефіциту поставок, значних порушень громадської безпеки та інших серйозних наслідків (Федеральне відомство безпеки інформації)
Італія	Матеріальні ресурси, послуги, IT-системи, мережі та інфраструктурні активи, які у разі пошкодження або знищення можуть мати серйозні наслідки для ключових функцій суспільства, включаючи ланцюг постачання, охорону здоров'я, безпеку та економічний або соціальний добробут держави. та населення (Міністерство внутрішніх справ)
Кенія	КІ описує активи, необхідні для функціонування суспільства та економіки (такі як електрична мережа, телекомунікації, водопостачання) (Національна стратегія кібербезпеки)
Нова Зеландія	Фізичні та цифрові активи, послуги та ланцюжки постачання, порушення (втрата, компрометація) яких серйозно вплине на підтримку національної безпеки, громадської безпеки, основних прав і добробуту всіх жителів Нової Зеландії (проект інфраструктурної стратегії, 2021 р.)
Пакістан	Критичні елементи інфраструктури, а саме активи, об'єкти, системи, мережі чи процеси, втрата чи порушення яких може призвести до: по-перше, значного згубного впливу на доступність, цілісність або надання основних послуг, у тому числі тих послуг, цілісність яких у разі порушення може призвести до значних втрат життя або жертв, враховуючи значні економічні чи соціальні наслідки; або, по-друге, значний вплив на національну безпеку, національну оборону або функціонування держави (Закон про запобігання електронним злочинам, 2016 р.)
Португалія	КІ визначається як компонент, система або їх частина, яка є важливою для підтримки життєво важливих функцій суспільства, здоров'я, безпеки та економічного чи соціального добробуту, і порушення її роботи або її знищення матиме значний вплив, оскільки було б неможливо продовжувати гарантувати ці функції (Закон № 20/2022)
Катар	Фізичні активи, системи чи установки, які, у разі порушення, скомпрометації чи знищення, могли б мати серйозний вплив на здоров'я, безпеку чи економічний добробут Катару чи ефективне функціонування уряду Катару (Стратегія кібербезпеки, 2014)
Саудівська Аравія	Інфраструктура, втрата чи сприйнятливість до порушень безпеки може призвести до значного негативного впливу на доступність, цілісність або надання основних послуг або може мати значний вплив на національну безпеку, національну оборону, економіку Саудівської Аравії чи національний потенціал Саудівської Аравії (законодавство про кібербезпеку) (Міністерство закордонних справ)
Південна Африка	Означає будь-яку будівлю, центр, установу, установку, установку, трубопровід, приміщення або системи, необхідні для функціонування суспільства, уряду або підприємств Республіки, і включає будь-яку транспортну мережу або мережу для доставки електроенергії або води (захист критичної інфраструктури). Акт, 2019)
Іспанія	Стратегічна інфраструктура, функціонування якої має важливе значення та не допускає альтернативних рішень, так що її порушення або знищення матиме серйозний вплив на основні послуги (Закон 8/2011)
Швейцарія	Процеси, системи та об'єкти, які мають вирішальне значення для функціонування економіки та добробуту населення (Національна стратегія захисту критичної інфраструктури на 2018–2022 роки)
Тринідад і Тобаго	КІ означає комп'ютерні системи, пристрої, мережі, комп'ютерні програми та комп'ютерні дані, настільки життєво важливі для країни, що непрацездатність, знищення або втручання в такі системи та активи матиме виснажливий вплив на безпеку, оборону чи міжнародні відносини держави; або надання послуг, безпосередньо пов'язаних з національною чи економічною безпекою, банківськими та фінансовими послугами, інфраструктурою зв'язку, національною охороною здоров'я та безпекою, громадським транспортом, інфраструктурою відкритих ключів або будь-якою комбінацією цих питань (Національна стратегія кібербезпеки, 2012 р.)
Україна	Функції та/або послуги, виконання яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої, перерви та збої в наданні яких призведуть до швидких негативних наслідків для нац. безпека (Закон про критичну інфраструктуру, 2021 р.)
Велика Британія	Ті критичні елементи інфраструктури (а саме активи, об'єкти, системи, мережі або процеси та основні працівники, які їх обслуговують і сприяють), втрата або компрометація яких може призвести до: (a) значного шкідливого впливу на доступність, цілісність або доставку найважливіших послуг - у тому числі тих послуг, цілісність яких у разі порушення може призвести до значних втрат чи жертв - з урахуванням значних економічних чи соціальних наслідків; та/або (b) значний вплив на національну безпеку, національну оборону або функціонування держави (Центр захисту національної інфраструктури)
США	Фізичні та кіберсистеми та активи, які є настільки життєво важливими для Сполучених Штатів, що їх непрацездатність або знищення матиме виснажливий вплив на нашу фізичну чи економічну безпеку чи здоров'я чи безпеку населення (CISA)

Крок 2: Визначення певних секторів як критичних

Другий крок у процесі ідентифікації КІ спрямований на визначення секторів і підсекторів, які вважаються «критичними». Ряд секторів, імовірно, будуть вважатися критичними всіма або більшістю держав-членів. Яскравим прикладом є енергетичний сектор, оскільки країни залежать від постачання електроенергії для виконання майже всіх соціальних і економічних функцій, від телекомунікацій і перекачування води до постачання життєво необхідної медичної допомоги. У той же час, певний сектор або підсектор може розглядатися як життєво важливий лише деякими державами-членами. Розмір, структура та особливості певної національної економіки можуть визначати, що є критичним, а що ні. Наприклад, деякі країни можуть сильно залежати від індустрії туризму для отримання прибутку та як передумови для підтримки соціальної єдності та внутрішньої стабільності. Для цих країн визначення туристичної індустрії як «критично важливої» може бути необхідним для забезпечення надання основних послуг суспільству.

Важливо те, що той факт, що певний сектор визначено як критичний, не означає автоматично, що всі базові послуги мають бути критичними. Наприклад, в енергетичному секторі послуга централізованого опалення, швидше за все, не буде включена як критична на національному рівні, але постачання електроенергії буде.

Крок 3: Віднесення конкретних активів, систем і процесів до кожного критичного сектора

Третій крок у процесі ідентифікації КІ пов'язує сектори та підсектори, які були визначені як «критичні», зі списком окремих активів, систем і процесів. Цифри можуть сильно варіюватися від кількох до кількох тисяч залежно від розміру країни, рівня економічного розвитку та інших факторів. Деякі держави-члени розробили набори показників, спрямованих на вимірювання наслідків збою інфраструктури або функціонального збою. Зазвичай вони поєднують наступне:

- *Географічне охоплення ефекту*
- *Тривалість ефекту*
- *Серйозність потенційних або передбачуваних впливів з точки зору:*
- *Економічні наслідки (вплив на ВВП, кількість постраждалих працівників, втрата податкових надходжень)*
    - *Кількість постраждалих та обсяг евакуйованого населення*
    - *Втрата повноважень Урядом або зрив державного управління*

- Шкода навколишньому середовищу

Різноманітні підходи можуть бути використані з метою віднесення конкретних активів, систем і процесів до кожного критичного сектора. Консорціум під керівництвом нідерландської дослідницької організації TNO намагався схематично згрупувати їх у три основні типи:[29]

- По-перше, підхід, що базується на послугах (наприклад, у Швейцарії), коли уряд визначає критичні активи на основі специфічних для сектора критеріїв, що визначають порогові значення рівня обслуговування та кількісно визначену продуктивність активів (наприклад, кількість поставлених мегават)
- По-друге, підхід на основі операторів (наприклад, у Франції), де завдання визначення того, які активи чи послуги є критичними, покладається на окремих операторів KI
- По-третє, підхід на основі активів або гібридний підхід (наприклад, у Сполученому Королівстві), який використовує елементи як орієнтованого на послуги, так і орієнтованого на оператора підходу.

---

29 Європейська комісія, Посібник із належної практики щодо політики CIP для політиків у Європі, Рекомендовані елементи захисту критичної інфраструктури для політиків у Європі (RECIPE), 2011 р. Доступно за адресою https://repository.tno.nl/islandora/object/uuid:29f15365-8885-4278-82fe-996567858ae9.

Вивчення Проблеми 4
Індикатор кваліфікації інфраструктури як критичної: Аргентина та Південна Африка

Аргентина

Резолюція 1523/2019 *встановила та визначила критерії визначення інфраструктури як критичної з особливим посиланням на ICI. Ці критерії ґрунтуються на потенційному впливі внаслідок руйнівної поведінки, як зазначено нижче:*

- *Вплив на життя людини: порушення роботи комп'ютерної системи створює ризик втрати життя або серйозну загрозу здоров'ю та фізичній цілісності людей.*
- *Економічний вплив: Порушення роботи комп'ютерної системи завдає шкоди або створює загрозу серйозної шкоди виробничій та/або фінансовій структурі країни.*
- *Вплив на навколишнє середовище: Порушення роботи комп'ютерної системи негативно впливає або завдає серйозної шкоди простору, в якому розвиваються живі істоти.*
- *Вплив на реалізацію прав людини та індивідуальних свобод: будь-яка дія, здійснена через комп'ютерну систему, необґрунтовано обмежує або скорочує повну та колективну реалізацію прав, закріплених у міжнародних договорах, національній Конституції чи законах.*
- *Суспільний або соціальний вплив: Порушення роботи комп'ютерної системи може спричинити серйозний шок у значної частини населення.*
- *Вплив на виконання державних функцій: Порушення роботи комп'ютерної системи суттєво впливає на нормальне функціонування органів виконавчої, законодавчої чи судової влади.*
- *Вплив на національний суверенітет: порушення роботи комп'ютерної системи ставить під загрозу або обмежує владу держави на національній території.*
- *Вплив на підтримку національної територіальної цілісності: Порушення роботи комп'ютерної системи призводить до порушення наземних, повітряних або морських кордонів держави.*

Південна Африка

Відповідно до Закону про захист критичної інфраструктури від 2019 *року, для визначення відповідності кваліфікаційним вимогам до* CI *необхідно застосовувати один або кілька з наведених нижче критеріїв:*

- Інфраструктура повинна мати значне економічне, громадське, соціальне чи стратегічне значення.
- Здатність країни функціонувати, надавати основні державні послуги або підтримувати правопорядок може постраждати, якщо послуга, що надається інфраструктурою, переривається, або якщо інфраструктура знищена, порушена, погіршена або виведена з ладу.
- Переривання послуги, що надається інфраструктурою, або знищення, порушення, погіршення чи збій такої інфраструктури матиме значний вплив на навколишнє середовище, здоров'я чи безпеку населення чи будь-якої частини населення, або інша інфраструктура, яка може негативно вплинути на функції та функціонування даної інфраструктури.
- Є обґрунтовані підстави вважати, що оголошення критичною інфраструктурою не матиме істотного негативного впливу на інтереси громадськості.
- Оголошення критичної інфраструктури є виконанням зобов'язань згідно з будь-яким обов'язковим міжнародним правом або міжнародним документом.

Будь-які інші критерії, які можуть час від часу визначатися міністром шляхом повідомлення в газеті після консультації з Радою критичної інфраструктури.

Джерело: www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf and www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918.

Вивчення проблеми 5

Методології ідентифікації KI: Австралія, Франція, Німеччина, Нідерланди, Південна Африка, Великобританія та Європейський Союз

Австралія

Критерії та процедури визначення активів як критично важливих викладено в Законі про безпеку критичної інфраструктури 2018 року. Закон визначає, що мається на увазі під «активом критичної інфраструктури» в різних секторах, посилаючись на такі критерії, як виробнича потужність певних активів. Для тих активів, які не відповідають встановленим критеріям, міністр може приватно оголосити актив об'єктом критичної інфраструктури, якщо він або вона переконається, що:

- Актив є критично важливою інфраструктурою, яка впливає на національну безпеку.
- Існував би ризик для національної безпеки, якби було публічно відомо, що актив є критичною інфраструктурою, яка впливає на національну безпеку.
- Секретар веде Реєстр активів критичної інфраструктури, що містить інформацію щодо цих активів. Реєстр не підлягає оприлюдненню.

Франція

У Франції уряд не ідентифікує окремі активи KI безпосередньо. Натомість він призначає так званих «важливих операторів» («OIV»), відповідальних за ідентифікацію окремих активів. Згідно з Кодексом оборони, життєво важливий оператор визначається відповідальним міністром («міністерством-координатором») певного сектора діяльності за погодженням з іншими відповідними міністерствами. Міністр-координатор повідомляє оператора про свій намір призначити його життєво важливим оператором. Процес сповіщення також являє собою можливість для початкових консультацій між урядом та оператором.

Щоб бути призначеним оператором життєво важливих умов, оператори повинні відповідати двом умовам:

- Їхня діяльність повністю або частково здійснюється в життєво важливому секторі.
- Вони керують або використовують принаймні одну установу, структуру чи об'єкт, пошкодження, недоступність або знищення яких внаслідок зловмисних дій, диверсій чи тероризму може мати значні наслідки для виживання нації або здоров'я чи життя населення.

Статус життєво важливих операторів можуть отримати:

- Корпорації
- Асоціації, фонди або міжнародні організації
- Державні служби, органи місцевого самоврядування, групи органів місцевого самоврядування, громадські установи, незалежні органи управління

У випадку корпорації життєво важливим оператором може бути материнська компанія або дочірня компанія. Вибір здійснюється після консультації з відповідним оператором. Кілька дочірніх компаній однієї групи потенційно можуть бути визначені. Якщо оператора призначають декілька міністрів одночасно, розпочинається процес консультацій, щоб визначити, який міністр виконуватиме роль координатора. Наскільки це можливо, міністерство-координатор має бути відповідальним за життєво важливий сектор, у якому життєво важливий оператор здійснює свою основну діяльність.

У рамках своєї звичайної діяльності життєво важливий оператор може мати субпідряд або аутсорсинг виконання однієї чи кількох функцій, які сприяють виконанню життєво важливої діяльності. У цьому випадку життєво важливий оператор повинен вжити необхідних заходів щодо свого субпідрядника або постачальника, щоб останній сприяв досягненню цілей безпеки та безпеки CIP.

Після призначення життєво важливі оператори розробляють свої «плани безпеки оператора». Аналіз ризиків, проведений під час розробки цих планів, дозволяє їм запропонувати, як додаток до свого плану, перелік установок, закладів або систем, які вони вважають доцільними для позначення «життєво важливих точок» (іменованих «PIV»).

Німеччина

Німецький Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz («Положення про ідентифікацію критичної інфраструктури», відоме як «BSI-KritisV») визначає, які об'єкти кваліфікуються як критична інфраструктура в Німеччині. Класифікація як «критична інфраструктура» залежить від двох умов:

- Інфраструктура, про яку йде мова, має належати до певної категорії секторів енергетики, водопостачання, продовольства, IT та телекомунікацій, охорони здоров'я, фінансів і страхування транспорту;

- Об’єкти, про які йдеться, мають відповідати певним пороговим вимогам щодо розміру та важливості.
- Оператори КІ стикаються з низкою зобов’язань, які включають, серед іншого, вимогу повідомляти про будь-які збої або значні порушення, а також впровадження найсучасніших засобів безпеки.

- Інвестиції інвесторів, які не входять до Європейського Союзу або Європейської асоціації вільної торгівлі (ЄАВТ), у компанії, що керують КІ, підлягають перевірці німецьких прямих іноземних інвестицій (ПІІ). Інвестиції в розмірі 10 відсотків або більше в бізнес, який вважається КІ, підлягають обов'язковій реєстрації ПІІ, а також зобов'язанню призупинення.

1 січня 2022 року набула чинності друга зміна до Положення. Поправка мала такі наслідки:

- Розширено визначення КІ, зокрема в секторах ІТ-послуг та енергетики, знизивши порогові значення для активів, які вважаються КІ.
- Розширено сферу застосування КІ в секторі охорони здоров'я шляхом введення нової категорії «лабораторні інформаційні мережі», іншими словами, мережі лабораторій, у яких одна лабораторія надає ІТ-послуги для інших лабораторій з тієї ж мережі.
- Додано декілька категорій КІ у транспортному секторі, включаючи компанії, що експлуатують аеропорти та порти, а також так звані інтелектуальні транспортні системи.
- Роз'яснено концепцію «спільної інфраструктури» як кількох об'єктів інфраструктури, необхідних для надання однієї критичної послуги. Це можна припустити, наприклад, якщо порушення доступності або цілісності одного об'єкта може призвести до порушення роботи іншого об'єкта. Якщо кваліфікувати як спільну інфраструктуру, обсяг усіх спільних об'єктів агрегується, що підвищує ймовірність досягнення порогових значень.

У результаті нещодавно розширеного обсягу нормативної бази КІ очікується, що кількість закладів КІ в Німеччині збільшиться приблизно на 15 %.

Південня Африка

Процес ідентифікації КІ починається з того, що особа, яка контролює інфраструктуру, подає заяву до національного комісара поліції Південної Африки, щоб така інфраструктура була оголошена критичною. Заявка повинна містити певну інформацію, зокрема сектор, у якому виконуються основні функції відповідної інфраструктури, ресурси, доступні особі, яка контролює інфраструктуру, щоб захистити її від збоїв і забезпечити її відновлення у разі інцидентів, рівень ризику, якому піддається відповідна інфраструктура, і ступінь, до якого оголошення критичної інфраструктури сприятиме інтересам громадськості.

Як правило, Національний уповноважений повинен опублікувати повідомлення про заявку в газеті, провести оцінку безпеки відповідної інфраструктури та подати свою оцінку Раді з КІ, яка є міжвідомчою державною організацією, відповідальною за координацію Дії, пов'язані з CIP, на національному рівні.

За рекомендацією Ради міністр ухвалює офіційне рішення щодо того, чи можна визнати відповідну інфраструктуру критичною. Якщо інфраструктура оголошується критичною, міністр видає «сертифікат декларації», у якому вказується: по-перше, категорія ризику, визначена міністром; по-друге, приміщення або комплекс, де розташована критична інфраструктура; по-третє, умови, які міністр може вважати необхідними встановити з метою забезпечення безпеки критичної інфраструктури; і, по-четверте, чи буде інформація щодо заходів безпеки обмежена.

Нідерланди

У 2014 політика КІ Нідерландів зазнала значних реформ. Це призвело до переходу від поняття «критичні сектори» до поняття «критичні процеси». Критичні процеси - це ті, які можуть призвести до серйозних соціальних руйнувань у разі їх невдачі або зриву. Оскільки не всі процеси в секторі є критичними, зараз увага зосереджена на критичних процесах, а не на критичних секторах. Виявлення критичних процесів дозволяє використовувати інструменти та дефіцитні ресурси більш ефективно та цілеспрямовано. Оцінка рівня критичності здійснюється на основі встановлених критеріїв впливу, таких як економічний збиток і фізичні наслідки. Оцінка розрізняє 2 критичні категорії, A і B. Відмова критичних процесів A має більший потенційний вплив, ніж відмова критичних процесів B. Розрізнення між критичними A та B-критичними може бути корисним для визначення пріоритетів втручання під час інцидентів і прийняття індивідуальних рішень для заходів підвищення стійкості.

Категорія A: включає інфраструктуру, для якої порушення, пошкодження або збій відповідають принаймні 1 з 3 критеріїв впливу та критерію каскадних ефектів.

- Економічний вплив: понад приблизно 50 мільярдів євро збитків або приблизно 5% падіння реального доходу.
- Фізичні наслідки: більше 10 000 загиблих, важко поранених або хронічно хворих.
- Соціальний вплив: більше млн страждають від емоційних проблем або серйозних проблем із елементарним виживанням.
- Каскадні ефекти: збій призводить до поломки принаймні двох інших секторів.

Категорія B: *включає інфраструктуру, для якої порушення, пошкодження або збій відповідають принаймні* 1 *з* 3 *критеріїв впливу*:

- Економічний вплив: понад приблизно 5 мільярдів євро збитків або падіння реального доходу приблизно на 1%.
- Фізичний вплив: більше 1000 загиблих, важко поранених або хронічно хворих.
- Соціальний вплив: понад 100 тис людей страждають від емоційних проблем або серйозних проблем із елементарним виживанням.

ВИВЧЕННЯ ПРОБЛЕМИ 5
Методології ідентифікації КІ: Австралія, Франція, Німеччина, Нідерланди, Південна Африка, Великобританія та Європейський Союз (продовження)

Кожне міністерство несе відповідальність за проведення оцінки критичних процесів, які підпадають під його відповідальність. Міністерство-координатор, Міністерство юстиції та безпеки регулярно перевірятиме методологію, щоб переконатися, що вона актуальна, і визначатиме, чи є ознаки можливих нових критичних процесів.

Великобританія

Сполучене Королівство визначило 13 національних інфраструктурних секторів. Для кожного сектору 1 або кілька провідних державних відомств гарантують, що для відповідних критично важливих активів існує захист. Так званий «процес критичності» дає провідному державному департаменту кожного сектору спільний підхід до збору та структурування даних про КІ, за яку він відповідає. Процес підтримує систематичну ідентифікацію основних функцій, критичних систем, які їх забезпечують (та їх взаємозалежності), а також організацій, які керують цими системами. Ця інформація пов'язана з наслідками, які матиме збій системи (усередині і між секторами). Процес критичності, зокрема, передбачає наступні етапи:

- Крок 1: зіставлення основні функції
- Крок 2: визначення системи
- Крок 3: оцінка впливу на сектор
- Крок 4: визначення допоміжні системи, відносини та організації
- Крок 5: оцінка міжгалузевого впливу

Sources: www.legislation.gov.au/Details/C2018A00029/Html/Text; www.legifrance.gouv.fr/download/pdf/circ?id=37828; www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf; https://english.nctv.nl/topics/critical-infrastructure-protection; and www.cpni.gov.uk/critical-national-infrastructure-0.

ВИВЧЕННЯ ПРОБЛЕМИ 6
Виявлення КІ в рамках Президентської програми протидії міському тероризму: Колоумбія

Створені в 2017 році Інструкцією 0002 від 24 березня Управління розвідки поліції, інтегровані інформаційні та розвідувальні центри (відомі як «CI3») представляють собою міжвідомчий механізм для обміну інформацією та формулювання стратегічних напрямків дій. перед обличчям явищ і загроз, які впливають на безпеку та співіснування громадян.

У рамках цієї організаційної моделі підрозділ, відомий як CI3-T, зосереджується на боротьбі з тероризмом. У рамках Ci3-T під керівництвом Управління розвідки поліції та за підтримки Президентської ради з національної безпеки та Міністерства національної оборони було розроблено Президентську програму протидії міському тероризму. Програма включає 16 напрямків діяльності, один із яких стосується картографування критичної інфраструктури та заходів захисту та призначений для запобігання та уникнення вчинення терористичних атак на стратегічні об'єкти в Боготі.

Місто Богота наразі має 120 критичних точок, які були обрані на зустрічах CI3-T. Відбір відбувався через оцінку відповідності критеріям, встановленим для пріоритетності стратегічної інфраструктури, яка може бути об'єктом потенційних терористичних дій. Ці критерії наступні:

- Наявність історичних терористичних планів
- Наявність останніх терористичних планів
- Наявність неминучих терористичних планів
- Історія зафіксованих вчинення терористичних дій
- Оцінка рівня критичності - оцінка впливу
- Вразлива зона: охоронний периметр, середовище з масовим перебуванням людей і місця з високим притоком громадськості

Виходячи з вищевикладеного, інфраструктурний ризик класифікується як високий, середній або низький, що, у свою чергу, визначає пріоритети для боротьби з терористичними актами.

Джерело: Постійне представництво Колумбії при ООН.

Інструмент 4

На шляху до визначення критичної національної інфраструктури в процесі національної стратегії кібербезпеки – документ GFCE

https://cybilportal.org/wp-content/uploads/2022/03/White-Paper-Towards-Identifying-CNI-in-the-NCS-Process.pdf

Цей білий документ пропонує певні практичні міркування та заходи, за допомогою яких країни можуть розробити підходи до ідентифікації KI та KII у рамках процесів розробки та реалізації національної стратегії кібербезпеки.

Білий документ стосується 3 основоположних елементів. Четвертий розділ визначає області, де необхідні додаткові дослідження.

- У розділі I розглядаються потенційні підходи до визначення аспектів ризику ІКТ у KI та KII.
- У розділі II обговорюються потенційні підходи до формалізації ідентифікації KI та KII у національній стратегії

2.4.2. Критична інформаційна інфраструктура

У сучасній економіці промислові виробничі ланцюги та постачання товарів і послуг як державними, так і приватними організаціями – значною мірою – керуються комп'ютерно керованими системами, відомими як промислові системи управління (іноді їх називають «ICS»). За останні кілька десятиліть промислові системи управління поступово отримали підключення до Інтернету та мереж приватних підприємств. Ця зміна оптимізувало виробництво та надання послуг. Крім того, як зазначив один дослідник, «об'єднання промислових систем управління в мережу в більшому масштабі призвело до підвищення синергії та ефективності, і через потреби ринку інформація в реальному часі для цих систем стає все більш важливою для маркетингових цілей». [30]

Той факт, що промислові системи управління все більше пов'язані з комп'ютерними системами компаній через Інтернет, робить їх значно більш вразливими до кібератак. Специфічні виклики безпеці створюють застарілі системи, а саме ті промислові системи керування, які були встановлені в епоху до Інтернету і спочатку не були задумані для цілей підключення.

Системи промислового керування використовуються практично в усіх секторах KI, оскільки вони часто керують безперервною роботою на електростанціях, дамбах, мостах, телекомунікаційних вежах та інших подібних об'єктах і тому є ключовими компонентами KII. Існує ряд національних визначень ICI. OECP, наприклад, визначає ICI як «ті взаємопов'язані інформаційні системи та мережі, збій або знищення яких матиме серйозний вплив на здоров'я, безпеку, безпеку чи економічне благополуччя громадян або на ефективне функціонування уряду або економіки».[31]

Важливо, щоб стратегії CIP визнавали та забезпечували захист ICI на рівній основі з захистом критично важливих активів у фізичному світі, тим більше, що, як зазначив Клементе, «ми можемо наближатися до точки, де відмінності між «інфраструктурою» та «інформаційна інфраструктура» не мають значення, оскільки вони зливаються в одне коло критичних «матеріалів», що постійно розширюється»[32]. Із зростанням залежності від кіберінфраструктури зростає також поширення так званих «критичних вузли» - а саме точки в системі, де збій значно погіршить роботу мережі.

---

[30] Дана Ши, «Критична інфраструктура: системи контролю та терористична загроза», Дослідницька служба Конгресу, 14 липня 2003 р., с. CRS-3. Доступний на https://digital. library.unt.edu/ark:/67531/metacrs5038/m1/1/high_res_d/RL31534_2003Jul14.pdf.

[31] Рекомендація Ради OECP щодо захисту критично важливих інформаційних інфраструктур [C(2008)35], OECP, 2008. Доступно за адресою www.oecd.org/sti/40825404.pdf.

[32] Дейв Клементе, Кібербезпека та глобальна взаємозалежність, с. 17.

2.4.3 Взаємозв'язки та взаємозалежності

Доставка основних товарів і послуг суспільству все більше досягається завдяки взаємодії багатьох постачальників. Вони перетинають усі сектори та підсектори KI, утворюючи складні взаємозв'язки. Хоча взаємозв'язок активів, систем і процесів ґрунтується на більш ефективному управлінні ресурсами, він збільшує залежність. Вони можуть бути широко визначені як «відносини між двома продуктами або послугами, в яких один продукт або послуга необхідний для створення іншого продукту або послуги»[33]. Наприклад, постачання продовольства залежить від транспорту, банківський і фінансовий сектори залежать від телекомунікації для автентифікації транзакцій, а сектор телекомунікацій залежить від безперебійного розподілу електроенергії. Більшість основних послуг залежить від одночасного надання послуг з кількох секторів. Наприклад, медична допомога не може надаватися за відсутності електроенергії, води та екстрених служб одночасно.

- Залежності можуть давати наслідки різної інтенсивності та бути різного типу:
- Фізичні залежності: функціонування однієї частини інфраструктури залежить від постачання матеріальних продуктів з іншої частини інфраструктури.
- Кіберзалежності: функціонування однієї частини інфраструктури залежить від інформації, що передається через інформаційну інфраструктуру.

Важливо розуміти, що залежності підвищують рівень уразливості активів. Вони, у свою чергу, посилюються через широку залежність урядових установ і приватного сектору від ІКТ, що посилює ефект міжгалузевої та транснаціональної залежності. У зв'язку з цим було зазначено, що «сценарій, який викликає найбільше занепокоєння серед експертів, — це комбіноване використання кібератаки на критичну інфраструктуру в поєднанні з фізичною атакою. Таке використання кібертероризму може призвести до посилення ефекту фізичної атаки. Прикладом цього може бути звичайний бомбовий напад на будівлю в поєднанні з тимчасовою відмовою електричного або телефонного зв'язку. Погіршення реагування на надзвичайні ситуації, що випливає з цього, до тих пір, поки не будуть встановлені та використані резервні електричні чи комунікаційні системи, може збільшити кількість жертв і паніку серед населення».[34]

Коли вразливі місця перетворюються на збої в результаті терористичної атаки, залежності можуть спричинити каскадні ефекти. Наприклад, розповсюдження токсичних речовин у водопроводі призводить до збоїв у системі охорони здоров'я.

Для стратегій CIP надзвичайно важливо використовувати причинно-наслідковий зв'язок, який

існує між взаємозв'язками, залежностями та вразливими місцями KI як спосіб:

- Досягніть належного рівня розуміння (з боку всіх залучених зацікавлених сторін, будь то з приватного чи державного сектору) системних уразливих точок, які мають бути відображені в більш точному управлінні ризиками та кризами. Завдання інтеграції концепції залежностей у процеси управління ризиками та кризами ускладнюється тим фактом, що залежності можуть змінюватися залежно від режиму роботи певної частини KI. Наприклад, хоча зазвичай лікарня не покладається на дизельне паливо, після збою в системі електроенергії вона може раптово стати залежною від дизельного палива для роботи генератора аварійної енергії. Стратегії CIP повинні оформляти залежності не статично, а скоріше в термінах динамічних і швидко мінливих відносин.
- Підвищення обізнаності про взаємну залежність за допомогою міжсекторальних мереж (на основі, наприклад, обговорення сценаріїв ризику), щоб стимулювати подальшу співпрацю між різними гравцями.

Взаємозв'язки та залежності часто перетинають кордони, що тягне за собою потребу в стратегіях CIP також враховувати їх міжнародний вимір. Цей аспект детальніше розглядається в розділі 6

---

[33] Проект CIPRNet, https://ciprnet.eu/home.html.

[34] Дана Шей, «Критична інфраструктура: системи контролю та терористична загроза», с. CRS-8.

ВИВЧЕННЯ ПРОБЛЕМИ 7
Взаємозалежності та «життєві зони»: Франція

Французька стратегія CIP операціоналізує поняття залежностей шляхом введення концепції «життєвої зони» («zone d'importance vitale» або ZIV). Життєво важлива зона – це область, у якій імплантовано кілька «життєво важливих точок» («PIV»), що належать різним «важливо важливим операторам» («D»), і для якої спільна оцінка безпеки та управління є додатковим значенням. З точки зору безпеки існує взаємозалежність між PIV, коли:

- Здійснення погрози одному з них матиме наслідки для цілісності чи діяльності інших, або
- Заходи безпеки, застосовані для однієї життєво важливої точки або в спільній зоні, впливають на безпеку однієї чи кількох інших життєво важливих точок

Існує три типи географічних зон:

- Випадок 1: область, що складається з сусідніх життєво важливих точок, які суміжні або розташовані на відносно невеликій відстані одна від одної.
- Випадок 2: Область, що складається з замкнутих життєвих точок, так що життєва точка «2» знаходиться всередині життєвої точки «1».
- Випадок 3: зона, що поєднує характеристики перших двох випадків..

Створення життєво важливої зони має відповідати оперативній потребі та сприяти покращенню захисту життєво важливих точок шляхом об'єднання та раціоналізації ресурсів. Відповідну територію слід розуміти

ВИВЧЕННЯ ПРОБЛЕМИ 8
Міжсекторальні семінари та семінари з обміну знаннями про залежності: Нідерланди

У рамках своєї стратегії CIP Нідерланди провели низку міжгалузевих семінарів, які дозволили секторам KI отримати уявлення про наслідки взаємних залежностей. Зацікавлені сторони-учасники визначили технічні та організаційні мережі, в яких працюють критичні сектори. Це дозволило державним і приватним сторонам передбачати й обговорювати сценарії загроз. Жодних конкретних моделей для аналізу залежностей не використовувалося, основна ідея полягала в тому, що обмін знаннями через мережу та обмін досвідом дозволить секторам краще зрозуміти залежності та способи усунення вразливостей. Крім того, залучені сторони ближче познайомляться 1 з 1 та своїми відповідними можливостями, таким чином збільшуючи потенціал для ефективної співпраці у випадку аварій. Сценарії використовувалися, зокрема, для обговорення:

- Вплив збоїв KI, наприклад прямих чи непрямих, на ланцюг поставок, що впливає на доступ, дефіцит або цілісність, період збою, характеристики сектора та людський фактор

2.5 Проектування архітектури CIP

За відсутності міжнародно-правового інструменту, який визначає, яку інституційну модель країни-члени повинні прийняти для захисту KI, розташованих на їхній території, очікується, що уряди виберуть систему, яка найкраще відповідає розміру та структурі їхніх економік, культурі їхньої державної політики та встановленим інституційним практики. Архітектура управління CIP повинна, зокрема, враховувати основну конституційну структуру країни, іншими словами, чи є вони унітарними та централізованими чи федеральними та децентралізованими державами. Це особливо важливо при розподілі ролей і обов'язків між різними рівнями уряду..

2.5.1 Основні моделі управління

Архітектури CIP коливаються між двома основними моделями. На одному кінці спектру управління KI базується на принципах саморегулювання, стимулів і добровільного дотримання. Так званий «добровільний підхід» підкреслює політику, зосереджену на необов'язкових вказівках. За цією моделлю всі зацікавлені сторони (з державного чи приватного сектору) заохочуються робити внесок у визначення та реалізацію політики CIP шляхом рекомендацій, переконань та створення спільного сприйняття досягнення спільної мети. Обов'язкова сила законодавства та регуляторних схем використовується легковажно і лише як додатковий інструмент, за винятком певних секторів, таких як ядерний сектор, де вона може відігравати домінуючу роль.

На іншому кінці спектру знаходиться так званий «обов'язковий підхід», який базується на передумові, що співпраця у сфері CIP найкраще досягається шляхом встановлення обов'язкових правових рамок, що супроводжуються санкціями для операторів CI, які не дотримуються необхідних стандартів безпеки.

На практиці країни застосовують елементи обох підходів. Їхні системи можна визначити лише як переважно «добровільні» або «обов'язкові». Прикладами перших є Канада, Швейцарія, Сполучене Королівство та Сполучені Штати. Прикладами останніх є Бельгія, Естонія, Франція та Іспанія.

Країнам може бути важко визначити, яка модель найкраще відповідає їхнім потребам. Зокрема, коли вони встановлюють політику CIP вперше, вони можуть прийняти структури та процеси, які зрештою виявляться неадекватними. З цієї причини країни часто встановлюють механізми, які гарантують, що стратегії періодично переглядаються. Сполучені Штати є прикладом країни, яка почала з чистої концепції добровільної участі операторів KI в цьому процесі. Незважаючи на те, що його система все ще базується на цьому принципі, з часом він усе більше бачив потребу у зміцненні своєї правової бази для захисту CIP. Урок тут полягає в тому, що країни повинні вчитися на досвіді.

Таблиця 3
Інституційні рамки CIP у вибраних державах-членах

Австралія	Основною основою зусиль CIP в Австралії є Закон про безпеку критичної інфраструктури 2018 року, який забезпечує основу для управління ризиками для національної безпеки, пов'язаними з КІ, зокрема шляхом: • Підвищення прозорості власності та операційного контролю СІ в Австралії, щоб краще зрозуміти ці ризики. • Сприяння співпраці та співпраці між усіма рівнями влади, регуляторними органами, власниками та операторами КІ з метою виявлення та управління цими ризиками. На підтримку вищезазначених цілей інституційна основа складається з таких елементів: • Ведення реєстру інформації щодо активів ІП (реєстр не є публічним). • Вимагання від певних суб'єктів, пов'язаних з активом КІ, надавати інформацію щодо активу та повідомляти, якщо певні події відбуваються щодо активу. • Дозвіл компетентному міністру вимагати від певних суб'єктів, пов'язаних з активом КІ, виконати або утриматися від виконання дії чи процесу, якщо міністр переконаний, що існує ризик дії чи бездіяльності, які завдадуть шкоди безпеці. • Дозволити міністру внутрішніх справ вимагати від певних організацій, пов'язаних з активом КІ, надання певної інформації чи документів. • Дозволити Секретарю провести оцінку активу КІ, щоб визначити, чи існує ризик для національної безпеки, пов'язаний з активом. У 2022 році до Закону про безпеку критичної інфраструктури було внесено зміни, додавши нові положення, які включають: • Зобов'язання для визначених активів КІ приймати та підтримувати програму управління ризиками КІ. • Додаткові зобов'язання щодо кібербезпеки, які можуть бути застосовані до систем національного значення. • Положення, згідно з якими вказівки, що сприяють державній допомозі промисловості у випадку серйозного інциденту кібербезпеки, переважають над вимогами програми управління ризиками. • Змінені положення, що дозволяють використання та розкриття захищеної інформації. • Положення, відповідно до яких повноваження міністра декларувати актив як актив КІ включають повноваження вимагати дотримання програми управління ризиками. • Повноваження міністра оголошувати актив КІ системою національного значення.

Канада	Архітектура CIP має сильний добровільний компонент. Відповідальність поділяють федеральні, провінційні та територіальні органи влади, місцеві органи влади, а також власники та оператори КІ. Усі ці організації представлені в національних галузевих мережах (для кожного з 10 визначених секторів КІ), цілями яких є: • Сприяти своєчасному обміну інформацією. • Визначте проблеми національного, регіонального чи галузевого характеру. • Використовуйте предметний досвід секторів КІ, щоб надати рекомендації щодо поточних і майбутніх викликів. • Розробити інструменти та найкращі практики для посилення стійкості КІ у всьому спектрі запобігання, пом'якшення, готовності, реагування та відновлення. Участь у цих мережах є добровільною. Їх члени також керують планами роботи в окремих галузях. Щоб підтримувати комплексний та спільний підхід до підвищення стійкості критичної інфраструктури, Національний міжгалузевий форум сприяє обміну інформацією між галузевими мережами та вирішує питання міжюрисдикційної та міжгалузевої взаємозалежності.
Франція	Координацію CIP забезпечує Генеральний секретаріат з питань оборони та національної безпеки за дорученням Прем'єр-міністра. Генеральний секретаріат затверджує директиви національної безпеки, розроблені міністерствами-координаторами в кожному критичному секторі. Ці міністерства також є контактними особами операторів. Префекти зон і департаментів (іншими словами, представники держави в департаменті чи регіоні) діють під загальним керівництвом Міністерства внутрішніх справ як територіальні координатори стратегії CIP. Після призначення оператори повинні виконати кілька кроків, зокрема: • Призначення представника з питань оборони та безпеки (привілейований співрозмовник з адміністративним органом) • Складання плану безпеки оператора, який визначає політику безпеки оператора • Складання конкретного плану захисту для кожної з визначених життєво важливих точок
Німеччина	Архітектура CIP країни базується на визначенні шести робочих пакетів, що відповідають різним фазам циклу управління ризиками. Державний сектор (під координацією Федерального міністерства внутрішніх справ і громади) бере на себе ініціативу щодо реалізації перших чотирьох пакетів у співпраці з приватним сектором і операторами КІ. У реалізації пакетів 5 і 6 ролі змінюються, а компанії та оператори виконують роль провідних суб'єктів. Пакети робіт наступні: • Визначення загальних цілей захисту. • Аналіз загроз, вразливостей і можливостей управління. • Оцінка відповідних загроз. • визначення цілей захисту з урахуванням існуючих захисних заходів; аналіз існуючих нормативних актів і, за необхідності, визначення додаткових заходів, що сприяють досягненню мети; якщо і де потрібно, законодавство. • Реалізація заходів для досягнення цілей, насамперед, за допомогою, по-перше, специфічних рішень асоціації та внутрішніх положень; по-друге, угоди про самозобов'язання між бізнесом і промисловістю; і по-третє, розробка компаніями концепцій захисту. • Безперервний, інтенсивний процес комунікації ризиків (діалог про результати аналізу, оцінки, цілі захисту та варіанти дій). Система передбачає низку інституціоналізованих платформ із залученням органів державної влади, компаній та асоціацій. Хоча ця загальна архітектура спочатку не розрізняла інституційні підходи до фізичної безпеки та кібербезпеки, існуюча архітектура CIP була доповнена Стратегією кібербезпеки Німеччини 2001 року. Стратегія описує довгострокові цілі політики кібербезпеки уряду Німеччини (включаючи сприяння безперервності бізнесу операторів КІ) і цифровий суверенітет, а також забезпечує стратегічну основу для держави, приватного сектору та громадянського суспільства через керівні принципи, операційні та стратегічні цілі.
Іспанія	Державний секретар з питань безпеки, який діє через Національний центр захисту критичної інфраструктури, є вищим органом Міністерства внутрішніх справ, відповідальним за CIP. Для кожного стратегічного сектору принаймні один орган Генеральної державної адміністрації призначений відповідальним за сприяння, у межах своєї компетенції, урядовій політиці безпеки та за забезпечення її застосування. З точки зору залучення операторів КІ, Іспанія є типовим прикладом того, що можна назвати «мандатним підходом». Система базується на детальних нормативних положеннях, що вимагають ухвалення різних рівнів стратегічних планів і планів безпеки, розробка та затвердження яких покладається на різні суб'єкти в певні часові рамки. До них належать такі плани: • Національний план захисту КІ: він встановлює критерії та вказівки для мобілізації оперативних можливостей державних адміністрацій у координації з операторами КІ. • Галузеві стратегічні плани: вони дозволяють визначити обсяг основних послуг у кожному з визначених секторів, уразливості системи, потенційні наслідки бездіяльності та стратегічні заходи, необхідні для стійкості системи. • Плани безпеки оператора: вони визначають загальну політику операторів CI щодо забезпечення безпеки об'єктів або систем, якими вони володіють або керують. Вони повинні бути подані протягом шести місяців після повідомлення Міністерства внутрішніх справ про призначення оператора. • Спеціальні плани захисту: вони визначають конкретні заходи, які мають вжити оператори КІ для забезпечення безпеки КІ. Вони повинні бути подані протягом чотирьох місяців після затвердження плану безпеки оператора Міністерством внутрішніх справ. • Плани оперативної підтримки: вони визначають конкретні заходи, які повинні бути впроваджені державними адміністраціями для підтримки операторів КІ.
Нідерланди	Основну відповідальність за безперервність і стійкість критичних процесів несуть їх фактичні оператори. Очікується, що вони отримають уявлення про загрози, вразливі місця та ризики, а також розроблять і підтримують потенціал, який підвищує та забезпечує стійкість критичних процесів. Відповідальні міністерства встановлюють загальні рамки для секторів, які підпадають під їхню відповідальність (через політичні або регуляторні інструменти). Міністерства разом з операторами критичних процесів несуть відповідальність за збереження та інспектування можливостей, пов'язаних з КІ. Національний координатор з питань безпеки та боротьби з тероризмом Міністерства юстиції та безпеки є органом, відповідальним за загальну координацію та управління.

Саудівська Аравія	Вища комісія з промислової безпеки забезпечує захист критично важливої інфраструктури (нафти, промисловості та послуг) від терористичних атак, насамперед тих, що здійснюються з використанням безпілотників і малих човнів. У співпраці з різними військовими та силовими установами Верховна комісія відповідає за розробку політики боротьби з тероризмом щодо CIP. Він також містить конкретні інструкції, зокрема такі: • Нормативні директиви промислової безпеки: опубліковані в рішенні міністра 11131 11131 від 22 Зу аль-Када 1430 (10 листопада 2009 р.), вони включають • багато адміністративних вимог щодо створення відділів промислової безпеки на об'єктах CI для посилення спроможності протистояти терористичним атакам. Такі вимоги включають: ієрархію та організаційну структуру безпеки; вимоги до зайнятості з промислової безпеки; нормативні правила промислової безпеки. • Директиви безпеки: видані міністерськими рішеннями 5100 і 5101, 02/07/1438 (за арабським календарем), вони включають розділи, що стосуються будівництва • системи безпеки для підвищення безпеки та інтеграції з різними регулюючими та охоронними органами: системи безпеки на промислових об'єктах; охоронні огороджувальні системи; трубопроводи та трубопровідні коридори; засоби з морським інтерфейсом; управління безпекою на промислових об'єктах; безпеки комунікацій і мереж передачі даних. • Директиви щодо безпеки та протипожежного захисту: видані міністерськими рішеннями 5098 і 5099, 02/07/1438 (за арабським календарем), вони стосуються: загальних вимог- інструкції щодо безпеки протипожежного захисту; розташування рослин, відстань і доступ; безпека берегової та прибережної свердловини; напірні трубопроводи транспортні трубопроводи та посудини під тиском; виробництво транспорту зберігання та використання вибухових матеріалів; шахти та збагачувальні комбінати; доаварійне планування та управління надзвичайними ситуаціями; Повідомлення та розслідування інцидентів. Вищезазначені директиви утворюють однорідну та інтегровану систему управління безпекою під наглядом Верховної комісії.
Велика Британія	Секретаріат із надзвичайних ситуацій, що входить до складу Секретаріату національної безпеки, підтримує Прем'єр-міністра та Кабінет міністрів і очолює ширші зусилля уряду щодо планування та реагування на надзвичайні ситуації цивільного характеру. Конкретні політичні обов'язки Секретаріату полягають у наступному: • Національна оцінка ризиків та Національний реєстр ризиків (виявлення та оцінка ризиків для національної безпеки та безпеки, що виникають внаслідок тероризму, основні • промислові аварії та стихійні лиха, понад п'ять років) • Оцінка ризиків для національної безпеки (визначення глобальних ризиків для інтересів безпеки Сполученого Королівства за період від 5 до 20 років) • Керівництво міжурядовою програмою підвищення стійкості для покращення реагування державного сектора на такі надзвичайні ситуації • Планування на випадок надзвичайних ситуацій та нарощування спроможності щодо ризиків катастрофічних надзвичайних ситуацій • Політика безпечної та стійкої національної інфраструктури та корпоративної стійкості в приватному секторі Співпрацюючи з власниками KI та регуляторами, урядові департаменти, відповідальні за 13 критичних секторів, зобов'язані щорічно розробляти секторальні плани безпеки та стійкості. Ці плани, які ґрунтуються на ризиках, визначених у Національній оцінці ризиків, визначають розуміння кожним департаментом ризиків для своїх секторів і ключові заходи, які воно здійснюватиме для усунення цих ризиків протягом наступного року. Декілька агенцій надають центральному уряду, регуляторним органам, власникам і операторам інфраструктури поради щодо ризиків інфраструктури та їх пом'якшення, зокрема Центр захисту національної інфраструктури та Національний центр кібербезпеки. Жодних чітких санкцій чи інших наслідків не встановлено у випадку, якщо оператор KI не співпрацює з урядом.
США	Міністр внутрішньої безпеки забезпечує стратегічне керівництво та координує загальні федеральні зусилля. Секторальні федеральні агентства керують спільними процесами безпеки KI в кожному з 16 секторів KI. Кожне таке агентство несе відповідальність за розробку та реалізацію секторального плану, заснованого на унікальних характеристиках кожного сектора. Державні, місцеві, племінні та територіальні органи влади забезпечують безпеку та стійкість KI під їхнім контролем, а також тих, що належать і управляються іншими сторонами в межах їхньої юрисдикції. Механізми співпраці між власниками та операторами приватного сектору та державними установами сформульовані навколо кількох галузевих і міжгалузевих координаційних структур.

2.5.2 Державно-приватне партнерство для CIP

Додаток до Мадридських керівних принципів

Керівний принцип 51

У своїх подальших зусиллях щодо захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевою владою, повинні також розглянути:

...

(c) Встановлення процесів для обміну оцінками ризиків між урядом, промисловістю та приватним сектором для сприяння та підвищення обізнаності про ситуацію та посилення

У більшості країн переважна більшість критичних активів є приватною власністю. Ця обставина в поєднанні з тим фактом, що основна відповідальність за захист активів і систем КІ лежить на їхніх власниках і операторах, підкреслює важливість встановлення ефективних ДПП для досягнення належного рівня стійкості КІ.[35]

Маючи справу з PPP, розробники стратегій ЗІВ повинні прагнути створити умови для їхньої ефективності, по-перше, визначивши сферу їх застосування; по-друге, визначення їх форм; і по-третє, передбачення проблем і викликів..

2.5.2.1 Визначення сфери застосування

PPPs не повинні зосереджуватися на одній конкретній стадії циклу захисту, а охоплювати їх усі, від розробки планів безпеки до управління кризою та відновлення. Переваги об'єднання ресурсів, взаємної підтримки та спільного прийняття рішень між державним сектором і приватними операторами КІ поширюються на такі сфери, як оцінка безпеки, перегляд заходів безпеки, ідентифікація критичних активів і процесів, розробка планів на випадок надзвичайних ситуацій, реагування на аварії навчання та ін.

Обмін інформацією є ключовим – хоча й не виключним – аспектом PPP і створює певні проблеми, наприклад, у сфері захисту даних. Ключові питання, пов'язані з обміном інформацією, розглядаються в розділі 4.

2.5.2.2 Визначення форм

Найдоцільніша форма конкретного PPP залежить від багатьох факторів, таких як цілі, кількість зацікавлених сторін, які будуть залучені, і чи очікується, що партнерство вирішуватиме стратегічні чи операційні питання. PPP можуть приймати різноманітні форми, починаючи від дуже неформальних типів співпраці до більш офіційних умов. Ступінь формальності часто пов'язаний з рівнем контролю, який урядові установи прагнуть здійснювати. З іншого боку, стверджується, що так звані «проектно-орієнтовані» PPP, як правило, більш ефективні, ніж «процесно-орієнтовані», оскільки перші, як правило, включають більш чітко визначені місії, часові рамки та бюджети.[36]

2.5.2.3 Передбачання проблем і викликів

PPPs недостатньо продумані піддаються ризику стати тим, що іноді називають «порожніми ящиками», приносячи обмежену або не приносячи жодної додаткової вартості CIP. Щоб переконатися, що державно-приватні кооперативні домовленості зароджуються та продовжують залишатися актуальними та продуктивними зусиллями, державам-членам

необхідно пам'ятати про найпоширеніші причини невдачі. Недоліки можуть бути спричинені розбіжностями в очікуваннях між приватним і державним сектором, нестабільними моделями фінансування, нечітким розподілом праці та іншими подібними факторами. Можна стверджувати, що, як зазначено у випуску World Security Report за 2017 рік, «уподобання та уявлення про витрати та вигоди суб'єктів-учасників остаточно визначатимуть успіх чи провал партнерства. Почуття терміновості допомагає створити зв'язок між державним і приватним секторами, сприяючи виникненню бажання співпрацювати та досягати спільного бачення, що в кінцевому підсумку дозволяє партнерству розвиватися та розвиватися. Довговічність партнерства залежить від взаємодії цих факторів і є динамічним процесом з періодами як слабкої, так і сильної ефективності».[37]

Інші проблеми можуть бути пов'язані з відсутністю мотивації для операторів інвестувати фінансові ресурси в захист власних KI. У розділі 2.7.2 обговорюється необхідність стратегій CIP для визначення відповідних типів стимулів у цьому відношенні..

---

[35] Процес приватизації кількох секторів і підгалузей KI, таких як газ, поштові системи та телекомунікаційні послуги, який історично відбувався в багатьох країнах, призвів до того, що певні операції KI потрапили в приватні руки. Це, у свою чергу, породило потребу в сильних ДПП. Обмін інформацією для цілей CIP у життєво важливому завданні, яке має виконуватися в рамках такого партнерства.

[36] Ліна Колеснікова, «Виклики PPP у часі нових типів загроз безпеці», Звіт про світову безпеку, січень-лютий 2017 р. Доступно за адресою https://issuu.com/ torchmktg/docs/wsrjanfeb17/15.

[37] Там же

Вміст 8
Цінності, що лежать в основі ефективного PPP для CIP

Меридіанний процес, відкритий форум для обміну ідеями щодо CIP та співпраці між вищими державними політиками, визначив ряд ключових факторів, що лежать в основі ефективних PPP для CIP:

- Довіра: оскільки PPP часто стосуються делікатних питань, важливо створити атмосферу довіри, у якій усі організації усвідомлюють потребу одна одної в обережності. Чіткі вказівки членства щодо правил роботи можуть сприяти зміцненню довіри.
- Цінність: PPP повинні приносити користь як умову для підтримки ентузіазму та мотивації учасників протягом тривалого часу
- Повага: кожна залучена організація має визнавати додаткову цінність, яку інші організації привносять у спільну роботу.
- Кодекс поведінки: необхідно мати чіткі, конкретні та передбачувані правила, які не дають можливості для розсуду та запобігають будь-якому конфлікту інтересів.
- Усвідомлення можливостей і обмежень один одного: це запобігає конфлікту через неправильне оцінювання причини негативної відповіді та дозволяє отримати оптимальну віддачу від докладених зусиль. Це означає, що кожна організація повинна бути знайома з бізнесом інших організацій.

ВИВЧЕННЯ ПРОБЛЕМИ 9
Державно-приватне партнерство для стійкості KI: Фінляндія

У Фінляндії Національному агентству екстреного постачання доручено планувати, розвивати та підтримувати безпеку постачання в країні. Незважаючи на те, що його історична роль у підтримці резервних запасів для захисту засобів до існування населення, а також функціонування економіки залишається частиною його стратегічних завдань, Агентство все активніше впроваджує безперервність і стійкість бізнесу в різних секторах економіки через публічні -приватне партнерство.

Національне агентство екстреного постачання створило мережу тематичних кластерів, де ключові зацікавлені сторони критично важливих секторів розвивають партнерства з метою оцінки вразливості та ефективності, а також планування стійкості. Він також пропонує спеціалізовані інструменти, такі як інформаційні системи, засоби зберігання та транспортування для підтримки безперервності бізнесу в цих

ВИВЧЕННЯ ПРОБЛЕМИ 10
Платформа державно-приватного партнерства **UP KRITIS** *для CIP: Німеччина*

Інституціоналізований у 2007 році та адаптований у 2013 році, UP KRITIS є німецьким державно-приватним партнерством, яке забезпечує галузеву та міжгалузеву співпрацю для CIP. Основою його роботи є взаємна довіра. Учасники обмінюються ноу-хау та досвідом, а також навчаються один в одного щодо CIP. В рамках UP KRITIS розробляються концепції, налагоджуються контакти, проводяться навчання та розробляється та запускається спільний підхід для управління IT-кризами. У той же час UP KRITIS займається темами, які виходять за межі сфери IT, виходячи з визнання того, що окремого дослідження фізичної безпеки та безпеки IT недостатньо для досягнення спільної мети захисту критичної інфраструктури..

В рамках UP KRITIS відбувається дві форми співпраці: оперативно-технічна (між усіма учасниками) та стратегічно-концептуальна (у створених органах). Важливо, що бізнес залучається поступово і може бути більш чи менш інтенсивним, залежно від готовності компаній до проактивного залучення, мета полягає в тому, щоб гарантувати, що система залишається керованою, охоплюючи якомога більше компаній з усіх секторах KI. Зокрема, організація спочатку інтегрується в UP KRITIS як «учасник». Усі німецькі оператори KI, національні професійні та галузеві асоціації секторів KI, а також компетентні державні органи можуть подати заявку на участь у UP KRITIS. Учасники призначають представників своєї організації, яким надається доступ до продуктів UP KRITIS, у тому числі до конфіденційної інформації. Якщо організація бажає активніше співпрацювати, вона може стати «партнером» і подати заявку на інтеграцію своїх представників у галузеві робочі групи та тематичні робочі групи. Кожна робоча група утворює власну інформаційну мережу, в якій можна обмінюватися інформацією на конфіденційній основі.

Іншими ключовими складовими організаційної структури є Пленум і Рада. Пленум є комітетом взаємодії системи. Він діє між секторами, встановлюючи стратегічні ключові види діяльності UP KRITIS, *приймаючи рішення про створення або розпуск робочих груп, плануючи майбутні спільні дії та інші заходи. До складу Пленуму входять представники операторів KI, їх професійних та галузевих асоціацій, а також представники громадського сектору. Рада зміцнює партнерство та співпрацю в рамках* UP KRITIS *і дає поштовх для стратегічних цілей і проектів. Це також гарантує, що платформа може виконувати свої завдання, використовуючи відповідні ресурси та за необхідної підтримки керівництва з боку державного та приватного секторів. Рада складається з високопоставлених осіб, які приймають рішення, з операторів KI та державного сектору.*

Після прийняття Закону про безпеку IT у 2015 році та кількох поправок до Закону про Федеральне управління інформаційної безпеки (BSI), *категорії KI, які передбачають юридичні зобов'язання для їхніх операторів, наразі визначено в Законі про* BSI *разом із Постановою* BSI Kritis. *Зокрема, розділ 8a Закону про* BSI *вимагає від операторів KI вживати належних організаційних і технічних запобіжних заходів, щоб уникнути перебоїв у доступності, цілісності, автентичності та конфіденційності їхніх IT-систем, компонентів або процесів, які є вирішальними для функціональності KI, що експлуатуються ними.*

Федеральне відомство інформаційної безпеки здійснює наглядову функцію відповідно до Закону BSI *щодо операторів KI. Ця наглядова функція доповнюється спільною роллю на стратегічному та оперативному рівнях в рамках* UP KRITIS, *яка спрямована на покращення захисту KI в різних секторах. Міжгалузева співпраця між промисловістю та державою в рамках* UP KRITIS *стала успішною: понад 750 організацій співпрацюють на основі взаємної довіри в рамках галузевих і тематичних робочих груп. У той же час* UP KRITIS *займається темами, які виходять за межі сфери IT, виходячи з визнання того, що окремого дослідження фізичної безпеки та безпеки IT недостатньо для досягнення спільної мети захисту критичної інфраструктури та її стійкості.*

Конструктивний діалог між урядом та операторами CIP щодо майбутніх розробок, пов'язаних із фізичною безпекою та стійкістю критичних KI, залишається необхідним. Таким чином, UP KRITIS пропонує форум для обміну інформацією між урядом та операторами CIP щодо нового та майбутнього законодавства, наприклад майбутніх директив Європейського Союзу щодо питань, що стосуються CIP.

Джерело: Information provided by the Permanent Mission of Germany to the United Nations.

Інструмент 5

Посібник із надання допомоги у встановленні державно-приватного партнерства для захисту вразливих об'єктів UNICRI

Посібник був розроблений після серії семінарів, зустрічей експертів, аналізу та тестування, орієнтованого на дії. Розрахований на практиків безпеки з державних організацій і приватних компаній, він дотримується методології з 10 кроків і пропонує кілька інструментів, які допомагають у створенні або вдосконаленні PPP для

Інструмент 6
Восьмикрокове керівництво щодо PPPs для CIP – ОБСЄ

www.osce.org/files/f/documents/4/b/103500.pdf

ОБСЄ розробила основні вісьмокрокові вказівки щодо того, як країни мають максимізувати переваги, які можуть отримати PPP, враховуючи спільні інтереси всіх зацікавлених сторін. Хоча керівні принципи були розроблені в рамках передової практики для критично важливої енергетичної інфраструктури, вони, як видається, загалом застосовуються в усіх секторах:

- Крок 1: Проаналізуйте та визначте мотивацію кожного партнера бути включеним до партнерства CIP, щоб прояснити взаємні очікування та внески.
- Крок 2: Визначте амбіції та цілі CIP партнерства на основі загальних національних цілей CIP; уточнити мету партнерства CIP та завдання, які необхідно виконати (див. також крок 5).
- Крок 3: перевірка існуючої нормативно-правової бази, що стосується кожного сектора критичної інфраструктури; визначати обов'язкові та обов'язкові норми, правила та принципи; оцінити адекватність існуючої нормативно-правової бази з огляду на очікувані ризики та існуючі рівні готовності; обговоріть, як закрити можливі прогалини.
- Крок 4: Забезпечте механізми, захист і правову визначеність для обміну інформацією, пов'язаною з CIP, між усіма зацікавленими сторонами. Крім того, забезпечте механізми для добровільних зусиль, включаючи розвиток та обмін передовим досвідом, консультації та діалог для забезпечення постійного та ефективного партнерства.
- Крок 5: Створіть інституційну структуру, яка сприятиме міжорганізаційній співпраці та обміну інформацією; уточнити ролі та внески кожного партнера (наприклад, державних установ, власників та операторів критичної інфраструктури, постачальників продукції, асоціацій); визначити єдині точки контакту для кожного партнера; визначити орієнтири співпраці.
- Крок 6: Почніть з малого, зосередившись на одному або двох секторах критичної інфраструктури; стабільно зростати, спираючись на готовність усіх зацікавлених сторін співпрацювати та враховувати рівні загроз.
- Крок 7: Визначте важливі етапи, щоб переглянути те, що було досягнуто, і визначити можливі наступні кроки.
- Крок 8: Забезпечте постійний процес перевірки для перегляду та оновлення партнерських відносин, щоб забезпечити постійний прогрес, який відповідає загальному ландшафту ризиків, а також заходи безпеки та безпеки, необхідні для забезпечення оптимального рівня захисту.

2.5.3 Роль громадянського суспільства та громадськості

Громадськість загалом відіграє важливу роль як у запобіганні атакам на KI, так і в зменшенні шкоди після нападу (управління кризовими ситуаціями). Деякі держави-члени чітко передбачають роль окремих осіб у контексті стратегій CIP. Наприклад, французький план Vigipirate[38] *інструктує громадян, як поводитись у разі атак у конкретних контекстах, які мають відношення до захисту KI, як-от у метро, потягах, літаках і на кораблях, або у разі атак із застосуванням токсичний продукт. У Швеції впроваджено підхід, що охоплює все суспільство, усвідомлюючи, що окремі особи та сім'ї часто найбільше постраждали від кризи, або присутні на місці раніше, ніж служби першої допомоги чи інші соціальні представники. Окремих осіб слід розглядати як активи*[39]*. В авіаційному секторі так звана ініціатива «культури безпеки», запроваджена IKAO, спрямована на допомогу суб'єктам авіаційної галузі в покращенні реалізації заходів авіаційної безпеки добре підготовленими, мотивованими та професійної робочої сили та підвищення обізнаності серед громадськості (див. вміст 9).*

Методи та канали для досягнення ставлення до співпраці з боку громадськості суттєво відрізняються від тих, які необхідні для залучення операторів КІ. Як відправна точка, залучення громад та окремих осіб до загальних зусиль щодо стійкості КІ передбачає впровадження широких освітніх програм та кампаній з підвищення обізнаності. Комунікаційні стратегії мають відрізнятися відповідно до цільової групи. Ці стратегії можуть бути підтримані на місцевому рівні та залежно від контексту такими заходами, як встановлення спеціальних номерів екстрених служб, повторення повідомлень через гучномовці, що нагадують користувачам громадського транспорту про їхні обов'язки, серед іншого.

---

[38] Дивитись https://www.gouvernement.fr/vigipirate.

[39] Хелена Ліндберг і Бенгт Санделіус, «Стійкість суспільства до стихійних лих: шведський шлях», у Довіднику з внутрішньої безпеки McGraw-Hill (2-е видання), David Kamien (ed.), New York: McGraw-Hill, 2013, стор. 1295–1319. Доступний на https://www.semanticscholar.org/paper/Whole-of-Society-Disaster-Resilience-%3A-The- Swedish-Lindberg-Sundelius/9524aa4182828716ba5834c40ee6128f8674f54f.

Наприклад, після хвиль терористичних нападів на транспортні системи великих столиць за останні двадцять років державні адміністрації кількох країн запровадили заходи, щоб спонукати громадян бути пильними та повідомляти владі про підозрілі ситуації.

Широке використання технологічних продуктів громадськістю також означає, що соціальні медіа можуть відігравати важливу роль у підвищенні обізнаності про ситуацію, інформувати людей про дії, які вживає уряд, і своєчасно надавати інструкції щодо безпеки. Усе це видається особливо актуальним у кризових сценаріях, що швидко розвиваються..

Вміст 9
ICAO ініціатива «культура безпеки».

У резолюції A40-11 ICAO зазначено, що ІКАО має продовжувати розробляти інструменти для підвищення обізнаності та культури безпеки, культура безпеки визначена як головний пріоритет.40 Для досягнення цієї мети 2021 рік було оголошено «Роком культури безпеки». Відповідно ІКАО зосередила свою роботу на наступних пріоритетних видах діяльності:

- Проведення глобальної кампанії культури безпеки, яка підтримуватиме організацію національних, регіональних і глобальних заходів для підвищення обізнаності щодо безпеки в авіації.
- Посилення співпраці з державами-членами та галуззю в підтримці зусиль із просування культури безпеки у ширшому авіаційному співтоваристві, де безпека є відповідальністю кожного.
- Видання відповідних вказівок щодо практичних комунікаційних стратегій культури безпеки, планів і кампаній.
- Продовжувати пропонувати навчання та допомогу, зосереджену на просуванні ефективної та сталої культури безпеки в усіх організаціях, залучених до цивільної авіації.

Держави-члени, сім'я Організації Об'єднаних Націй, міжнародні та регіональні організації та зацікавлені сторони галузі працювали разом над кампанією підтримки та популяризації Року культури безпеки шляхом проведення та підтримки глобальних заходів культури безпеки (конференції, семінари, навчальні курси, семінари та вебінари) протягом 2021 року. Незважаючи на те, що кампанія офіційно завершилася в 2022 році, робота планується продовжити, оскільки Рік культури безпеки стане поштовхом для того, щоб усі працівники цивільної авіації постійно зосереджувалися на культурі безпеки.

Веб-сайт ICAO Security Culture41 надає світовій авіаційній спільноті найкращі практики культури безпеки та містить керівні документи, відео, статті та навчальні посилання від держав і галузей, а також безкоштовні інструменти та ресурси ICAO усіма офіційними мовами ООН. , включаючи набір інструментів ICAO щодо підвищення культури безпеки та стартовий пакет для кампанії ICAO з культури безпеки.

[40] Резолюція A40-11 була прийнята Асамблеєю ICAO на її сороковій сесії в 2019 році. Текст доступний за адресою https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf.

41 Дивитись https://www.icao.int/Security/Security-Culture/Pages/default.aspx.

ВИВЧЕННЯ ПРОБЛЕМИ 11
Методи екстреного оповіщення населення: Чилі, Франція та Велика Британія

Чилі

З моменту створення в 2012 році та офіційного впровадження в 2017 році Чилі використовує систему екстреного сповіщення для надсилання сповіщень та інформації про стихійні лиха, такі як повені, лісові пожежі, цунамі та землетруси. З 2017 року всі мобільні телефони, які продаються в країні, згідно із законом, повинні бути сумісні з системою. Незважаючи на те, що система розроблена для реагування на стихійні лиха, вона потенційно може бути розгорнута у випадку масштабних антропогенних катастроф.

Франція

Французька Reseau National d'Alerte («Національна мережа оповіщення») діє з метою попередження про неминучість ситуації, що стосується безпеки населення. Сигнал тривоги, що складається з приблизно 4500 сирен, може бути активований, наприклад, у разі токсичної або вибухонебезпечної хмари, радіоактивного ризику, загрози повітряної агресії та певних природних ризиків. Сирени випромінюють модульований сигнал, наростаючий і спадаючий, що складається з трьох послідовностей по 1 хвилині 41 секунді, розділених тишею тривалістю 5 секунд. Почувши сигнали, від громадян вимагається невідкладно вийти в закрите приміщення, вимкнути систему кондиціонування, опалення та вентиляції, послухати радіо.

Велика Британія

Національна система оповіщення через мобільний телефон – це система екстреного оповіщення населення, яка зараз розробляється і використовує стільникове мовлення. Перше тестування почалося в 2014 році, а перше тестове сповіщення було надіслано в березні 2020 року. Система призначена для використання під час великих криз, таких як повінь або терористичні атаки.

Технологія стільникового мовлення передбачає одночасне надсилання повідомлень кільком користувачам мобільних телефонів у певній зоні. Повідомлення стільникового мовлення спрямовуються на радіосоти, а не на певний телефон. Оскільки на нього не впливає навантаження трафіком, стільникове мовлення становить особливий інтерес у разі гострих криз, коли стрибки навантаження даних (соціальні мережі та мобільні додатки), регулярне використання SMS і голосових дзвінків (масові дзвінки) мають тенденцію значно перевантажувати мобільний зв'язок мережі.

Джерело: http://www.sae.gob.cl; https://www.alpes-de-haute-provence.gouv.fr/Actions-de-l-Etat/Securite-et-protection-des-populations/Protection-civile/Le-reseau-national-d-alerte-sirene/Les-sirenes-d-alerte; and https://www.gov.uk/alerts.

2.6 Побудова стратегій CIP на основі концепцій управління ризиками та управлінні кризами

Додаток до Мадридських керівних принципів

Керівний принцип 50

У своїх зусиллях щодо розробки та впровадження заходів для захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевими органами влади, повинні:

...

(b) ... регулярно проводити оцінку ризиків, щоб йти в ногу з мінливим характером загрози та супротивника, в тому числі використовуючи наявні інструменти та вказівки, розроблені міжнародними та регіональними організаціями;

Щоб бути ефективною, будь-яка національна стратегія повинна помістити процеси управління ризиками та управління кризами в центрі зусиль CIP. Незалежно від того, чи буде обрана добровільна чи обов'язкова модель захисту, зацікавлені сторони, залучені до CIP (будь то власники та оператори KI приватного сектору чи державні органи), повинні бути знайомі з цими концепціями та послідовно застосовувати їх у своїх відповідних секторах і сферах компетенції..

У контексті зусиль CIP проти тероризму управління ризиками та кризовими ситуаціями можна розглядати як ключові інструменти для досягнення оптимального рівня стійкості. Ця остання концепція розуміється як здатність конкретної KI, цілого критичного сектору або членів постраждалих громад протистояти лиху, спричиненому одним або кількома терористичними актами. В ідеалі, стійка інфраструктура – це така інфраструктура, яка не тільки відновлюється після кризи, але й вчиться на минулих кризах, щоб стати сильнішою перед обличчям майбутніх загроз.

2.6.1 Управління ризиками

Управління ООН зі зменшення ризиків стихійних лих визначає управління ризиками як «систематичний підхід і практику управління невизначеністю для мінімізації потенційної шкоди та збитків. Управління ризиками включає оцінку та аналіз ризиків, а також впровадження стратегій і конкретних дій для контролю, зменшення та передачі ризиків. Це широко практикується організаціями для мінімізації ризиків у прийнятті інвестиційних рішень і вирішення операційних ризиків, таких як зрив бізнесу, збій у виробництві, збиток навколишньому середовищу, соціальні наслідки та збиток від пожежі та стихійних лих».[42]

У контексті CIP важливо мати чітке розуміння ключових концепцій, що лежать в основі управління ризиками
концепція та пов'язані з нею процеси. Вони можуть бути визначені наступним чином:

- *Загроза:* все, що використовує вразливість KI.
- *Наслідок:* результат конкретних видів атак на конкретні KI.
- *Вразливість:* слабкість KI, яка може бути використана загрозою.
- *Ризик:* потенціал втрати, пошкодження, знищення або втручання в здатність KI надавати свої послуги в результаті загрози, яка використовує вразливість.

Щоб визначити та впровадити найбільш ефективні заходи зменшення ризику, системи

управління ризиками повинні спочатку детально розробити механізми отримання дійсної інформації, пов'язаної із загрозами, та проведення відповідних оцінок загроз. Вони мають враховувати місцеві, національні та міжнародні обставини. У межах існуючих фінансових і технічних обмежень результуючі заходи пом'якшення мають бути пропорційними характеру та рівню оціненого ризику. Система також має бути побудована з необхідною гнучкістю, щоб гарантувати, що вона може швидко адаптуватися до швидко мінливих ландшафтів безпеки.

---

[42] 2009 Термінологія щодо зменшення ризику лиха. Доступний на https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction.

Вміст 10
Стандарти ISO з управління ризиками

Міжнародна організація зі стандартизації (ISO) є незалежною неурядовою організацією, до складу якої входять 162 національні органи стандартизації. Через своїх членів ISO об'єднує експертів для обміну знаннями та розробки добровільних, заснованих на консенсусі ринкових міжнародних стандартів, які підтримують інновації та пропонують рішення для глобальних проблем. ISO опублікувала понад 22 000 міжнародних стандартів і пов'язаних документів, що стосуються майже всіх галузей, від технологій до безпеки харчових продуктів, сільського господарства та охорони здоров'я..

ISO 31000 був розроблений технічним комітетом ISO з управління ризиками як стандарт, застосовний до всіх організацій незалежно від типу, розміру, діяльності та місця розташування. Він охоплює всі типи ризиків і призначений для використання всіма, хто займається управлінням ризиками, а не лише професійними менеджерами з ризиків. ISO 31000 спеціально спрямований на те, щоб допомогти організаціям розробити стратегію управління ризиками для ефективного виявлення та пом'якшення ризиків, тим самим підвищуючи ймовірність досягнення своїх цілей і покращуючи захист своїх активів. Її головна мета — розвинути культуру управління ризиками, у якій співробітники та зацікавлені сторони усвідомлюють важливість моніторингу та управління ризиками.

Дотримуючись того самого підходу до управління ризиками, що й ISO 31000, серія ISO 27000 забезпечує еталонний стандарт у сфері систем інформаційної безпеки. Таким чином, ISO 27000 пропонує керівну основу для захисту ICI.

Підключений стандарт, розроблений ISO у 2021 році, стосується управління ризиками подорожей. Це вимагає від організацій передбачати та оцінювати потенціал подій, розробляти лікування та повідомляти своїх мандрівників про очікувані ризики. Консультування та надання мандрівникам відповідних медичних рекомендацій і вказівок щодо реагування на надзвичайні ситуації, запобіжних заходів безпеки та інформаційної безпеки, включно з проблемами логістики подорожей, можуть мати вплив на результат руйнівних подій, зокрема, коли вони стосуються KI..

Джерело: https://www.iso.org/iso-31000-risk-management.html/; https://www.iso.org/standard/73906.html; and https://www.iso.org/standard/54204.html.

2.6.2 Антикризовий менеджмент

Стосовно CIP, управління кризою стосується процесів, які діють для роботи з подіями, які порушують або загрожують

порушити надання послуг KI. Системи антикризового управління зазвичай вимагають виконання наступних кроків:

- Передбачення та планування відповідних реакцій на потенційні кризи[43]
- Виявлення поточної чи неминучої кризи
- Протистояння кризі, щоб мінімізувати її вплив і забезпечити якнайшвидше повернення до нормального

надання послуг

У рамках кризового менеджменту поняття «відповідь» часто використовується для позначення дій, вжитих під час і відразу після вчинення терористичного акту або загрози вчинення терористичного акту. Дії у відповідь зазвичай спрямовані на:

- Запобігання або мінімізація наслідків атаки, таких як втрата життя, поранення, пошкодження майна та пошкодження або порушення інфраструктури
- Розслідування кримінальних справ
- Надання негайної допомоги та підтримки постраждалому населенню

У порівнянні з відповіддю, «відновлення» зазвичай визначає дії, виправдані в довгостроковій перспективі для підтримки зусиль з реконструкції, включаючи фізичну інфраструктуру та відновлення статус-кво з точки зору фізичного, соціального та економічного добробуту громад. Розширені психологічні наслідки терористичних актів за межі конкретного місця інциденту свідчать про те, що в деяких випадках відновлення можна розуміти як процес, що вимагає інтегрованої та сталої співпраці між урядовими установами, приватним сектором та організаціями громадянського суспільства.

---

[43] Країни часто використовують терміни «планування на випадок непередбачених обставин» і «планування на випадок надзвичайних ситуацій» як синоніми. Однак, строго кажучи, плани на випадок надзвичайних ситуацій є реактивними за своєю природою, тоді як плани на випадок надзвичайних ситуацій є більш активними. У той час як плани на випадок надзвичайних ситуацій призначені для обмеження наслідків або впливу інциденту, плани на випадок надзвичайних ситуацій розроблені для передбачення подій і підготовки всіх зацікавлених сторін до надзвичайної ситуації, а також для забезпечення повернення.

2.6.3 Оцінка ризику

Порівняно з оцінками ризиків, які проводяться щодо інших небезпек, ідентифікація та оцінка терористичних ризиків для KI породжує певні проблеми. Деякі з цих проблем виникають через високу невизначеність, що оточує цей тип дослідження. Як було зазначено, «фундаментальною проблемою в цьому контексті є те, що терористи адаптують свою поведінку до змін у ландшафті безпеки»[44]. З цієї точки зору терористичну загрозу слід розглядати як динамічну, яка пристосовується, наприклад, до змін у ресурси, доступні терористичній групі, і зміни в функціях безпеки потенційної цілі.

Стратегії CIP також повинні визнавати, що оцінка ризику, пов'язаного з тероризмом, щодо KI базується на здатності працювати з кількома наборами індикаторів, а також контекстуалізувати доступну інформацію. Зміни в геополітичних реаліях, економічній ситуації, динаміці влади між злочинними організаціями та іншими обставинами слід враховувати та заохочувати до проведення оцінки ризиків через регулярні проміжки часу.

Важливо, що для оцінки можуть бути використані докази попередніх атак або загроз проти KI, особливо якщо вони відбувалися неодноразово протягом тривалого часу або постійно були спрямовані на певні сектори чи KI в певних регіонах. Оцінки також можуть спиратися на дані, доступні з інших країн, зокрема, коли можна зробити висновок про аналогії. Наприклад, якщо певна терористична група атакувала критично важливі об'єкти в країні X і країні Y, і відомо, що ця група також активна в країні Z, цей факт слід враховувати при плануванні безпеки для подібних об'єктів у країні Z.

Слід також докласти зусиль для виявлення «низькоінтенсивних» ознак потенційних терористичних планів. Зафіксовані акти порушень проти CI, наприклад звичайне проникнення, можуть свідчити про зацікавленість терористів у тому, як функціонує CI, або про спроби здійснювати ретельне спостереження за певними місцями. Водночас на основі одиничних і спорадичних вчинків часто неможливо зробити висновки. Розвідувальні служби відіграють ключову роль у виявленні закономірностей подій, які здаються незначними, якщо розглядати їх окремо.

Хоча очікується, що стратегії CIP не містять повних переліків індикаторів і джерел загроз, вони повинні бути побудовані таким чином, щоб надати повноваження (або повноваження, залежно від обраних моделей управління CIP) відповідним органам влади формувати процеси оцінки ризиків

відповідно до текучості і мінливий характер терористичної загрози.

[44] Виконавчий директорат Контртерористичного комітету, «Фізичний захист критичної інфраструктури від терористичних атак», Звіт про тенденції CTED, 2017 р. Доступно за адресоюhttps://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf.

Вміст 11

Методика ICAO для оцінки ризиків авіаційної безпеки

Методологія оцінки ризиків авіаційної безпеки ICAO була розроблена для розуміння та відносного ранжування поточного залишкового ризику з метою інформування при виробленні політики. Незважаючи на те, що методологія була розроблена з урахуванням загроз цивільній авіації, більшість її елементів можна вважати загальноприйнятними. Цей процес оцінки ризику складається з наступних елементів:

- Визначення й аналіз вірогідних і конкретних сценаріїв загрози та їхньої ймовірностіAssessment of their consequences
- Оцінка існуючих заходів пом'якшення та вразливості, що залишилися
- Отримання значення ризику на основі результатів ймовірності, наслідків і вразливостей
- Оцінки конкретного сценарію загрози
- Рекомендації щодо подальшої роботи з оцінки ризиків та можливі заходи пом'якшення

Ключовими компонентами завершення оцінки ризику є наступні:

- *Сценарій загрози:* ідентифікація та опис достовірного акту незаконного втручання, що включає ціль (наприклад, термінал аеропорту, пов'язану з ним інфраструктуру, літак чи іншу КІ), спосіб дії (включаючи передачу та приховування) та методи атаки (наприклад, саморобний вибуховий пристрій) і супротивник (на основі ролі та ролі супротивника в авіаційній системі – пасажир, особа, яка не подорожує, або інсайдер). Це повинно бути достатньо детально, щоб дозволити точну оцінку та аналіз; «Напад на літак» недостатньо хороший як сценарій, тоді як «пасажир нападає на термінал аеропорту з використанням саморобного вибухового пристрою (СВУ) у багажі» буде достатнім.
- *Ймовірність атаки (загрози):* ймовірність або ймовірність спроби цієї атаки (сценарію загрози) на основі намірів і можливостей терористів, але без урахування поточних заходів безпеки. Ймовірність використовується як показник загрози, враховуючи як намір, так і здатність злочинця реалізувати сценарій загрози.
- *Наслідки:* характер і масштаб наслідків конкретної атаки в людському, економічному, політичному та репутаційному планах за обґрунтованого найгіршого сценарію.
- *Поточні заходи пом'якшення:* відповідні стандарти та рекомендації (які не всі можуть бути в Додатку 17 ІКАО та які, як зазвичай припускається, ефективно застосовуються; якщо це явно не так, ризик буде вищим) або інші відповідні національних або місцевих програм і правил, щоб зменшити ймовірність успішної атаки або зменшити наслідки, якщо атака станеться. Передбачається, що жодна загроза не може бути повністю усунена.
- *Вразливість:* ступінь вразливості, що залишилася після врахування поточних заходів пом'якшення.
- *Ризик*: загальний ризик успішної атаки, який залишається, якщо припустити, що поточні заходи пом'якшення були впроваджені, враховуючи ймовірність загрози та наслідки.
- *Можливі додаткові заходи пом'якшення:* визначені заходи, які можуть бути реалізовані для подальшого пом'якшення залишкових ризиків, якщо це необхідно.

Важливо, щоб оцінка ризику ретельно та достатньо детально ідентифікувала всі вірогідні сценарії, а також була конкретною та ретельною для розгляду кожної форми загрози. Загрози можуть бути спрямовані на конкретні аеропорти, термінали чи іншу інфраструктуру, таку як паливні ферми, засоби управління повітряним рухом або навігаційне обладнання, а також на літаки, включаючи різні типи авіації, такі як авіація загального призначення, пасажирські літаки та вантажні літаки. . Слід також оцінити засоби та методи, за допомогою яких може бути реалізована загроза. Це включало б, як може бути виготовлена зброя чи вибуховий пристрій, засоби, за допомогою яких вони можуть бути передані (наприклад, чи перевозиться на людині чи транспортному засобі) і ким (працівник, пасажир чи представник громадськості)), як його можна було приховати та як його можна було активувати або використати для вчинення акту незаконного втручання.

Джерело: Представник ICAO.

Формулюючи свої стратегії CIP навколо підходу до управління ризиками, країни повинні втілити в життя два основні керівні принципи, викладені нижче..

2.6.3.1 Багаторівненва вправа

Визначення характеру та рівнів загроз для КІ та пов'язаних з ними вразливостей обов'язково є спільним і узгодженим результатом оцінок, проведених кількома зацікавленими сторонами на різних рівнях управління (федеральному, якщо це можливо, національному та місцевому). Стратегія CIP повинна встановити основу для інтеграції ландшафту загроз, які спостерігаються на національному рівні, рівні критичного сектора та рівні оператора КІ.

Що стосується оцінок на національному рівні, їхня мета полягає в тому, щоб досягти розуміння загрози, з якою стикається КІ країни, її наслідків і пов'язаних із цим вразливостей. Важлива додаткова цінність загальнонаціональних оцінок полягає в тому, що вони підкреслюють, як різні критичні сектори взаємодіють один з одним. Процеси та висновки на основі розвідувальних даних, які підтримують розробку оцінок національної безпеки та боротьби з тероризмом, також є важливими для визначення ландшафту загроз, що впливають на КІ.

Окрім оцінки ризиків на національному рівні, важливо розробити профілі ризиків для конкретних секторів КІ. Ці профілі повинні містити оцінку існуючих заходів пом'якшення. Залежно від галузі, що розглядається, оцінки ризиків можуть проводитися для конкретних підгалузей і згодом використовуватися для ширших профілів ризиків галузі.[45]

На рівні інфраструктури оператори КІ часто є тими, хто найкраще знає, як працюють конкретні активи та процеси, які вони контролюють. Отже, вони мають конкретне уявлення про свої внутрішні вразливі місця. Крім того, компанії часто запускають цикли управління ризиками незалежно від інституційної ролі, яку вони покликані відігравати в CIP. Корпорації в основному займаються управлінням ризиками, щоб мінімізувати шкоду, яка може вплинути на цілі компанії, з метою гарантування безперервності бізнесу або обмеження наслідків загрози. Не зосереджуючись на CIP, цей тип управління ризиками спрямований на виявлення ризику для безперервності виробництва та встановлення заходів для пом'якшення. У результаті це може принести пряму користь інфраструктурі компаній і підвищити рівень стійкості. Таким чином, держави-члени повинні ретельно розглянути роль, яку мають відігравати процеси управління ризиками компанії в контексті стратегій CIP, включаючи те, як інтегрувати оцінки корпоративного рівня в процеси прийняття рішень CIP.

2.6.3.2 Процес із залученням багатьох зацікавлених сторін

Ефективна оцінка ризику є результатом консультаційного процесу, який базується на точках зору та висновках різноманітних державних установ, служб екстреної допомоги та організацій приватного сектора. Хоча за звичайних умов державні установи беруть на себе провідну роль у розробці національних і галузевих оцінок загроз, а оператори КІ беруть на себе ініціативу щодо конкретних планів КІ, внесок усіх зацікавлених сторін завжди бажаний. Хоча залучення широкого кола зацікавлених сторін може уповільнити весь процес, досвід країн показує, що цінності інклюзивності та прозорого прийняття рішень відіграють важливу роль у досягненні визнання. Це ключова передумова, враховуючи, що кілька зацікавлених сторін несуть відповідальність за впровадження

стратегій CIP.

Інклюзивність процесу також дає змогу розглядати ризики з різних точок зору. Отримано спільне розуміння взаємодії між різними типами інфраструктури та критичними секторами. Однак забезпечення широкого участі процесу та його загальної узгодженості супроводжується проблемами. Загальна проблема полягає в тому, що різні зацікавлені сторони сприймають ризики по-різному. Як зазначено в Плані захисту національної інфраструктури Міністерства внутрішньої безпеки Сполучених Штатів від 2013 року, «партнери з критично важливої інфраструктури керують ризиками на основі різноманітних зобов'язань перед суспільством, зосереджені на добробуті клієнтів і структурах корпоративного управління. Допуски до ризику відрізнятимуться від організації до організації, а також від сектора до сектору, залежно від бізнес-планів, ресурсів, операційної структури та нормативного середовища. Вони також відрізняються між приватним сектором і урядом через основні обмеження. Різні організації, ймовірно, матимуть різні пріоритети щодо інвестицій у безпеку, а також потенційно різні судження щодо того, якою може бути відповідна точка толерантності до ризику».[46]

---

[45] Наприклад, Австралійська стратегія стійкості критичної інфраструктури розбиває транспортний сектор на такі підгалузі: авіація, масовий наземний пасажирський транспорт (включаючи мости та тунелі), наземні вантажні перевезення та морські перевезення (судноплавство та порти). Згідно з цією ж Стратегією, енергетичний сектор складається з електроенергетичних систем, постачання нафти та газу на суші, а також постачання вугілля. Додаткова інформація доступна за адресою https://www.cisc.gov.au/help-and-support-subsite/Files/ critical_infrastructure_resilience_strategy_plan.pdf.

[46] Міністерство внутрішньої безпеки США, «NIPP 2013: партнерство для безпеки та стійкості критичної інфраструктури», 2013 р., стор. 15. Доступно за адресою https://www.cisa. gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Важливо не тільки визнати існування різних поглядів і підходів зацікавлених сторін, але й зрозуміти, як вони можуть вплинути на загальний процес встановлення спільних пріоритетів. З цієї точки зору досягнення «безпеки та стійкості критично важливої інфраструктури залежить від застосування практик управління ризиками як промисловості, так і уряду, у поєднанні з наявними ресурсами та стимулами для спрямування та підтримки зусиль».[47]

ВИВЧЕННЯ ПРОБЛЕМИ 12
Регіональна програма оцінки стійкості: Канада

Канадська регіональна програма оцінки стійкості є комплексною програмою оцінки ризиків для власників і операторів канадських КІ. Він містить оцінки сайтів, щоб допомогти організаціям виміряти та покращити свою стійкість до всіх небезпек у Канаді, включаючи кіберзагрози та навмисні техногенні події. Оцінки сайтів є добровільними, нерегульованими, безкоштовними та конфіденційними. Вони також визначають додаткові економічно ефективні заходи, щоб допомогти власникам і операторам зменшити ризики та покращити їх здатність реагувати на збої та відновлюватися після них.

Щоб підвищити стійкість критичної інфраструктури, регіональна програма оцінки стійкості використовує наступні чотири інструменти:

- Інструмент стійкості критичної інфраструктури (1 день на завершення)

  Інструмент на основі огляду на місці, який вимірює стійкість і захисні заходи об'єкта. Результати включають звіт та інтерактивні інформаційні панелі, які надають оцінки та порівняння аналогів, висвітлюють залежності та параметри підвищення стійкості для фізичної безпеки, стійкості та кібербезпеки.

- Мультимедійний інфтру

  Віртуальна візуалізація об'єкта на основі планів поверхів. Він містить панорамні фотографії внутрішніх і зовнішніх значних ділянок, ними можна поділитися з особами, які швидко реагують, і використовувати їх під час навчань.

  Незважаючи на те, що робити це на їхній розсуд, організаціям настійно рекомендується ділитися мультимедійним інструментом критичної інфраструктури з особами, які швидко реагують, щоб його можна було використовувати як інструмент для підготовки до надзвичайних ситуацій і реагування на них.

- Огляд кіберстійкості Канади (від одного до півтора днів на виконання)

  Інструмент на основі опитування на місці, який вимірює стан кібербезпеки організації.

  Результати включають два звіти (короткий і всеосяжний) з оцінками в 10 сферах системи кібербезпеки Національного інституту стандартів і технологій, порівняння аналогів і варіанти підвищення стійкості.

- Інструмент аналізу стійкості безпеки мережі (1 день на виконання)

  Інструмент технічного аналізу на місці, який забезпечує виправлення конфігурації пристрою та порівнює мережу кібербезпеки на відповідність стандартам.

  Результати включають звіти (короткі та вичерпні) з візуалізацією мережі, ідентифікацією шляхів

критичного ризику атак, а також виявленням невідповідності мережевих пристроїв і параметрами підвищення стійкості.

Інструмент забезпечення стійкості критичної інфраструктури та перевірка кібервідмовостійкості вимагають присутності осіб, які є експертами в галузі безпеки об'єктів, IT та управління об'єктами. Організації можуть запитувати кожен із інструментів окремо або всі інструменти як пакет. Використання всіх трьох інструментів зазвичай займає три дні. Перевірки після оцінки можуть проводитися в організації протягом 24 місяців після оцінки. Організації також можуть виявити зацікавленість в участі в ширшій регіональній оцінці. Ці проекти зазвичай передбачають роботу кількох організацій у певному регіоні. Під час вивчення конкретної небезпеки мета полягає в тому, щоб допомогти у визначенні ключових взаємозалежностей, а також можливостей для індивідуальної та колективної мінімізації впливу та ймовірності збою. Під час регіонального оцінювання індивідуальні інструменти оцінювання розгортаються разом із інструментами моделювання, семінарами, зустрічами зацікавлених сторін та інтерв'ю з експертами.

Джерело: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

[47] там же, стор. 15.

ВИВЧЕННЯ ПРОГРАМИ 13
Національні та субнаціональні оцінки ризиків: Фінляндія

Національні оцінки ризиків

Розробка проекту національної оцінки ризику Міністерством внутрішніх справ Фінляндії почалася в 2015 році і ґрунтується на рішенні № 1313/2013/ЄС Європейського парламенту та Ради щодо «Механізму цивільного захисту Союзу».[48]

Національні оцінки ризиків є об'єднанням оцінок ризиків, проведених різними гілками національної адміністрації. Вони обирають сценарії загроз і збоїв, які вважаються такими, що погіршують життєві функції суспільства на національному рівні. Компетентні міністерства несуть відповідальність за розробку власних сценаріїв загроз і збоїв шляхом формування груп для написання, які також використовують експертні думки у відповідних галузях адміністрації міністерств. Зусилля авторських груп об'єднуються та редагуються в остаточному вигляді Національною робочою групою з оцінки ризиків. При складанні національної оцінки ризиків використовуються рекомендації Європейського Союзу. На етапі планування також враховуються національні оцінки ризиків інших країн.

Сценарії загроз, враховані останньою національною оцінкою, яка була проведена в 2019 *році, включають*:

- Терористичні акти, спрямовані проти суспільних структур або великих натовпів
- Порушення суспільного господарства
- Збої в роботі фінансової системи
- Значні перебої в електропостачанні
- Серйозні перебої з доступністю палива
- Серйозні збої в роботі комунікаційних мереж і послуг
- Перебої з водопостачанням
- Збої в постачанні продуктів харчування
- Морські багатогалузеві аварії
- Серйозна аварія на атомній електростанції у Фінляндії або в сусідніх з країною областях

Субнаціональні оцінки ризиків

Субнаціональні оцінки ризиків проводяться як окремий проект одночасно з національною оцінкою. Вони розроблені з використанням міжгалузевого підходу, щоб у робочих групах були представлені муніципалітети, органи влади, підприємства та організації регіону. Представники широко використовують досвід і знання своїх власних спільнот і референтних груп.

Метою субнаціональних оцінок є не виявлення та перелік усіх можливих сценаріїв загрози, що впливають на регіон, а радше вибір тих, які є найбільш значущими. Результати складаються в письмовий звіт, який розповсюджується операторам у регіоні для використання та, якщо необхідно, іншим зацікавленим сторонам. Очікується, що як національні, так і субнаціональні оцінки ризиків будуть використовуватися, серед іншого, оцінкою ризиків кожного оператора КІ як спільної основи для готовності.

Джерело: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161351/9_2019_National%20risk%20assessment.pdf

[48] Згідно зі статтею 6 рішення, держави-члени зобов'язані розробляти оцінки ризиків на національному або відповідному субнаціональному рівні та подавати Комісії зведення відповідних елементів кожні три роки.

ВИВЧЕННЯ ПРОБЛЕМИ 14
Національна оцінка ризику: Швеція

Шведське агентство з надзвичайних ситуацій відповідає за питання, пов'язані з цивільним захистом, громадською безпекою, управлінням у надзвичайних ситуаціях і цивільною обороною, доки жоден інший орган не несе відповідальності до, під час і після надзвичайної ситуації чи кризи. Агентство працює шляхом підвищення знань, підтримки, навчання, навчань, регулювання, нагляду та власних операцій у тісній співпраці з муніципалітетами, окружними радами, іншими державними органами та приватним сектором.[49]

Згідно з національним законодавством, усі державні установи зобов'язані розробити та подати аналіз ризиків і вразливості до Агентства цивільних непередбачених ситуацій. На основі таких звітів Агентство проводить національні оцінки ризиків з 2011 року. Ці документи мають на меті забезпечити стратегічну основу для спрямування та подальшого розвитку цивільних непередбачених ситуацій.

На основі національної оцінки ризиків за 2021 рік Агентство склало документ щодо посилення цивільної готовності, в якому висвітлено кілька соціальних викликів, а також найбільш суттєві загрози та ризики, з якими стикається Швеція. Серед визначених сфер, де необхідно розвинути посилені можливості, документ наголошує на важливості вдосконалення критичної інфраструктури та безпеки постачання. У ньому, зокрема, підкреслюється необхідність визначення критичної

ВИВЧЕННЯ ПРОБЛЕМИ 15
Розвідувальний підхід до захисту KI від терористичних атак: Австралія

Австралія покладається на потужний режим запобігання та готовності, який керується розвідкою, щоб підтримувати заходи щодо боротьби з тероризмом. Цей підхід включає цілеспрямовані заходи запобігання та готовності, засновані на принципах управління ризиками та підтримці спроможності керувати різними видами терористичних загроз, нападів та їх наслідків. Антитерористична розвідка та кримінальні розслідування проводяться Австралійською організацією безпеки та розвідки (ASIO) та правоохоронними органами. Передача інформації про терористичну загрозу KI власникам і операторам KI швидко та належним чином дає змогу цим власникам і операторам приймати більш обґрунтовані рішення щодо управління ризиками та вживати ефективних заходів із зменшення ризиків у відповідь на загрозливе середовище.

Оцінки загроз ASIO вказують на рівні загрози та ймовірний характер тероризму, політично мотивованого насильства, шпигунства, іноземного втручання, насильницьких протестів і диверсій. Оцінки загрози можуть проводитися для конкретних подій, об'єктів, людей або секторів і відрізняються від національного рівня загрози тероризму. ASIO розповсюджує оцінки загроз відповідним урядовим установам Австралії, урядам штатів і територій, федеральній поліції Австралії, а також поліції штатів і територій. Власникам і операторам KI також надається копія національної оцінки терористичної загрози, і очікується, що вони будуть використовувати її у своїх процесах підготовки та планування. ASIO надає консультації щодо загроз приватному сектору та державним установам через відділ зв'язку з бізнесом. У разі особливої терміновості ASIO зв'язується з поліцією штату та території та іншими відповідними організаціями, включаючи власників і операторів CI, якомога швидше та до надсилання письмової консультації. Хоча оцінки загроз ASIO враховують наміри та можливості терористів, вони не оцінюють вразливість або достатність існуючої безпеки KI. Згодом оцінки загроз слід використовувати в аналізі ризиків безпеки, щоб визначити вимоги та тип заходів пом'якшення для будь-якого конкретного об'єкта KI.

Джерело:https://www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf.

[49] Уряд Швеції керує Агенцією з надзвичайних ситуацій за допомогою ряду інструкцій і щорічних асигнувань. Інструкція визначає обов'язки та завдання Агентства. Асигнування визначає його цілі та вимоги до звітності, а також ресурси, виділені для його управління та діяльності.

Інструмент 7
Рамкова система оцінки національних можливостей – ENISA

https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

Рамкова система оцінки національних можливостей є результатом роботи, проведеної Агентством Європейського Союзу з кібербезпеки (ENISA). Він спрямований на надання країнам самооцінки рівня зрілості з точки зору можливостей кібербезпеки як на стратегічному, так і на оперативному рівні. Рамкова програма була розроблена за підтримки експертів із предметних питань ENISA та представників 19 держав-членів Європейського Союзу та країн ЄАВТ. Цільова аудиторія включає політиків, експертів і державних службовців, відповідальних або залучених до розробки, впровадження та оцінки національних стратегій кібербезпеки та, на більш широкому рівні, можливостей кібербезпеки.

Рамкова програма базується на п'яти рівнях зрілості, що визначають етапи, через які проходять країни, створюючи можливості кібербезпеки. Рівні представляють зростаючі стадії зрілості, починаючи з рівня 1

Інструмент 8
Глобальний огляд інструментів оцінювання

https://cybilportal.org/publications/global-overview-of-assessment-tools-goat/

Глобальний огляд інструментів оцінювання, розроблений Робочою групою A (Стратегія та оцінка цільової групи) Глобального форуму з кіберекспертизи, ґрунтується на необхідності підвищення обізнаності про різні існуючі інструменти оцінки кіберпотужності та надання детальної інформації про їх методології, результати і вплив. Метою Огляду є підтримка процесу формування політики у визначенні відповідних інструментів і підходів, орієнтованих на переважаючі потреби та прогалини в знаннях, а також надання вказівок щодо того, що робити та до кого звертатися, якщо країна бажає отримати оцінку.

Спеціально вибрані інструменти для оцінки кіберпотужності країни включають наступне:

- Боротьба з кіберзлочинністю: інструмент Світового банку для нарощування потенціалу
- Кіберзрілість в Азіатсько-Тихоокеанському регіоні: Австралійський інститут стратегічної політики
- Індекс кіберготовності 2.0: Потомакський інститут політичних досліджень
- Модель зрілості потенціалу кібербезпеки для країн: Глобальний центр потенціалу кібербезпеки
- Структура розробки та реалізації кіберстратегії: Корпорація MITRE

2.6.4 Зменшення ризику

У попередньому розділі було підкреслено важливість проведення комплексної та інтегрованої оцінки ризиків на різних рівнях управління та кількома зацікавленими сторонами. Управління ризиками має зрештою перетворитися на конкретні заходи пом'якшення, спрямовані на мінімізацію ризику руйнівної події, що вплине на CI. Відповідно, у цьому розділі розглядається роль трьох конкретних типів заходів пом'якшення в контексті зусиль CIP. Примітно, що стратегії CIP та пов'язані з ними дії щодо реалізації мають ґрунтуватися на ідеї, що ефективні заходи захисту на рівні CI вимагають інтеграції фізичних, пов'язаних з персоналом елементів та елементів кібербезпеки.

У той же час, зниження ризику терористичних атак на КІ має бути частиною широкого, багатопрофільного та загальнонаціонального завдання передбачення та зриву планів, змов та інших видів підготовки з метою здійснення терористичних актів загалом. Захист КІ зрештою залежить від скоординованих дій розвідувальних служб і правоохоронної спільноти в цілому, серед інших факторів. Ступінь, до якого кримінальне законодавство використовує превентивний підхід, у поєднанні зі здатністю слідчих органів бути проактивними (на відміну від простого реагування на вчинення терористичних актів), відіграє фундаментальну роль у зусиллях із зменшення ризиків.

Ефект від заходів пом'якшення, як правило, можна максимізувати за допомогою реалізації так званої концепції «поглибленого захисту», згідно з якою низка послідовних захисних заходів розташовується на рівні, щоб захистити критично важливий актив або процес. Якщо один набір заходів не спрацьовує, правопорушник негайно стикається з іншим набором заходів. Основний принцип полягає в тому, що безпека інфраструктури суттєво не погіршується через втрату будь-якого окремого рівня.

Нарешті, при визначенні найбільш відповідних заходів пом'якшення, які слід застосовувати до СІ, держави-члени повинні оцінити ступінь їхнього потенційного впливу на реалізацію прав людини (наприклад, вплив на свободу пересування, спричинений обмеженнями безпеки сайту, втручанням у особисті конфіденційність, викликана технологіями відеоспостереження, та інші ефекти). Мета захисту КІ від терористичних атак повинна бути збалансована з необхідністю поважати основні права людини, закріплені в міжнародних договорах, таких як Міжнародний пакт про громадянські та політичні права. Зокрема, слід впроваджувати лише ті заходи, які вважаються суворо необхідними для досягнення CIP. Заплановані заходи також повинні бути оцінені та, якщо вони реалізовані, переоцінені з точки зору їх пропорційності поставленим цілям.

2.6.4.1 Заходи фізичного захисту

У рамках багаторівневого підходу до поглибленого захисту можна вжити ряд заходів для посилення фізичного захисту КІ. Деякі з цих заходів включають:

- Окреслення периметрів зони КІ та захист фізичними бар'єрами.
- Патрулювання та спостереження правоохоронними органами та операторами СІ з метою швидкого виявлення підозрілої діяльності, що відбувається навколо критичного об'єкта (наприклад, розвідка об'єкта), і повідомлення про це компетентним органам.
- Контроль доступу з функціями безпеки, які використовуються для підвищення його

продуктивності або ефективності (наприклад, покриття з колючого дроту, система виявлення вторгнень по периметру, освітлення або система замкнутого телебачення).

- Використання таких технологій, як перевірка та інші засоби контролю безпеки (такі як звичайне рентгенівське обладнання або рентгенівське обладнання високої чіткості, собаки для виявлення вибухових речовин, ручні обшуки, ручні металодетектори та виявлення слідів вибухових речовин).

Заходи фізичної безпеки повинні підтримуватися належним чином перевіреним і навченим персоналом, надійним і комплексним плануванням на випадок надзвичайних ситуацій і планами безпеки, розробленими на рівні оператора КІ. Більше того, держави-члени все частіше впроваджують так звані підходи «безпеки за проектом» як інструмент для досягнення цілей фізичної безпеки на етапі проектування та будівництва (або реконструкції) будівель, які містять КІ.

ВИВЧЕННЯ ПРОБЛЕМИ 16
Закон про захист безпеки 2019: Швеція

Закон про захисну безпеку 2019 року поширюється як на державні, так і на приватні організації, які займаються чутливою до безпеки діяльністю, важливою для національної безпеки та інфраструктури Швеції. Він охоплює широкий спектр компаній, які працюють в IT, правоохоронних органах, транспорті та інших секторах. Перш ніж наймати нового персоналу, будь-яка компанія, яка обробляє «конфіденційну інформацію», як це визначено в Законі, повинна провести захисний аналіз безпеки, запровадити заходи безпеки та провести оцінку безпеки персоналу.

Шведський закон про захисну безпеку поширюється на будь-яку організацію, яка займається чутливою до безпеки діяльністю. Вони визначаються як види діяльності:

- Вирішальний для національної інфраструктури Швеції, або
- Важливо для безпеки Швеції, або
- На нього поширюється міжнародне зобов'язання щодо безпеки, яке є обов'язковим для Швеції
  Організації, які працюють у наведених нижче секторах, вважаються такими, що здійснюють діяльність, чутливу до безпеки:
  - Захист
  - Правоохоронні органи
  - Енергопостачання
  - Водопостачання
  - Телекомунікації
  - Транспорт

Будь-яка компанія, яка займається діяльністю, пов'язаною з безпекою, підпадає під дію Закону про захисну безпеку, незалежно від того, чи працює вона в одному з перелічених вище секторів.

Для виконання Закону підприємства повинні:

- Проведіть захисний аналіз безпеки
- Впровадити заходи захисту безпеки на основі цього аналізу, охоплюючи:
  - *Інформаційна безпека*
  - *Фізична охорона*
- Перш ніж найняти будь-яку особу, проведіть оцінку безпеки персоналу будь-якого співробітника, який буде це робити:
  - *Мати доступ до секретної інформації*
  - *Займайтеся діяльністю, яка стосується безпеки*
  - *Беріть участь в операціях, що потребують захисту від терористичних актів*
- Захищайте інформацію про національну безпеку від розголошення
- Обмежте доступ до операцій, які:
  - *Вимагати захисту від терористичних актів, або*
  - *Мають вирішальне значення для національної безпеки*
- Укладайте угоди про захисну безпеку щоразу, коли третя сторона може отримати доступ до конфіденційної, таємної чи секретної діяльності (лише державні органи)
- Призначте менеджера з захисної безпеки (фактично головного спеціаліста з інформаційної безпеки, який контролює інформаційну безпеку в усій організації)

Як державний орган, який відповідає за національну безпеку та боротьбу з тероризмом у країні, Шведській службі безпеки («Säkerhetspolisen») доручено забезпечити дотримання Закону про безпеку та інших правил безпеки в державних установах і компаніях. Зокрема, Служба безпеки Швеції може:

- Вирішіть, чи потрібно проводити захисну перевірку безпеки
- Проводити захисні перевірки безпеки
- Видавати рекомендації щодо покращення захисної безпеки
- Надавати консультації та підтримку організаціям, які займаються чутливою до безпеки діяльністю

- Проведіть перевірку на безпеку, перш ніж особі буде дозволено брати участь у діяльності, що стосується безпеки, або отримати доступ до секретної інформації

Компанії, на які поширюється Закон про захисну безпеку, можуть звернутися до Служби безпеки Швеції за порадою щодо дотримання закону.

Джерело: https://www.termsfeed.com/blog/swedish-protective-security-act/.

ВИВЧЕННЯ ПРОБЛЕМИ 17
Розроблена безпека критичної інфраструктури: Сінгапур

Концепцію «запроектної безпеки» можна застосувати не лише до фізичних активів, а й до ICI. Стратегія кібербезпеки Сінгапуру до 2021 року конкретно встановлює мету попередження кіберуразливостей шляхом сприяння методам «безпеки за проектом». Вони визначаються як «підхід до розробки програмного та апаратного забезпечення, спрямований на мінімізацію вразливостей системи та зменшення поверхні атаки шляхом розробки та створення безпеки на кожному етапі розробки».

Згідно зі Стратегією, Уряд зобов'язується «посилити взаємодію з … професійними організаціями, такими як інженери та розробники програмного забезпечення, щоб заохотити їх створювати безпечні продукти та послуги.

Джерело: https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

Інструмент 9
Інструкції з фізичної безпеки від Німеччини, Сінгапуру, Великобританії та США

Країна	Інструмент
Німеччина	**Захист критичної інфраструктури – базова концепція захисту, рекомендації для компаній** www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.html *Цей інструмент розроблено Федеральним міністерством внутрішніх справ і громадськості, Федеральним управлінням цивільного захисту та реагування на стихійні лиха та Федеральним управлінням кримінальної поліції. Бізнес-спільнота надала свій досвід із самого початку. Базова концепція захисту надає компаніям у Німеччині рекомендації з точки зору внутрішньої безпеки. Він містить анкету та контрольний список.* **Центр компетенції з фізичної безпеки (державних будівель)** https://bundesbau-bw.de/fileadmin/BBBW/Ueber_uns/2021-10_FLY_MaterielleSicherheit_8-Seiter_DE_ES_screen.pdf *На основі директиви нової коаліційної угоди від 2022 року Федеральне міністерство внутрішніх справ і громади створило Центр компетенції для фізичної безпеки цивільних урядових будівель. Центр відповідає за розробку основних концепцій і вказівок щодо фізичної безпеки (зокрема проти терористичних загроз) і технічних консультацій на етапі планування та реалізації проектів будівництва урядових будівель.*
Великобританія	**Центр захисту національної інфраструктури (CPNI)** www.cpni.gov.uk/advice CPNI *пропонує поради, набори інструментів і посібники з наступних тем і підтем*: • Безпека персоналу та людей (зниження внутрішнього ризику; оптимізація безпеки людей; зрив ворожої розвідки) • Фізична безпека (пошук і скринінг для запобігання загрозам; фізичний захист; контроль доступу та замки; виявлення та моніторинг зловмисників; активна затримка доступу; будівельні конструкції; вікна та фасади; двері; будівельні послуги та приміщення; диспетчерські; конфіденційна інформація та активи))
Сінгапур	***Рекомендації щодо підвищення безпеки будівель у Сінгапурі*** www.bca.gov.sg/Publications/BuildingSecurity/building_security_booklet.html Рекомендації містять перелік належних практик безпеки та міркувань, щоб допомогти власникам будівель включити прагматичні процедури безпеки, концепції фізичного захисту та технології безпеки в плани безпеки своїх будівель. Оскільки Рекомендації призначені для використання для всіх типів приміщень, і враховуючи, що ризики, пов'язані з цими приміщеннями, значно відрізняються, метою є не надання рекомендацій, а радше інформація, яку варто враховувати під час планування безпеки будівлі. Намір також полягає в тому, щоб заходи, пов'язані з безпекою, не були нав'язливими та залишалися відповідними загальному дизайну будівлі, за допомогою комплексних рішень, які служать як функціональним, так і безпековим цілям. Очікується, що Рекомендації слугуватимуть загальною системою відліку та забезпечуватимуть мінімальний рівень прийнятних стандартів безпеки в галузі.. ***Стандарт системи відеоспостереження за будівлями*** www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security *Камери в стратегічних місцях по всій будівлі та її периметру можуть допомогти власникам будівель завчасно виявляти аномалії, ефективно реагувати на можливі загрози безпеці та злочини та координувати ресурси під час непередбачених ситуацій. Система відеоспостереження також діє як інструмент, який підтримує розслідування інцидентів і надає докази. Однак система не виконує активну роль у захисній безпеці та не повинна бути розроблена, щоб служити єдиним захисним засобом у визначеній зоні, але повинна працювати разом з іншими заходами безпеки, такими як контроль доступу, сигналізація виявлення вторгнення системи, системи виявлення вторгнень в огорожі,*

реагування безпеки та інші.

Стандарт системи відеоспостереження для будівель призначений для підтримки впровадження відеоспостереження для покращення загального управління безпекою та захистом будівлі. Він ґрунтується на ряді рекомендацій, якими можна керувати та надавати власникам будівель

послідовний підхід до рекомендованих специфікацій, встановлення та експлуатації відеоспостереження в будівлях у Сінгапурі. Стандарт також може бути використаний іншими країнами як джерело керівництва та натхнення. Враховуючи динамічний характер індустрії відеоспостереження, цей документ зосереджується на гарному дизайні та експлуатаційних міркуваннях і може не описувати всі конкретні технології та можливості в системі відеоспостереження. Оскільки на ринку доступно багато варіантів відеоспостереження, власникам будівель слід розглянути можливість залучення послуг консультанта з питань безпеки при проектуванні комплексної системи відеоспостереження..

Інструмент 9

Інструкції з фізичної безпеки від Німеччини, Сінгапуру, Сполученого Королівства та Сполучених Штатів (продовження)

США	***Охорона громадських зібрань* (Cyber ISA)** cisa.gov/securing-public-gatherings CISA надає низку ресурсів для нарощування потенціалу для власників і операторів CI для підвищення безпеки громадських зібрань. Доступні ресурси охоплюють численні вектори загроз, включаючи несанкціонований доступ до об'єктів, кібербезпеку, безпеку виборів, активну стрільбу, бомбові атаки та малі безпілотні літальні системи. **Пильність співробітників за допомогою «Power of Hello» (CISA)** cisa.gov/employee-vigilance-power-hello CISA розробила інфографіку, щоб допомогти фахівцям, не пов'язаним із безпекою, і співробітникам CI ідентифікувати та оцінити підозрілу поведінку, яку можна спостерігати. Продукт пропонує запитання для розгляду під час навігації щодо потенційної загрози та містить інформацію про те, коли та як отримати допомогу. Інструмент доступний 17 мовами. ***Деескалація для власників і операторів KI* (CISA)** cisa.gov/de-escalation-series CISA розробив чотири інструменти, щоб допомогти власникам і операторам KI розпізнавати попереджувальні ознаки того, що хтось на шляху до насильства; оцінити, чи загострюється ситуація чи особа, що викликає занепокоєння, чи потрібна екстрена реакція; і, можливо, деескалацію ситуації шляхом цілеспрямованих дій, вербальної комунікації та мови тіла. Інструменти підкреслюють важливість повідомлення про ситуацію за допомогою встановлених протоколів, включаючи місцеві правоохоронні органи щодо безпосередніх загроз. **Активна підготовленість стрільця (CISA)** cisa.gov/active-shooter-preparedness Програма готовності до активних стрільців CISA спеціально зосереджена на підтримці зусиль державного та приватного секторів щодо створення потенціалу безпеки проти загрози активних стрільців, яка є найпоширенішим вектором атак у Сполучених Штатах. Програма складається з продуктів, інструментів, відео та перекладених ресурсів, які надають інформацію про поведінкові показники, потенційні методи нападу, створення плану дій у надзвичайних ситуаціях, дії, які можуть бути вжиті для підвищення ймовірності виживання, і як швидко відновитися після інцидент. Ресурси включають: • Відео про варіанти для розгляду, перекладене кількома мовами • Посібник, відео та шаблон плану дій у надзвичайних ситуаціях • Перекладені ресурси підготовки до стрільців (cisa.gov/translated-active-shooter-resources)

2.6.4.2 Загроза безпеки персоналу (внутрішня загроза)

Малоймовірно, що злочинні та терористичні групи досягнуть успіху у своїх спробах зруйнувати об'єкт CI без змови співробітників об'єкта, які надають доступ до конфіденційних даних та інформації про слабкі місця та процеси, а також інші вразливі області. Це підкреслює необхідність захисних стратегій не лише для захисту зовнішніх периметрів KI та утримання небажаних відвідувачів, але й для використання управління людськими ресурсами як ключового інструменту для запобігання вербування елементів, пов'язаних із злочинними та терористичними групами..

Поняття безпеки персоналу також відноситься до політики та процедур, необхідних для зниження ризику, пов'язаного з внутрішніми загрозами (а саме, загрозами, створеними нинішніми чи колишніми працівниками, сторонніми підрядниками чи діловими партнерами), які

використовують свій законний доступ до приміщень. , системи або процеси KI з метою здійснення несанкціонованих дій. Ефективна безпека персоналу передбачає низку заходів, починаючи від перевірок і процедур відбору до навчання з питань безпеки, сприяння пильності та загальної культури безпеки.

Інструмент 10
Зниження внутрішньої загрози – CISA (США)

cisa.gov/insider-threat-mitigation

CISA надає ресурси та тренінги, зосереджені на допомозі зацікавленим сторонам у досягненні кращого розуміння потенційних загроз, створених інсайдерами, і методів зменшення ризиків. Доступні інструменти розроблені, щоб допомогти організаціям втрутитися до того, як особа з привілейованим доступом порушить роботу KI ненавмисно (через недбалість) або через навмисні дії.

Ресурси включають:

- Посібник із зменшення внутрішньої загрози

2.6.4.3 Заходи кібербезпеки

Заходи кібербезпеки призначені для захисту КІ від кібератак. Не обов'язково технологічного характеру, вони допомагають зберегти цілісність, стійкість і нормальне функціонування КІ. Вони можуть, наприклад, включати процедури та політику безпеки, організаційні заходи, підвищення обізнаності та навчання, спеціальні вказівки щодо розвитку та регулярні оцінки безпеки.

ВИВЧЕННЯ ПРОБЛЕМИ 18
Національні системи кібербезпеки щодо захисту ІСІ: Японія, Португалія, Сінгапур та США

Японія: Політика кібербезпеки для захисту критичної інфраструктури, 2017 р

Метою Політики кібербезпеки Японії є підтримка безпечного та безперервного надання послуг КІ на основі концепції забезпечення місії, запобігання серйозним впливам на національне життя та соціально-економічну діяльність, спричинених будь-якими збоями КІ внаслідок кібератак, і забезпечення швидкого відновлення після збоїв. Політика базується на низці всеосяжних принципів, у т.ч:

- Очікується, що оператори КІ будуть впроваджувати заходи кібербезпеки під свою власну відповідальність, хоча спільні зусилля між зацікавленими сторонами вважаються необхідними. У той час як оператори КІ повинні прагнути до постійного вдосконалення цих заходів як організації, що надають послуги та несуть соціальну відповідальність, державні установи повинні надавати їм необхідну підтримку.
- Усі зацікавлені сторони повинні розуміти важливість задавати питання «коли», «де», «хто», «чому», «що» і «як» під час реагування на збої КІ, залежно від масштабу збоїв, і повинні мати можливість спокійно розглядати ознаки або виникнення будь-яких відключень. Вони також повинні бути здатними співпрацювати з іншими зацікавленими сторонами та реагувати на співпрацю та узгоджено, на додаток до забезпечення міцного зв'язку між різними зацікавленими сторонами та вжиття проактивних заходів.
- Вище керівництво має розвивати готовність до інцидентів навіть у звичайний час і, у разі інциденту, належним чином розкривати інформацію про реагування з метою завоювання довіри та виховання почуття безпеки серед зацікавлених сторін. Вони також повинні постійно забезпечувати управлінські ресурси, такі як бюджети та персонал, необхідні для вищезазначених заходів, і належним чином розподіляти їх з точки зору ризику.

Португалія: Національна стратегія безпеки кіберпростору (2019-2023)

Стратегія ґрунтується на трьох стратегічних цілях, які перетворюються на шість осей втручання. Осі 3 («Захист кіберпростору та інфраструктури») окреслює наступні напрямки діяльності:

- Визначити та закріпити знання СІІ, слідуючи змінам у національній та міжнародній правовій базі безпеки кіберпростору.
- Сприяти безперервному розвитку потенціалу та зрілості національних організацій щодо запобігання, виявлення, реагування та відновлення за наявності несприятливих сценаріїв для безпеки кіберпростору, які можуть вплинути на їхні мережі та інформаційні системи та загальну систему, яка їх підтримує, зміцнюючи взаємну довіру, обмін інформації та знань, а також швидкої та ефективної співпраці.
- Сприяти національним та галузевим структурам співпраці для захисту кіберпростору, включаючи державний сектор на центральному, регіональному та місцевому рівнях, а також приватний сектор, включаючи малі та середні підприємства, для обміну інформацією та сприяння взаємна співпраця у захисті спільних інтересів.
- Забезпечити застосування механізмів і стимулів, що сприяють розробці національних і міжнародних еталонних рамок для управління безпекою в кіберпросторі та їх прийняття національними структурами, які відповідають за критичну інфраструктуру та основні послуги.
- Максимально підвищити безпеку та захист мереж та інформаційних систем збройних сил і національної оборони з метою збереження здатності діяти в кіберпросторі за допомогою кіберзахисту.

Сінгапур: Закон про кібербезпеку 2018 року

Прийнятий у 2018 році Закон формалізує політику країни в цій сфері та чітко формулює захист ІСІ з точки зору концепцій кібербезпеки та заходів захисту. Закон переслідує чотири цілі:

- Створити нормативну базу, яка формалізує зобов'язання власників КІІ щодо забезпечення кібербезпеки відповідних КІІ.
- Надати Агентству кібербезпеки Сінгапуру повноваження керувати загрозами та інцидентами кібербезпеці та реагувати

на них.

- Створити структуру для обміну інформацією про кібербезпеку з Агентством кібербезпеки та захистом такої інформації.
- Створити систему ліцензування для постачальників послуг кібербезпеки.

Підхід та ініціативи США щодо захисту КІІ

Агентство з кібербезпеки та безпеки інфраструктури (CISA) керує зусиллями федерального уряду щодо захисту КІ країни, включно з КІ. З метою запобігання, пом'якшення та реагування на кіберзагрози в цій сфері ініціативи CISA спрямовані на:

- Розроблення технологічно нейтральної добровільної структури кібербезпеки
- Сприяння та стимулювання впровадження практик кібербезпеки
- Збільшення обсягу, своєчасності і якості обміну інформацією про кіберзагрози
- Включення надійного захисту конфіденційності та громадянських свобод у кожну ініціативу для забезпечення критичної інфраструктури
- Розвитку здатності ситуаційної обізнаності, яка розглядає як фізичні, так і кібернетичні аспекти функціонування інфраструктури майже в реальному часі
- Розуміння каскадних наслідків збоїв інфраструктури
- Оцінка і вдосконалення державно-при
- Оновлення Національного плану захисту інфраструктури
- Розробка комплексного плану досдаджень і розробок

CISA *заохочує прийняти Рамку кібербезпеки Національного інституту стандартів і технологій для покращення кібербезпеки критичної інфраструктури. Переглянута в* 2018 *році Рамкова основа містить вказівки щодо чотирьох ключових функцій, що покращують управління ризиками кібербезпеки*:

- Визначення - розвиток організаційного розуміння для управління ризиками кібербезпеки для систем, людей, активів, даних і можливостей.
- Захист - розробка та впровадження відповідних заходів безпеки для забезпечення надання критично важливих послуг
- Виявлення - розробка та впровадження відповідних заходів для виявлення виникнення події кібербезпеки.
- Реагування - розробка та впровадження відповідних заходів для вжиття заходів у відповідь на виявлений інцидент кібербезпеки.
- Відновлення - розробка та впровадження відповідних заходів для підтримки планів стійкості та відновлення можливостей або послуг, які були порушені внаслідок інциденту кібербезпеки.

Джерело : https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf; https://www.csa.gov.sg/legislation/cybersecurity-act; https://www.cisa.gov/resources-tools/resources/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and; *та* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. *Інформація надана Постійним представництвом Португалії при ООН.*

Інструмент 11

Інструменти захисту КІІ: Посібник із національної стратегії кібербезпеки та репозиторій - ITU

Щоб підтримати своїх держав-членів у розробці національних стратегій кібербезпеки для захисту ІСІ, Міжнародний союз електрозв'язку (МСЕ) розробив два основні інструменти:

Керівництво з розробки національної стратегії кібербезпеки (NCS Guide), 2021

- https://ncsguide.org/the-guide/

Друге видання Посібника містить гнучку та зручну структуру, що встановлює контекст для соціально-економічного бачення країни та поточного стану безпеки. Він допомагає розробникам політики у розробці стратегії, яка враховує конкретну ситуацію в країні, культурні та соціальні цінності та заохочує прагнення до безпечних, стійких, зміцнених ІКТ та пов'язаних суспільств.

Посібник був розроблений на основі ітераційного підходу, який мав на меті досягти згоди шляхом досягнення консенсусу. Він заснований на наявних ресурсах і має на меті полегшити його використання національними зацікавленими сторонами. Усюди, де це можливо, відповідні джерела та інструменти, використані для розробки кожного набору рекомендацій, перераховані в розділі «Довідка», щоб заохотити їх ширше використовувати.

- *Репозиторій національних стратегій кібербезпеки*

Інструмент 12

Інструменти та підходи до авіаційної кібербезпеки - ОБСЄ www.icao.int/cybersecurity/Pages/default.aspx

Протягом багатьох років сектор цивільної авіації пройшов через цифрову трансформацію, спрямовану на використання потужності технологій для підвищення безпеки, безпеки, ефективності та потенціалу сектора. Сектор цивільної авіації характеризується взаємопов'язаністю, складністю, високим рівнем медіа-освіти та критичною роллю, яку він відіграє в соціально-економічному розвитку країн. Таким чином, цивільна авіація є привабливою мішенню для злочинців як у фізичному світі, так і в кіберсфері..

Сектор цивільної авіації є глобальним за своєю природою, як і взаємодія систем і потоків даних, які виходять за межі національних кордонів. Відповідно, ІКАО бореться з кіберзагрозами інфраструктурі цивільної авіації, сприяючи та залучаючи до співпраці з боку всіх зацікавлених сторін.

Стратегія авіаційної кібербезпеки ОБСЄ

Визнаючи багатогранний і міждисциплінарний характер кібербезпеки та відзначаючи, що кібератаки можуть одночасно впливати на широкий спектр сфер і швидко поширюватися, Стратегія авіаційної кібербезпеки підтримує бачення ІКАО щодо збереження стійкості сектору цивільної авіації до кібератак, безпеки та довіри в усьому світі, а також продовжуючи впроваджувати інновації та рости. Стратегія визначає сфери, де необхідно забезпечити узгоджений і цілісний підхід до кібербезпеки та кіберстійкості цивільної авіації: міжнародне співробітництво; управління; ефективне законодавство та нормативні акти; політика кібербезпеки; обмін інформацією; управління інцидентами та реагування на надзвичайні ситуації; а також нарощування потенціалу, навчання та культура кібербезпеки.

www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

План дій з кібербезпеки

План дій є керівним документом, який підтримує держави та зацікавлені сторони у впровадженні Стратегії авіаційної кібербезпеки. Він розробляє сім основ Стратегії у 32 пріоритетних сферах, які далі розвиваються у 51 завдання для реалізації.

Методичний план

У 2020 році ІСАО почала розробку настанов з авіаційної кібербезпеки, щоб підтримати розвиток наскрізного гармонізованого підходу до авіаційної кібербезпеки в усіх дисциплінах цивільної авіації. Опубліковані на сьогоднішній день інструкції включають посібник із використання протоколу світлофора для підтримки обміну інформацією про кібербезпеку, інструкції щодо політики кібербезпеки та інструкції щодо розробки та впровадження надійної культури кібербезпеки в цивільній авіації.

Нарощування потенціалу

ІСАО також почала розробляти навчальний портфель авіаційної кібербезпеки для подальшої підтримки своїх держав-членів. На сьогодні завершено роботу над двома курсами: перший під назвою «Основи лідерства та технічного менеджменту авіаційної кібербезпеки» – це курс глибокої обізнаності, який охоплює всі аспекти авіаційної кібербезпеки та розроблений у партнерстві з Авіаційним університетом Ембрі-Рідл. Другий, «Управління ризиками безпеки в організації повітряного руху», поєднує елементи кібербезпеки та фізичної безпеки в середовищі організації повітряного руху. Він був розроблений у партнерстві з Європейською організацією з безпеки аеронавігації (EUROCONTROL). Продовжується робота над розширенням портфоліо навчальних курсів з авіаційної кібербезпеки. ІКАО зараз працює над третім курсом, який зосереджується на нагляді за кібербезпекою в цивільній авіації, який розробляється в партнерстві з Управлінням цивільної авіації Сполученого Королівства.

Панель кібербезпеки

У 2022 році ІСАО створила Групу з кібербезпеки для просування роботи з кібербезпеки авіації, яка раніше виконувалася неформальною групою. Завдання групи охоплюють широкий спектр сфер міжнародної цивільної авіації, таких як авіаційна безпека, безпека, аеронавігація та управління ризиками, оскільки вони стосуються кібербезпеки. Його повноваження охоплюють розробку стандартів авіаційної кібербезпеки, процедур та інструкцій для сектору міжнародної цивільної авіації, огляд та оцінку глобальної авіаційної кіберзагрози, а також надання експертних консультацій експертним групам і групам

експертів ICAO, коли вони розглядають елементи авіаційної кібербезпеки в їхня робота.

Інструмент 13
Готовність міста до кібертероризму – мережа боротьби з тероризмом

https://www.london.gov.uk/sites/default/files/ctpn_preparedness_for_cyber-enabled_terrorism_report_single_pages.pdf

Звіт, підготовлений Мережею підготовки до боротьби з тероризмом (CTPN) у 2022 році, підтримує зусилля із захисту критичної інфраструктури від кібератак і, як наслідок, кібертероризму. Він зосереджується на готовності до критичної інфраструктури, основних послуг і міських операцій, стверджуючи, що залежність суспільства від цифрової інфраструктури та взаємозалежність між нею відкриває потенційні шляхи для кібертероризму.

Звіт має на меті залучити органи влади (зокрема, ті, що діють на рівні міста), надавши докази необхідності постійного підвищення готовності до низки кіберзагроз і роботи, щоб гарантувати, що частота та серйозність кібертероризму не зростатиме

Інструмент 14
Посібник з конвергенції кібербезпеки та фізичної безпеки – Агентство з кібербезпеки та безпеки інфраструктури: США

https://www.cisa.gov/cybersecurity-and-physical-security-convergence

Посібник був розроблений як інформаційний інструмент про конвергенцію та переваги цілісної стратегії безпеки, яка узгоджує функції кібербезпеки та фізичної безпеки з організаційними пріоритетами та бізнес-цілями. Це базується на уявленні про те, що коли підрозділи фізичної безпеки та кібербезпеки працюють ізольовано, їм бракує цілісного уявлення про загрози безпеці, спрямовані на їхнє підприємство. Як наслідок, більша ймовірність успішних атак, які можуть призвести до таких наслідків, як компрометація конфіденційної або конфіденційної інформації, економічний збиток, порушення критичних функцій або втрата

Інструмент 15
Настанови та інструменти поради щодо кібербезпеки від Національного центру кібербезпеки: Велика Британія

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Велика кількість посібників доступна в Національному центрі кібербезпеки (NCSC) Сполученого Королівства. Різні інструменти впорядковано за темами в 46 категоріях, які включають:

- *Контроль доступу*
- *Активний кіберзахист*
- *Управління активами*
- *Автентифікація*
- *Сертифікація*
- *Хмарне сховище*
- *Криптографія*
- *Кіберобізнаність*
- *Кіберстратегія*
- *Тренування*
- *Управління інцидентами*
- *Паролі*
- *Безпека, орієнтована на людей*

Інструмент 16

Посібник із підвищення безпеки промислових інформаційних і керуючих систем: Швеція

www.msb.se/RibData/Filer/pdf/27473.pdf

На основі міжнародно визнаних вказівок, практик і методів роботи Шведське агентство з питань надзвичайних ситуацій розробило 17 рекомендацій щодо підвищення безпеки промислових інформаційних і контрольних систем. Хоча деякі рекомендації мають технічний характер, інші зосереджуються на методологічних аспектах, як зазначено нижче:

1. Забезпечити прихильність керівництва та відповідальність за безпеку промислової інформації та систем керування.
2. Уточнити ролі та відповідальність за безпеку промислових інформаційних та контрольних систем.
3. Підтримувати процеси системного обстеження та управління ризиками в промислових інформаційних та контрольних системах.
4. Забезпечити систематичне управління змінами в промислових інформаційних та керуючих системах.
5. Забезпечити систематичне планування на випадок надзвичайних ситуацій та управління інцидентами в промислових інформаційних і контрольних системах.
6. Запровадити вимоги безпеки до промислових інформаційних і контрольних систем із самого початку під час планування та закупівель.
7. Створити гарну культуру безпеки та підвищте усвідомлення необхідності безпеки в промислових інформаційних і контрольних системах.
8. Робота з архітектурою безпеки в промислових інформаційно-керуючих системах.
9. Постійно контролювати підключення та системи з метою виявлення спроб вторгнення в промислові інформаційні та контрольні системи.
10. Проводити регулярний аналіз ризиків промислової інформації та систем управління.
11. Проводити періодичні технічні аудити безпеки промислових інформаційно-керуючих систем.
12. Постійно оцінювати фізичну безпеку промислової інформації та систем керування.
13. Регулярно перевіряти, чи всі з'єднання з промисловими інформаційними та контрольними системами безпечні та відповідні.
14. Зміцнювати та модернізувати промислові інформаційні та контрольні системи у співпраці з постачальниками систем.
15. Проводити навчання та практику щодо IT-інцидентів у промислових інформаційних та керуючих системах.
16. Слідкувати за інцидентами в промислових інформаційних і контрольних системах і контролюйте зовнішні проблеми безпеки.
17. Брати участь в асоціаціях користувачів, органах стандартизації та інших мережах безпеки в промислових інформаційних і контрольних системах.

Посібник містить пояснення щодо кожної рекомендації, допоміжні рекомендації та приклади ризиків і проблем, з якими можна зіткнутися.

Інструмент 17

Найкращі практики захисту КІІ – Досвід Латинської Америки та Карибського басейну та окремих краї – Міжамериканський банк розвитку

https://publications.iadb.org/publications/english/document/Best-Practices-for-Critical-Information-Infrastructure-Protection-(CII- P)-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf

Структура цього посібника з найкращих практик, розробленого Міжамериканським банком розвитку, відображає типову структуру структури CIIP, *яка складається з наступних основ:*

- *Стратегія та законодавство*
- *Управління та регулювання*
- *Визначення та присвоєння*
- *Захист*
- *Обмін інформацією*
- *Антикризовий менеджмент*

Представлені тематичні дослідження надають цілеспрямований внесок у кожен із зазначених вище стовпів і

Інструмент 18
Належні практики КІІ – Глобальний форум кіберекспертизи - Меридіан

https://thegfce.org/wp-content/uploads/2020/06/CriticalInformationInfrastructureProtectionCIIP.pdf

Керований спільнотою Meridian, великою групою офіційних осіб із понад 60 країн, Глобальний форум кіберекспертизи – Ініціатива Meridian CIIP має на меті підтримати політиків, які відповідають за CIIP, щоб зрозуміти значення та наслідки проблем кібербезпеки та підтримувати обізнаність поточних подій. Працюючи разом у рамках глобальної ініціативи, ініціатори використали свій досвід на користь ширшої аудиторії, щоб допомогти розвинути можливості CIIP, зокрема в країнах, що розвиваються. У рамках ініціативи у 2017 році було розроблено два практичні посібники:

- Глобальні передові практики GFCE - захист критичної інформаційної інфраструктури (CIIP)

Базуючись на попередніх дослідженнях, матеріалах Глобального форуму з питань кіберекспертизи та зустрічі Meridian CIIP у Мексиці (2016), літературі та досвіді, отриманому під час інтерв'ю, цей документ надає політикам стислі знання, які допоможуть їм визначити стійкі та ефективні зусилля для захисту національних ICI.

- *Посібник із належної практики GFCE-Meridian щодо захисту критичної інформаційної інфраструктури для урядовців*

Цей посібник із належної практики було розроблено, щоб підвищити бар'єри захисту та досягти прогреси на

2.6.5 Планування та врегулювання криз, що впливають на КІ

Стратегії CIP повинні враховувати, які типи структур і процесів антикризового управління повинні бути на місці. Держави-члени можуть визначити, наприклад, що один державний орган має бути призначений головною відповідальністю та повноваженнями для визначення курсу дій, які необхідно вжити, коли виникає криза. Далі ця організація координуватиме втручання різних аварійних служб, забезпечуючи взаємодію систем зв'язку та достатній час реагування, а також плани евакуації для обмеження впливу поточної кризи. Для пом'якшення наслідків атаки необхідно заздалегідь спланувати, перевірити та оцінити реагування екстреної групи.

Ідентифікація найбільш підходящої системи управління кризою також вимагає визначення того, чи буде управління в надзвичайних ситуаціях застосовувати підхід до всіх небезпек або до конкретних небезпек. Обидва підходи мають переваги та недоліки. Коли структури управління кризою створені для конкретних типів загроз, можна запровадити індивідуальні процеси. Однак вибір підходу до конкретної небезпеки може виявитися проблематичним, коли природа інциденту не ясна, оскільки це може викликати невизначеність щодо застосовної основи для втручання.

Нормативні рамки для управління кризою в сфері КІ можуть ґрунтуватися на галузевому або міжгалузевому підході. Якщо вибрано перший підхід, законодавча база часто приймається міністерством, відповідальним за відповідний сектор, або регулюючим органом сектора. Навпаки, міжгалузевий підхід часто передбачає ухвалення одного або кількох законодавчих актів.50 Яку б

структуру управління кризою не було обрано, необхідно встановити чіткі правові та операційні рамки, сумісні з правами людини, усвідомлюючи, що управління кризою є важливо у випадку не лише особливо руйнівних терористичних атак, але й незначних інцидентів, щоб уникнути або зменшити вплив чи ескалацію кризи.

---

[50] У разі атаки на хімічний, біологічний, радіологічний або ядерний об'єкт потрібна спеціальна реакція, щоб захистити населення та перші служби реагування від зараження та пом'якшити потенційний викид небезпечних матеріалів. Спеціалізоване реагування передбачатиме конкретне планування на випадок надзвичайних ситуацій, а також спеціальне обладнання для виявлення, індивідуального захисту та дезактивації.

Після визначення основних структур і процесів антикризового управління стратегії CIP повинні забезпечити безперебійну роботу в разі потреби. Основні передумови для досягнення плавного та швидкого прийняття рішень розглядаються в розділі 5. У цьому ж розділі також обговорюються спільні державно-приватні заходи як ключові інструменти врегулювання криз..

Вміст 12
Протокол Європейського Союзу про реагування на надзвичайні ситуації правоохоронних органів (2019)

Прийнятий Радою Європейського Союзу в рамках Європейського Союзу «Проект скоординованої реакції на масштабні транскордонні інциденти та кризи в сфері кібербезпеки», Протокол 2019 року допомагає правоохоронним органам Європейського Союзу негайно реагувати на великі транскордонні кібератаки шляхом швидкої оцінки. , безпечний і своєчасний обмін важливою інформацією та координація міжнародних аспектів їхніх розслідувань.

Поштовхом для розробки Протоколу частково стали так звані кібератаки «WannaCry» і «NotPetya» 2017 року, які були безпрецедентними за масштабом і підкреслили, наскільки підходи, орієнтовані на інциденти, і реагування були неадекватною відповіддю на кіберзлочинців, що швидко розвиваються образи дії.

Доповнюючи існуючі механізми врегулювання кризових ситуацій Європейського Союзу, Протокол повною мірою використовує ресурси Європолу, зокрема, призначаючи центральну роль його Європейському центру боротьби з кіберзлочинністю (відомому як «EC3»). Оскільки його сфера застосування обмежена подіями кібербезпеки зловмисного та підозрюваного кримінального характеру - за винятком криз, спричинених стихійними лихами, людськими помилками чи збоями системи - Протокол передбачає фундаментальне завдання для тих, хто першими реагує, щодо збереження електронних доказів, знайдених в уражених IT-системах, з метою підтримки будь-якого подальшого кримінального розслідування чи судового розгляду.

Джерело: www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-

ВИВЧЕННЯ ПРОБЛЕМИ 19
Секторальні та міжгалузеві системи управління кризою: приклади країн

Спеціальні нормативні рамки KI для сектора телекомунікацій часто зустрічаються в секторі телекомунікацій. У Нідерландах, наприклад, Національний телекомунікаційний форум безперервності (NCO-T) *спрямований на забезпечення того, щоб оператор міг надавати важливі телекомунікаційні послуги за виняткових обставин. До складу* NCO-T *входять призначені оператори та Генеральний директорат з енергетики, телекомунікацій та ринків Міністерства економіки.*

У Франції план Piranet *визначає структуру управління кризою та процеси, за допомогою яких держава вживає необхідних заходів у конкретному випадку великої кризи IKT. План* Piranet *є доповненням до плану* Vigipirate. *Він розробляється Національним агентством з безпеки інформаційних систем* (ANSSI) *і Генеральним секретаріатом оборони та національної безпеки* (SGDSN) *і може бути ініційований прем'єр-міністро.*

Інші сектори KI можуть встановлювати еквівалентні домовленості на основі законодавчої бази, прийнятої регуляторними органами для окремих галузей. Як зазначає Інститут Маккензі, наприклад, після атак 11 вересня 2001 року «Нью-Йоркська фондова біржа – постійна потенційна мішень терористичних атак – змогла продовжити свої торговельні операції, оскільки вона вже створила альтернативний торговий майданчик. за межами Нью-Йорка, як і інші фінансові установи з того часу, щоб відтворити свої бізнес-операції за межами своїх муніципальних районів у разі катастроф, спричинених тероризмом».[51]

Навпаки, прикладом міжгалузевої нормативної бази є Кризовий акт Естонії, розділ IV *якого стосується організації безперервної роботи життєво важливих служб. Закон визначає ролі та обов'язки міністерств, місцевих і національних агенцій з управління кризами, а також операторів KI, необхідних для гарантування безперервного надання* 41 *критично важливої послуги.*

Європейська комісія підтримує веб-сайт із детальними оглядами національних систем боротьби зі стихійними лихами, що діють у 24 європейських країнах.

Джерело: https://itlaw.fandom.com/wiki/National_Continuity_Forum_Telecommunications; www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/; www.riigiteataja.ee/en/eli/525062014011/consolide; and https://ec.europa.eu/echo/what/civil-protection/national-disaster-management-system_en

[51] Джошуа Сінай, «Нові тенденції тероризму, спрямованого проти бізнес-сектору», Інститут Маккензі, 2016 р. Доступно за адресою https://mackenzieinstitute.com/2016/05/new-trends-in-terrorisms-targeting-of-the-business-sector/.

ВИВЧЕННЯ ПРОБЛЕМИ 20
Структура управління антикризовим управлінням: Нова Зеландія

У Новій Зеландії основним документом, який визначає всеохоплюючу структуру управління, що враховує всі небезпеки, для управління потенційними кризами, що розвиваються або фактичними (включаючи, але не обмежуючись, ті, що впливають на KI), є Посібник із системи національної безпеки. Критерії для спрацьовування системи національної безпеки поділяються на дві великі категорії. Вони стосуються або характеристик ризиків, або способу управління ризиками.

Характеристики ризику

- Незвичайні особливості масштабу, природи, інфтенстивності або можливих наслідків
- Виклики для суверітету або загальнонаціонального закону та порядку
- Численні або взаємопов'язані проблеми, які, разом узяті, становлять національний чи загальносистемний ризик
- Високий ступінь невизначеності або складності, так що лише центральний уряд має можливості впоратись з ними
- Взаємозалежні проблеми з потенціалом каскадних ефектів або ескалації

Вимоги до управління

- Вимоги до відповіді є надзвичайно вимогливими до ресурсів.
- Неоднозначність щодо того, хто має лідерство в управлінні ризиком, або існують суперечливі точки зору щодо рішень.
- Початкова відповідь є невідповідною або недостатньою з національної точки зору.
- Є міжвідомчі наслідки.
- Є можливість для уряду зробити свій внесок у створення умов, які посилять загальну національну безпеку.

Для будь-якого ризику для національної безпеки (або основного елемента такого ризику) визначається провідне агентство. Ці агенції уповноважені (чи чітко через законодавство, чи через їхній спеціальний досвід) керувати надзвичайними ситуаціями, що виникають із переліку конкретних небезпек.

Кризове управління в Новій Зеландії використовує функції кількох різних органів, у тому числі:

- *Групи спостереження:* вони покликані отримати ясність ситуації в тому, що часто є хаотичним середовищем, і відповідають за забезпечення наявності систем для забезпечення ефективного управління складними проблемами. Групи спостереження зазвичай складаються з вищих посадових осіб, здатних виділяти ресурси та погоджувати дії від імені своєї організації. Точний склад спостережних груп залежить від характеру події та включає агентства, які відіграють роль у реагуванні на поточну проблему. Це може включати органи, які зазвичай не вважають себе органами «національної безпеки» та не мають великого досвіду роботи в структурах системи національної безпеки.
- *Офіційний комітет з координації внутрішньої та зовнішньої безпеки:* цей орган, відомий як ODESC, забезпечує стратегічне керівництво, підтримує головне агентство та має зв'язки з політичним рівнем, зокрема консультує Комітет з національної безпеки Кабінету міністрів.
- *Робочі або спеціалізовані групи:* вони створюються, коли для професії чи дисципліни бажано визначити та представити консолідовану точку зору або конкретну пораду групі спостереження або ODESC. Приклади включають Урядову юридичну мережу, Економічну консультативну групу, Наукову мережу та Розвідувальну спільноту.
- *Національний центр управління кризовими ситуаціями:* забезпечує безпечне централізоване об'єкт для виконання різноманітних координаційних завдань, таких як керівництво операціями реагування, планування та підтримка; збір, управління та обмін інформацією; і зв'язок між оперативним реагуванням і національною стратегічною реакцією.
- *Червоне об'єднання:* Червоне об'єднання передбачає піддавання плану, ідей або припущень ретельному аналізу та перевірці з метою підвищення достовірності та якості остаточного плану. Міжвідомчі червоні групи можуть бути створені на всіх етапах кризи - і, власне, проекту - і можуть працювати паралельно з реагуванням. Під час національної кризи червона команда допомагає по-новому поглянути на підхід, який використовується для управління загрозою.

У рамках ширшої програми оновлення національної системи управління надзвичайними ситуаціями Нова Зеландія перебуває в процесі обговорення можливих змін для подальшого забезпечення стійкості інфраструктури. Дискусія розгортається навколо кількох тем, зокрема:

- *Визначення мінімальних рівнів обслуговування:* вимоги щодо визначення мінімальних рівнів обслуговування для критичної інфраструктури у випадку надзвичайної ситуації слід уточнити та посилити. Це включає вимоги до постачальників інфраструктури щодо розкриття інформації про готовність та очікуваний рівень обслуговування. Проактивне розкриття цієї інформації сприятиме прозорості та допоможе уряду, окремим особам і організаціям зрозуміти ризики, з якими вони стикаються, підготуватися та прийняти рішення про те, як найкраще керувати цими ризиками.

ВИВЧЕННЯ ПРОБЛЕМИ 20 (Продовження)

- *Скоординований підхід до управління ризиками:* для забезпечення скоординованого підходу до управління ризиками в критичній інфраструктурі країни необхідне постійне збільшення ресурсів. Провідним галузевим агентствам потрібні більш чіткі ролі для координації заходів щодо стійкості всередині та між секторами критичної інфраструктури. Це відображає взаємозалежність мереж інфраструктури. Ці зміни потрібні, щоб уточнити очікування щодо стійкості критичної інфраструктури, а також ролі та ресурси різних сторін, які беруть участь у створенні цієї інфраструктури.

Джерело: https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security/new-zealands-national-security; https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf; and www.tewaihanga.govt.nz/assets/Uploads/211012-Draft-New-Zealand-Infrastructure-Strategy.pdf

ВИВЧЕННЯ ПРОБЛЕМИ 21
Нові реагування на кіберінциденти в США: Закон про звітність про кіберінциденти для КІ 2022 року

When cyber incidents occur, the Department of Homeland Security provides assistance to potentially affected entities, analyses the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response. The Department works in close coordination with other agencies with complementary cyber missions, and also private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

У цьому контексті 15 *березня* 2022 *року було підписано Закон про звітність про кіберінциденти для критичної інфраструктури. Закон накладає на власників і операторів критичної інфраструктури два нових зобов'язання звітності*:

- Зобов'язання повідомляти CISA про певні кіберінциденти протягом 72 годин з моменту, коли організація «обґрунтовано вважає», що такий інцидент стався
- Зобов'язання повідомляти про платежі програм-вимагачів протягом 24 годин

По суті, Закон засновує CISA як центральне федеральне агентство, відповідальне за кіберзвітність для компаній, що працюють у секторі критичної інфраструктури, просування майбутнього процесу створення правил і координацію з іншими агентствами щодо обміну інформацією та нових ініціатив. Після повідомлення про інцидент, зокрема, суб'єкти, на які поширюється дія, зобов'язані подавати оновлення, коли «стане доступною значна нова або інша інформація», доки суб'єкт, на який поширюється дія, не повідомить CISA про те, що інцидент було повністю пом'якшено та вирішено..

Закон також вимагає від CISA *агрегувати, аналізувати та обмінюватися інформацією, отриманою з наданих звітів, щоб надавати державним установам, Конгресу, компаніям і громадськості оцінку ландшафту кіберзагроз, що постійно змінюється. При обміні інформацією з нефедеральними суб'єктами та громадськістю* CISA *зобов'язана анонімізувати організації-жертви, які подали звіти.*

З огляду на вимоги Закону, очікується, що суб'єкти, які потенційно постраждають від цього, визначать, чи потрібні зміни до їхніх кіберпрограм; перевірити свою внутрішню політику та процедури відповідно до вимог Закону; а також розглянути та підготуватися до дублюючих зобов'язань щодо розкриття інформації відповідно до державного, федерального та міжнародного законодавства.

Джерело: www.cisa.gov/cyber-incident-response and www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/

Інструмент 19

Інциденти кібербезпеки та реагування на вразливі місця – CISA: США

www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

Посібники призначені для того, щоб надати федеральним цивільним агенціям Сполучених Штатів оперативні процедури для планування та проведення заходів з реагування на інциденти кібербезпеки та вразливості. Вони застосовуються до інцидентів, пов'язаних із підтвердженою зловмисною кіберактивністю та щодо яких було оголошено серйозний інцидент або ще не обґрунтовано виключено. Деякі приклади включають інциденти, пов'язані з боковим переміщенням, доступом облікових даних або викраденням даних; мережеві вторгнення за участю більш ніж одного користувача або системи; або

2.7 Забезпечення фінансової стійкості та постійної актуальності стратегій

Стратегії CIP повинні закласти основу для, по-перше, забезпечення фінансової життєздатності загальних зусиль CIP; і, по-друге, встановлення, перегляд і моніторинг механізмів як частини процесів управління ризиками для оновлення існуючих списків KI та, якщо необхідно, ідентифікаційних критеріїв, додавання нових критичних секторів та інших заходів. Інституційні рамки та процеси, що лежать в основі стратегій CIP, також повинні підлягати регулярній перевірці, щоб переконатися в їх постійній актуальності в умовах зміни ландшафту загроз, уроків, отриманих з минулих криз, та інших факторів.

2.7.1 Фінансова стійкість

Хоча оператори KI несуть основну відповідальність за забезпечення захисту та стійкості критично важливих активів і процесів під їх контролем, посилення заходів фізичного та кіберзахисту часто вимагає виділення значних обсягів ресурсів. Досягнення стійкості KI може бути дорогим завданням. У такому контексті стратегії CIP повинні гарантувати, що інвестиції в забезпечення оптимального рівня захисту KI є фінансово стійкими. На практиці держави повинні знайти збалансовані та життєздатні домовленості про розподіл витрат між власниками та операторами KI, державними установами та страховими компаніями.

Важливим інструментом заохочення залучення власників і операторів KI є створення фінансових стимулів. Вони варіюються від субсидій до податкових пільг і позик. Стимули стають ще більш важливими під час економічної кризи, коли оператори можуть природно схилятися до витрачання ресурсів на короткострокові цілі зростання, а не на довгострокові цілі безпеки.

Потреба в державному втручанні у формі фінансової підтримки також може виникнути у разі руйнівних подій, які впливають на KI. Згідно з дослідженням, проведеним Міжнародним банком реконструкції та розвитку, «економічні та соціальні наслідки збоїв у роботі критичної інфраструктури пов'язані насамперед із втратою послуг, які вони надають, а не з вартості фізичного пошкодження самих активів. Наприклад, прямі збитки від стихійних лих для виробництва електроенергії та транспортної інфраструктури оцінюються в 18 мільярдів доларів США на рік у країнах з низьким і середнім рівнем доходу в усьому світі..''[52]

Стратегії CIP також можуть враховувати роль механізмів страхування, зокрема, з метою підтримки відновлювальних заходів, необхідних для реконструкції серйозно пошкоджених активів і відновлення перерваних послуг. Обговорення схем страхування KI почалося лише після подій 11 вересня 2001 року. До цього ризик тероризму зазвичай включався в стандартні страхові поліси без сплати будь-яких вищих премій. Після тих подій та інших надзвичайно руйнівних терористичних актів, таких як ті, що відбулися в Мадриді 11 березня 2004 року, сприйняття радикально змінилося через безпрецедентні суми компенсацій, які повинні були виплатити страхові компанії. Як було зазначено, «аналіз тероризму як частини проблеми «захисту критичної інфраструктури» показує, що тероризм зараз є визнаним джерелом гострих ризиків, тих, які є найближчими до зовнішньої межі страхування»[53]. Як чиста довіра щодо ринкових механізмів не було задовільним, уряди мали визначити характер і ступінь своєї фінансової участі в діях з відновлення KI. Сьогодні «створення та впровадження адекватного фінансового покриття для таких подій все частіше стає предметом національного розгляду, що виходить за рамки лише страхової галузі».[54]

---

[52] Світовий банк, Фінансовий захист послуг критичної інфраструктури, Вашингтон, округ Колумбія, 2021 р. Доступно за адресою https://www.financialprotectionforum.org/publication/ financial-protection-of-critical-infrastructure-services.

[53] Ерванн Мішель-Кер'ян, Фінансовий захист критичної інфраструктури: невизначеність, можливість страхування та ризик тероризму, Institut Veolia Environnement, Париж, 2018 р., доступно за адресою http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1268&rep=rep1&type=pdf.

[54] Там же

ВИВЧЕННЯ ПРОБЛЕМИ 22
Стимули та механізми фінансування стійкості KI: Японія, Швеція та США

Японія

Японія активізувала зусилля, щоб переконати бізнеси в тому, що приватні дії, спрямовані на посилення кібербезпеки, слід розглядати не як витрати, а як інвестиції для просування продуктів і послуг компаній і підвищення конкурентоспроможності. У цьому контексті уряд створив механізм винагороди компаній (через фінансові виплати), які надають пріоритет кіберпитанням. Крім того, він спонсорує програми для заохочення професійного розвитку працівників, які володіють навичками промислової кібербезпеки.

Швеція

Шведська стратегія CIP *визнає, що її реалізація вимагає підвищеної потреби в ресурсах, як людських, так і фінансових. Згідно з Указом про готовність до надзвичайних ситуацій та підвищену тривогу від* 2006 *року, органи влади можуть подати заявку на отримання коштів із розподілу коштів на готовність до надзвичайних ситуацій. Інші організації можуть опосередковано отримати вигоду від цього механізму фінансування, співпрацюючи в проектах з органами влади, визначеними в постанові.*

США

Завдяки програмі безпеки та стійкості Національного плану захисту інфраструктури (іменованого «NIPP»), CISA у партнерстві з Національним інститутом безпеки рідного міста фінансує інноваційні ідеї, які можуть надати технології та інструменти спільноті критичної інфраструктури. Проекти, що фінансуються в рамках NIPP Challenge, мають не лише мати відчутні короткострокові результати, щоб їх можна було швидко розробити та впровадити, але й бути фінансово, практично та матеріально стійкими в довгостроковій перспективі, щоб вони могли підвищити безпеку і стійкість критичної інфраструктури в багатьох секторах на довгі роки. Проекти оцінюються незалежною комісією Національного інституту безпеки рідного міста за низкою критеріїв, які також враховують їх життєздатність і очікуваний вплив.

Джерело: www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/; www.msb.se/RibData/Filer/pdf/27412.pdf; www.cisa.gov/nipp-security-and-resilience-challenge

ВИВЧЕННЯ ПРОБЛЕМИ 23

Схеми страхування стійкості КІ проти терористичних актів: Франція, Іспанія, Великобританія та США

Франція

З 2002 року орган, відомий як Gestion de l'Assurance et de la Réassurance des Risques d'Attentats et Actes de Terrorisme (Управління страхуванням і перестрахуванням ризиків нападів і терористичних актів, скорочено «GAREAT»), є некомерційна структура, що складається зі страхових компаній. GAREAT управляє перестрахуванням ризиків терористичних актів, які завдають шкоди у Франції (незалежно від країни, в якій скоєно терористичний акт). GAREAT складається з двох розділів: розділу «Великі ризики», який включає ризики, страхова сума яких становить 20 мільйонів євро або більше, і розділу «Малі та середні ризики», який керує ризиками зі страховими сумами менше 20 мільйонів євро. GAREAT спирається на принцип взаємності, відповідно до якого всі учасники несуть солідарну відповідальність з іншими в рамках одного розділу. Держава надає необмежену кількість програм GAREAT через Caisse Centrale de Réassurance.

Іспанія

Consorcio de Compensación de Seguros (Консорціум страхових компенсацій) надає компенсацію за шкоду, заподіяну людям і майну внаслідок так званих «надзвичайних ризиків». Щоб мати право на компенсацію від Consorcio, необхідно оформити страховий поліс у певних конкретних філіях. Спеціальне покриття Consorcio надається автоматично, якщо пошкодження є результатом терористичного акту. Консорціо є громадською організацією при Міністерстві економіки, промисловості та конкурентоспроможності..

Великобританія

Система, що діє у Сполученому Королівстві, є державно-приватним партнерством під назвою «Pool Re». Більшість страховиків, що надають страхування комерційної власності та непрямих збитків у Сполученому Королівстві, є членами Pool Re і погодилися запропонувати страхування від тероризму своїм клієнтам. Очікується, що будь-які власники полісів, які взяли таке покриття та зазнали збитків у результаті шкоди внаслідок терористичного акту, зв'яжуться зі своїм страховиком, який організує розгляд претензії відповідно до звичайних процедур. Pool Re має домовленості з усіма своїми членами про відшкодування їм вартості позовів, виплачених ними під прикриттям тероризму, яке вони надають. Для цього страховики сплачують премії Pool Re. Уряд зобов'язався підтримати Pool Re, якщо в останньої буде недостатньо коштів для оплати законної вимоги.

США

Система, що діє в США, ґрунтується на домовленості про розподіл ризиків між федеральним урядом, страхувальником і страховиком. Відповідно до Закону про страхування ризиків тероризму від 2002 року страховики зобов'язані пропонувати своїм клієнтам страхування від тероризму (хоча страховики можуть самостійно встановлювати ціну покриття). У свою чергу, клієнти не зобов'язані оформляти покриття. Важливо те, що відповідно до закону напад має бути сертифікований як «терористичний акт» міністром фінансів. Визначення вимагає, щоб напад був здійснений іноземними інтересами.

20 грудня 2019 року Президент підписав закон про переоформлення Програми страхування ризиків тероризму, який продовжив дію Програми до 31 грудня 2027 року.

Джерело: www.gareat.com; www.consorseguros.es/web/inicio; www.poolre.co.uk/ and https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program.

Інструмент 20

Фінансовий захист послуг КІ – Міжнародний банк реконструкції та розвитку

www.financialprotectionforum.org/publication/financial-protection-of-critical-infrastructure-services

Цей технічний звіт, підготовлений Міжнародним банком реконструкції та розвитку у 2021 році відповідно до порядку денного фінансування ризиків стихійних лих і страхування на зустрічі міністрів фінансів Азіатсько-Тихоокеанського економічного співробітництва у 2020 році, зосереджується на захисті послуг критичної інфраструктури, а не на базових активах. Хоча він в основному стосується збоїв, пов'язаних із стихійними лихами, його також можна використовувати як план для подолання криз, спричинених людськими потрясіннями, такими як тероризм і кібератаки. У звіті окреслено контури операційної основи для фінансового захисту критичної інфраструктури, яка поєднує три взаємопов'язані компоненти:

- *Фінансовий захист фізичних активів. Цей компонент передбачає наявність фінансів і планів відновлення чи реконструкції критично важливих активів після катастрофи. Захист може включати, наприклад, страхування державних активів або бюджетні механізми, такі як фонди на випадок стихійних лих.*
- *Системи, що реагують на удари, поєднують фінансову та операційну готовність для забезпечення швидкого відновлення критичних послуг. Відповідно до цієї складової, готовність передбачає наявність планів, фінансування та систем для швидкої мобілізації дій у разі шоку, таким чином або забезпечуючи*

Інструмент 21

Економічні та фінансові стимули: інструментарій політики щодо управління стійкістю критичної інфраструктури – OECD

www.oecd-ilibrary.org/governance/good-governance-for-critical-infrastructure-resilience_fc4124df-en

Набір політичних інструментів OECD (див. Інструмент 2) містить конкретні рекомендації, ключові політичні питання та порівняльні показники щодо того, як економічні та фінансові стимули можна використовувати для посилення стійкості операторів КІ. Зокрема, «уряди повинні визначити поєднання політичних інструментів для стимулювання інвестицій операторів у стійкість і досягнення спільних цілей щодо стійкості. Такі заходи повинні стосуватися всього життєвого циклу інфраструктури від планування до експлуатації, технічного обслуговування та оновлення або модернізації. Урядові заходи щодо стабілізації стійкості повинні ґрунтуватися на аналізі витрат і вигод з урахуванням наслідків для вартості послуг.

Чому це важливо?

Уряди можуть вибирати з різноманітних політичних інструментів і механізмів для просування реалізації цілей стійкості, від добровільних рамок і механізмів стимулювання до регуляторних або правових інструментів. Оператори дуже зацікавлені в підтримці безперервності своїх послуг і своєї репутації шляхом інвестування в стійкість. Однак інвестиції в стійкість часто спричиняють початкові витрати, навіть якщо вони повинні бути компенсовані з точки зору більшої надійності обслуговування та стійкості до потрясінь. Питання в тому, як знайти правильний баланс. Додаткові вимоги, які встановлюють уряди для посилення стійкості, можуть призвести до додаткових витрат, які в кінцевому рахунку несуть клієнти, громадяни та підприємства. Важливо пристосувати інструменти державної політики, щоб забезпечити ефективні стимули для операторів інвестувати в стійкість, одночасно керуючи фінансовими наслідками.

Регуляторний підхід має сильні сторони в тому, що він передбачає чіткі та вимірювані зобов'язання, наприклад, встановлення вимог до надійності або вимогу до планів безперервності бізнесу, механізмів страхування та мінімальних стандартів безпеки. Однак, якщо він буде занадто жорстким, це також може виявитися дорогим, не встигати за швидким технологічним розвитком і створювати проблеми з дотриманням вимог. Запровадження компенсаційної схеми для клієнтів, чиї послуги були порушені, або інші види заходів можуть запропонувати більш ефективний спосіб стабілізації інвестицій у стійкість, зокрема, у державно-приватному партнерстві. Цей підхід також надає операторам можливість вибору способів підвищення їх стійкості. Добровільні рамки, такі як розробка керівних принципів стійкості, заходи з підвищення обізнаності або обмін передовим досвідом, часто є кращим варіантом, оскільки вони сприяють залученню зацікавлених сторін, але вони також мають значні невизначеності. Знайти баланс між державною фінансовою підтримкою та приватними інвестиціями для таких заходів стійкості можна досягти за допомогою методів аналізу витрат і вигод, які визначають пріоритетність найбільш ефективних способів розподілу витрат на загальні колективні зусилля для досягнення спільних цілей стійкості.

Ключові питання політики:

- Чи визначені стійкості для підвищення рівня захисту, надійності, резервування або адаптивності протягом життєвого циклу критичної інфраструктури?
- Чи існують мінімальні стандарти безпеки, які гарантують, що оператори інвестують у стійкість?
- Чи відіграють галузеві регулятори певну роль у стабілізації стійкості критичної інфраструктури?
- Чи використовується аналіз витрат і вигод для визначення пріоритетності заходів стійкості, оцінки їх впливу на вартість послуг і пошуку домовленостей про розподіл витрат?

Еталонні показники:

- Плани впровадження для забезпечення стійкості критичної інфраструктури
- Правила інфраструктури з положеннями щодо стійкості
- Оцінка витрат і вигод від заходів стійкості

2.7.2 Перегляд і моніторинг механізмів

Інфраструктура, яка визначена як така, що надає критичні послуги в певний момент часу, може

більше не виконувати ці функції на пізнішому етапі. І навпаки, зміни в економіці та очікуваннях суспільства можуть зробити незамінними певні активи та процеси, які раніше не були пріоритетними. Наприклад, нинішня фаза глобального енергетичного переходу може зробити постачання певних видів палива менш критичними, водночас збільшуючи стратегічну цінність інших.

Крім того, характер та інтенсивність загроз, що впливають на КІ, змінюються з часом. Наприклад, деякі терористичні групи можуть становити меншу загрозу в певних країнах, продовжуючи чинити тиск в інших країнах. Наприкінці 2017 року ДАІШ втратив контроль над приблизно 95 відсотками території, яку він контролював у 2014 році. КІ, розташовані в цих районах, стали менш схильні до типу загроз з боку ІДІЛ, хоча потенційно були з іншими джерелами та видами загроз. Навпаки, геополітичні потрясіння, що відбуваються на Близькому Сході – супроводжувані поверненням кількох бойовиків ДАІШ та іноземних бойовиків-терористів до країн походження – викликають дедалі більше занепокоєння розвідувальних служб щодо підвищеного ризику терористичних атак, націлених на КІ в тих країнах.

Стратегії CIP – і пов'язані з ними інституційні рамки та процеси – також можуть стати неадекватними у світлі досвіду, накопиченого країнами в реальному врегулюванні криз. Певні процеси, закріплені в стратегічних документах і планах дій, можуть виявити свою неадекватність під час перевірки цих процесів на місцях.

З огляду на це, стратегії CIP повинні передбачати механізми, які через регулярні проміжки часу спрямовані на:

- Оновити часто великі списки національних КІ
- Визначити, чи потрібно додати або видалити певні сектори та підсектори з тих, що вважаються «критичними»
- Переконатися, що всі зацікавлені сторони беруть участь у регулярній переоцінці загроз, що впливають на КІ та пов'язані з ними вразливості
- Приймати підхід на основі отриманих уроків до точного налаштування стратегічних цілей, рамок, механізмів координації та інших процесів

ВИВЧЕННЯ ПРОБЛЕМИ 24

Перегляд списків критичних активів і стратегій: Канада та Іспанія

Канада

Канадська національна стратегія щодо критичної інфраструктури вимагає, щоб «федеральні, провінційні та територіальні уряди [працювали разом для моніторингу реалізації Стратегії та підтримки оцінки програм і заходів, спрямованих на підвищення стійкості критичної інфраструктури в Канаді».

Іспанія

Відповідно до Королівського указу 704/2011, який встановлює правила захисту критичної інфраструктури, «у разі значних змін, що впливають на інфраструктури, перелічені [в Національному каталозі], коли ці зміни є актуальними для цілей, передбачених цими правилами, Компетентні оператори за допомогою засобів, наданих у їх розпорядження Міністерством внутрішніх справ, нададуть нову інформацію Національному центру захисту інфраструктури та кібербезпеки (CNPIC), який підтвердить її до включення до Каталог. У будь-якому випадку оновлення наявної інформації має відбуватися щорічно» (ст. 5.5)

Джерело: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf and www.boe.es/buscar/act.php?id=BOE-A-2011-8849.

3. Встановлення відповідальності

Резолюція Ради БЕзпеки 2341 (2017)

Рада Безпеки [...]

...

Нагадує про своє рішення в резолюції 1373 (2001) про те, що всі держави визнають терористичні акти серйозними кримінальними злочинами у внутрішньому законодавстві та

Стратегії CIP повинні враховувати двосторонній режим відповідальності для боротьби з поведінкою, яка ставить під загрозу безпеку KI:

- Режим кримінальної відповідальності для осіб, які здійснюють напади (або погрожують чи планують такі напади) на KI (пункти 3.1–3.3)
- Режим санкцій для фізичних та юридичних осіб із законодавчими та нормативними обов'язками щодо захисту та безпеки KI, які належать до їх повноважень (розділ 3.4)

3.1 Вимоги щодо криміналізації в універсальній правовій базі боротьби з тероризмом

Відмінною рисою резолюції 2341 (2017) є заклик до держав-членів спеціально криміналізувати дії проти KI. Роблячи це, Рада Безпеки спирається на низку раніше прийнятих документів, які встановлюють загальні вимоги до держав-членів щодо притягнення до відповідальності осіб, які вчинили терористичні акти, і їх сприльників. Епохальним документом у цій сфері є резолюція 1373 (2001). Прийнятий незабаром після подій 11 вересня 2001 року, цей документ передбачає, серед інших заходів, комплексний набір вимог кримінального правосуддя, таких як зобов'язання щодо:

- Криміналізувати надання або збирання коштів у зв'язку з вчиненням терористичних актів
- Не дозволити безпечного раю всім тим, хто планує, підтримує або вчиняє терористичні акти, і

притягнути їх до відповідальності

- Визначити терористичні акти тяжкими кримінальними злочинами у національному законодавстві

На додаток до резолюцій Ради Безпеки, серія договорів, що стосуються запобігання та припинення міжнародного тероризму, встановлює вимоги щодо криміналізації у сфері КІ. Через відсутність згоди щодо сфери застосування всеосяжного договору, який охоплює всі аспекти та прояви міжнародного тероризму, ці окремі документи ухвалювалися протягом приблизно п'ятдесяти років. Поступовий, галузевий і прагматичний підхід, якого дотримується міжнародне співтовариство, призвів до прийняття конвенцій і протоколів, що стосуються таких конкретних сфер, як морська та авіаційна безпека, фінансування ядерної зброї та тероризму та інші.

У тексті вищезазначених договорів, які разом складають те, що нижче називається «універсальною правовою базою проти тероризму», не використовується вираз «критична інфраструктура». Проте, як показано в таблиці 4, більшість із них включають положення, що створюють правопорушення, безпосередньо спрямовані на поведінку, спрямовану на знищення або втручання у функціонування КІ. У тій мірі, в якій держави-члени є сторонами цих договорів, вони зобов'язані включити їх положення у своє національне законодавство. Це передбачає, зокрема, визнання поведінки, визначеної в цих документах, кримінальним злочином у національному законодавстві[55]

Таблиця 4
Злочини, пов'язані з КІ, відповідно до універсальної правової бази проти тероризму

Сектор	Конвенції та протоколи	Головне правопорушення

Авіація	Токійська конвенція (1963): Конвенція про правопорушення та деякі інші дії, вчинені на борту повітряних суден, зі змінами, внесеними Монреальським протоколом	Вимагає від наступних Договірних держав встановити юрисдикцію для покарання за правопорушення, скоєні на борту повітряного судна: • Шатат реєстрації повітряного судна • Штат стану приземлення, коли повітряне судно, на борту якого скоєно правопорушення, приземляться на його території, а ймовірний порушник все ще перебуває на борту • Штат експлуатанта, якщо правопорушення вчинено вчинено на борту повітряного судна, зданого в оренду без екіпажу орендарю, основне місце діяльності якого або, якщо орендар не має такого місця бізнесу, постійне місце проживання якого знаходиться в цій державі
	Гаазька конвенція (1970 р.): Конвенція про боротьбу з незаконним захопленням повітряних суден і додатковий Пекінський протокол до неї (2010 р.)	Захоплення повітряного судна, що знаходиться в експлуатації, або здійснення контролю над ним силою чи загрозою її застосування, або шляхом примусу, або будь-якою іншою формою залякування, або будь-якими технологічними засобами
	Монреальська конвенція (1971): Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації, доповнена Монреальським протоколом (1988): Протокол про боротьбу з незаконними актами насильства в аеропортах, що обслуговують міжнародну цивільну авіацію; та Пекінська конвенція (2010): Конвенція про боротьбу з незаконними актами, що стосуються міжнародної цивільної авіації	• Здійснення акту насильства проти особи на борту літака під час польоту, якщо цей акт може загрожувати безпеці цього літака • Знищення повітряного судна, що знаходиться в експлуатації, або заподіяння пошкоджень такому літаку, що робить його нездатним до польоту або що може загрожувати його безпеці в польоті • Розміщення або встановлення на борту літака пристрою чи речовини, які можуть знищити цей літальний апарат або спричинити його пошкодження, що зробить його нездатним до польоту, чи спричинити його пошкодження, яке може загрожувати його безпеку в польоті • Руйнування або пошкодження аеронавігаційних засобів або втручання в їх роботу, якщо будь-яка така дія може загрожувати безпеці повітряного судна в польоті • Передача завідомо неправдивої інформації, що створює загрозу безпеці повітряного судна в польоті • Використання проти або на борту літака, що знаходиться в експлуатації, будь-якої біологічної, хімічної або ядерної зброї або вибухових, радіоактивних або подібних речовин у спосіб, який спричиняє або може спричинити смерть, серйозні тілесні ушкодження або серйозну шкоду майну чи навколишньому середовищу; • Руйнування або серйозне пошкодження об'єктів аеропорту, що обслуговує міжнародну цивільну авіацію, або повітряних суден, які не знаходяться в експлуатації, або порушення роботи аеропорту, якщо такий акт ставить під загрозу або може поставити під загрозу безпеку в цьому аеропорту

[55] Як передбачено резолюцією 1373 (2001), держави-члени, які ще не стали сторонами однієї чи кількох із вищезгаданих конвенцій і протоколів про боротьбу з тероризмом, закликаються зробити це якомога швидше..

Sector	Conventions and protocols	Main offences[a]
Морський	Конвенція 1988 р. про боротьбу з незаконними актами, спрямованими проти безпеки морського судноплавства	• Захоплення або контроль над судном за допомогою сили або погрози застосування сили чи будь-якої іншої форми залякування • Вчинення акту насильства проти особи на борту судна, якщо цей акт може загрожувати безпечному судноплавству • Знищення судна або завдання шкоди судну або його вантажу, що може загрожувати безпеці судноплавства • Розміщення або спричинення розміщення на судні будь-яким способом пристрою чи речовини, які можуть знищити це судно або завдати шкоди цьому судну чи його вантажу, що ставить під загрозу або може поставити під загрозу безпечне плавання цього судна • Руйнування або серйозне пошкодження морських навігаційних засобів або серйозне втручання в їх роботу, якщо будь-який такий акт може загрожувати безпеці плавання судна • Передача відомостей, які є завідомо неправдивими, що ставить під загрозу безпеку плавання судна Якщо метою дії є залякування населення або змусити уряд чи міжнародну організацію вчинити або утриматися від будь-яких дій: використання проти судна або на ньому або викиди з судна будь-якої вибухової речовини, радіоактивного матеріалу чи біологічного засобу, хімічної або ядерної зброї таким чином, що спричиняє або може спричинити смерть або серйозні травми чи пошкодження
	Протокол 2005 р. до Конвенції про боротьбу з незаконними актами, спрямованими проти безпеки морського судноплавства	
	Протокол 1988 року про боротьбу з незаконними актами, спрямованими проти безпеки стаціонарних платформ, розташованих на континентальному шельфі	• Захоплення стаціонарної платформи або здійснення контролю над нею за допомогою сили чи погрози застосування сили чи будь-якої іншої форми залякування • Вчинення акту насильства проти особи на борту стаціонарної платформи, якщо ця дія може загрожувати її безпеці • Руйнування стаціонарної платформи або її пошкодження, яке може загрожувати її безпеці • Розміщення або встановлення на стаціонарній платформі пристрою чи речовини, які можуть зруйнувати цю стаціонарну платформу або поставити під загрозу її безпеку. Коли мета дії полягає в тому, щоб залякати населення або змусити уряд чи міжнародну організацію вчинити будь-яку дію або утриматися від неї: використання проти стаціонарної платформи або на ній або викиди з неї будь-якої вибухової речовини, радіоактивного матеріальна або біологічна, хімічна чи ядерна зброя таким чином, що спричиняє або може спричинити смерть або серйозне поранення чи шкоду
	Протокол 2005 року до Протоколу про боротьбу з незаконними актами, спрямованими проти безпеки стаціонарних платформ, розташованих на континентальному шельфі	
Ядерний	2005 Міжнародна конвенція про боротьбу з актами ядерного тероризму та Поправка 2005 року до Конвенції про фізичний захист ядерного матеріалу	Використання або пошкодження ядерної установки, втручання в її роботу або вчинення будь-яких інших дій, спрямованих проти ядерної установки, у спосіб, що призводить до викиду або ризику викиду радіоактивного матеріалу, • З наміром заподіяти смерть або тяжкі тілесні ушкодження; або істотної шкоди майну чи навколишньому середовищу; • Знаючи, що дія може спричинити смерть чи серйозне ушкодження будь-якої особи або завдати суттєвої шкоди майну чи навколишньому середовищу через вплив радіації чи викид радіоактивних речовин, якщо дія не вчиняється відповідно до національного законодавства держави-учасниці. на території якого розташована ядерна установка; • Змусити фізичну чи юридичну особу, міжнародну організацію чи державу вчинити або утриматися від вчинення дії.
Дипломатичний персонал	1973 Конвенція про попередження та покарання злочинів проти осіб, які користуються міжнародним захистом	Здійснення насильницького нападу на службові приміщення, приватне житло чи транспортний засіб особи, яка користується міжнародним захистом, що може загрожувати її особистості чи свободі.
Державні установи, системи громадського транспорту	1997 Міжнародна конвенція про боротьбу з бомбовим тероризмом	Доставка, розміщення, скидання або підрив вибухового чи іншого смертоносного пристрою в або проти місця громадського користування, державного чи урядового об'єкта, системи громадського транспорту чи об'єкта інфраструктури з наміром спричинити масштабне руйнування такого місця, об'єкта або системи, де таке знищення призводить або може призвести до великих економічних втрат. Розміщення або надання коштів з метою або з усвідомленням того, що кошти будуть використані для вчинення акту тероризму (як визначено в самій Конвенції) або будь-якого іншого акту, викладеного в одному з універсальних інструментів проти тероризму
	1999 Міжнародна конвенція про боротьбу з фінансуванням тероризму	
Фінансування терористичних актів проти КІ	1999 Міжнародна конвенція про боротьбу з фінансуванням тероризму	Розміщення або надання коштів з метою або з усвідомленням того, що кошти будуть використані для вчинення акту тероризму або будь-якого іншого акту в 1 з універсальних інструментів проти тероризму

[a] Повний перелік вимог щодо криміналізації та точні формулювання, що використовуються в конвенціях, дивіться в їх офіційних текстах.

Окрім універсальної законодавчої бази проти тероризму, ряд регіональних інструментів боротьби з тероризмом встановлюють вимоги щодо криміналізації КІ, зокрема у сфері КІ. Новаторським інструментом у його галузі є Конвенція Ради Європи про кіберзлочинність 2001 року, яка вперше запровадила кримінальну поведінку, пов'язану з порушенням безпеки мережі (на додаток до встановлення повноважень і процедур, таких як пошук комп'ютерних мереж і перехоплення) . Нещодавно Європейський Союз прийняв директиву, спрямовану на гармонізацію кримінального законодавства держав-членів у сфері атак на інформаційні системи. Іншим прикладом є Конвенція Африканського Союзу про кібербезпеку та захист даних 2014 року

Вміст 13
Криміналізація атак на інформаційні системи: правові рамки ЄС та Африканського Союзу

- 2013 Директива Європейського Союзу про атаки на інформаційні системи

Ключовою метою Директиви Європейського Союзу 2013 року є встановлення мінімальних правил для визначення кримінальних правопорушень і відповідних санкцій. Директива передбачає кримінальне покарання принаймні за випадки, які не є малозначними. Держави-члени можуть визначати, що вважається незначною справою відповідно до їх національного законодавства та практики. Директива стосується, наприклад, створення так званих «ботнетів», іншими словами, акту встановлення віддаленого контролю над значною кількістю комп'ютерів шляхом зараження їх шкідливим програмним забезпеченням через цілеспрямовані кібератаки. Після створення інфікована мережа комп'ютерів, які утворюють ботнет, може бути активована без відома користувачів комп'ютера, щоб розпочати широкомасштабну кібератаку.

Директива визначає три обтяжуючі обставини, за які правопорушення, про які йде мова, мають каратися максимальним терміном позбавлення волі не менше п'яти років, а саме:

- Коли вони вчинені в рамках злочинної організації
- Коли вони завдають серйозної шкоди
- Коли вони вчинені проти інформаційної системи КІ

2014 Конвенція Африканського Союзу про кібербезпеку та захист даних

Прийнята в 2014 році Конвенція Африканського Союзу вимагає, щоб «кожна держава-учасниця ... ухвалювала такі законодавчі та/або регулятивні заходи, які вона вважає ефективними, вважаючи кримінальними злочинами дії, які впливають на конфіденційність, цілісність, доступність і збереження систем інформаційних і комунікаційних технологій. , даних, які вони обробляють, і базової мережевої інфраструктури» (ст. 25).

На додаток до встановлення злочинів, пов'язаних із прямими атаками на комп'ютерні системи, Конвенція приймає помітно превентивний підхід до скоєння кіберзлочинів. Відповідно до пункту 1 (h) статті 29, Сторони зобов'язуються «визнати кримінальним злочином незаконне виробництво, продаж, імпорт, володіння, розповсюдження, пропозицію, передачу чи надання доступу до комп'ютерного обладнання, програми або будь-якого пристрою чи даних. розроблені або спеціально пристосовані для вчинення правопорушень, або незаконно генерують або виробляють пароль, код доступу або подібні комп'ютеризовані дані, що дозволяють отримати доступ до частини чи всієї комп'ютерної системи».

3.1.1Криміналізація та міжнародна співпраця

Важливою причиною, чому держави-члени повинні криміналізувати дії, визначені в універсальній правовій базі проти тероризму, є сприяння міжнародній співпраці у кримінальних справах. Значні перешкоди для такої співпраці будуть усунені, якщо відповідні (а саме пов'язані з КІ) злочини будуть введені в кримінальне законодавство держав-учасниць. Важливо те, що вимога про те, що

екстрадиція та взаємна правова допомога можуть бути надані лише тоді, коли правопорушення, про яке йдеться, криміналізовано як у запитуваній, так і в запитуючій країні (відоме як принцип «подвійного визнання злочином») буде автоматично виконано, якщо обидві сторони сумлінно транспонують мову договору в їхні відповідні кримінальні статути.

У той же час, здатність окремих країн успішно переслідувати правопорушників часто залежатиме від ефективності існуючих міжнародних каналів співпраці правоохоронних органів, видачі втікачів та обміну доказами. Країни, які прагнуть максимізувати захист KI з точки зору кримінального правосуддя, повинні розглянути роль універсальної бази боротьби з тероризмом у забезпеченні правових основ для екстрадиції та взаємної правової допомоги, або на підтримку, або за відсутності двосторонніх чи регіональних угод з цією метою.

Незалежно від того, який канал співпраці використовується, держави-члени повинні забезпечити повну дотримання стандартів справедливого судового розгляду та належного процесуального права. Це стосується не лише внутрішніх проваджень, спрямованих на встановлення кримінальної відповідальності осіб, а й тих, які розпочинаються від імені інших країн для видачі втікачів або передачі доказів.

3.2 Національні підходи до встановлення кримінальної відповідальності за напади на КІ

Криміналізація дій, спрямованих на КІ, є важливою для досягнення трьох взаємопов'язаних цілей:

- Забезпечення належного рівня стримування шляхом застосування серйозних покарань до осіб, які вчинили терористичні акти проти КІ.
- Знищення злочинних і терористичних планів, спрямованих проти КІ, шляхом використання кримінального права як запобіжного засобу, враховуючи вимогу, викладену в резолюції 2341 (2017) для держав-членів щодо визнання кримінальними злочинами «планування, навчання та фінансування матеріально-технічне забезпечення» терористичних атак
- Створення правових основ та умов для безперебійного міжнародного співробітництва у сфері кримінального правосуддя з питань, пов'язаних з КІ

Як зазначено в розділі 3.1, національні органи влади визнають кримінальними злочинами дії, визначені в універсальних правових документах проти тероризму, сторонами яких вони є. Однак, оскільки ці інструменти охоплюють КІ лише частково, держави-члени також повинні визначити, до якої міри правопорушення, пов'язані з КІ, слід криміналізувати понад те, що суворо вимагається цими документами. Плануючи запровадження всеосяжного законодавства, пов'язаного з кримінальною діяльністю та тероризмом, держави-члени повинні пам'ятати, що не існує міжнародного визначення «критичної інфраструктури».

У загальних рисах можна передбачити три варіанти редакцій:

- Криміналізуйте поведінку, пов'язану з конкретними типами інфраструктури («підхід до конкретного сектора»)
- Криміналізуйте поведінку проти КІ незалежно від сектора або секторів, до яких належить

відповідна КІ («міжгалузевий підхід»)

- Покладайтеся на загальне кримінальне законодавство, яке застосовується до СІ, хоча воно не було розроблено для цілей захисту СІ («підхід, не пов'язаний із СІ»)

Варто зазначити, що вищезазначені підходи не виключають один одного, і на практиці країни часто приймають суміш трьох. Який би підхід (чи комбінацію підходів) не було обрано, кримінальні правопорушення мають бути сформульовані відповідно до принципу законності. Це вимагає, щоб кримінальна відповідальність і покарання ґрунтувалися на попередньому введенні в дію заборони, яка виражена з достатньою точністю та ясністю.

3.2.1 Секторальний підхід

Злочини, пов'язані з КІ, можуть бути спрямовані на конкретні критичні сектори, такі як ядерна, транспортна та інші галузі. Відповідна поведінка може бути криміналізована з або без передбачення конкретної терористичної мети як елементу злочину. Хоча резолюція 2341 (2017) закликає держави мати можливість встановлювати кримінальну відповідальність за терористичні атаки, вона, безперечно, не перешкоджає країнам розширювати сферу злочинів, про які йде мова, шляхом криміналізації поведінки, яка не пов'язана з терористичною метою. Дійсно, формулювання, що використовується в більшості універсальних правових інструментів проти тероризму, підтверджує цей результат. Наприклад, Конвенція про боротьбу з незаконним захопленням повітряних суден 1970 року вимагає, щоб сторони визначали як правопорушення акт захоплення управління повітряним судном (за допомогою сили чи погрози її застосування чи будь-якої іншої форми залякування) незалежно від конкретного наміру чи основи мотивації правопорушника.

Кілька прикладів галузевого законодавства можна знайти в країнах так званого «загального права», таких як Фіджійський закон про цивільну авіацію (Закон про безпеку) 1994 року, Закон Шрі-Ланки про боротьбу з вибухами терористів 1999 року та Сполучене Королівство про осіб, які користуються міжнародним захистом. Закон 1978 р. Часто, коли обирається галузевий підхід, відповідні правопорушення є частиною ширшої нормативної бази, яка також розроблена для детального регулювання галузевих операцій, ліцензійних вимог і процедур та інших подібних питань. Прикладом є Закон Японії про регулювання використання ядерних матеріалів, матеріалів для ядерного палива та реакторів..

Перевага цього підходу полягає в тому, що він дозволяє країнам точно налаштовувати свої вимоги щодо криміналізації відповідно до загроз, характерних для певних типів інфраструктури та секторів. Це також полегшує визначення штрафних санкцій, які більш точно відображають уявлення про рівень критичності певних активів і очікуваний вплив у разі збоїв. Головним недоліком цього підходу є те, що він обмежує охоплення кримінального права закритим списком секторів і активів, таким чином залишаючи інші без уваги та потребуючи окремих законодавчих заходів.

3.2.2 Міжгалузевий підхід

Деякі держави-члени приймають законодавство про кримінальну відповідальність за напади на КІ як такі, незалежно від секторів, до яких вони належать. Перевага цього підходу полягає в тому, що він забезпечує структуру для забезпечення охоплення всіх секторів КІ, включаючи ті, які потенційно можуть бути додані як критичні в майбутньому. Одним із можливих недоліків є недостатня точність, оскільки застосовне законодавство може встановлювати один набір санкцій, який неоднозначно застосовується в різних секторах. У таких випадках розробники політики можуть розглянути можливість – дотримуючись принципу законності – встановити ширший вікон покарань, дозволяючи суддям коригувати рівень санкцій відповідно до конкретних обставин кожної справи.

Міжгалузеві злочини можуть передбачати або не передбачати терористичний намір. Коли це відбувається, дії, вчинені проти КІ, прямо поміщаються в сферу дії законодавчої бази боротьби з тероризмом з усіма наслідками щодо спеціальних процедур, методів розслідування, компетентних органів і так далі. Найчастіше національні закони про боротьбу з тероризмом посилаються на «громадську інфраструктуру» або «необхідні послуги, об'єкти чи системи», якщо їх знищення або

втручання в їх функціонування призводить до великих економічних втрат, небезпеки для життя людей та інших подібних наслідків.[56]

Варто зазначити, що низка законів, які криміналізують напади на КІ як терористичні акти, надають винятки для дій, вчинених у контексті законного здійснення певних громадянських, політичних чи соціальних прав. Наприклад, Кримінальний кодекс Канади виключає з поняття «терористична діяльність» ті дії, які, незважаючи на те, що спричиняють «серйозне втручання або серйозний збій у роботі основної служби, об'єкта чи системи, незалежно від того, державні чи приватні», вчинені в результаті пропаганди , протест, незгода або припинення роботи, яка не має на меті призвести до поведінки чи шкоди, що визначається як терористична діяльність.[57]

[56] Наприклад, законодавство Кенії визначає «терористичний акт» як акт або загрозу вчинення дій, які, серед іншого, «втручаються в електронну систему, що призводить до порушення надання комунікаційних, фінансових, транспортних чи інших основних послуг [або] перешкоджає або порушує надання основних або екстрених послуг".

[57] Кримінальний кодекс, 83.01(1).

Вміст 14
КІ та Рамкове рішення Європейського Союзу про боротьбу з тероризмом

Згідно з Рамковим рішенням Європейського Союзу про боротьбу з тероризмом58 кілька видів нападів на КІ вважаються «терористичними злочинами», зокрема:

- *Масштабне руйнування урядового чи громадського об'єкта, транспортної системи, об'єкта інфраструктури, зокрема інформаційної системи, стаціонарної платформи, розташованої на континентальному шельфі, громадського місця чи приватної власності, що може загрожувати життю людей або призвести до великих економічних збитків*
- *Захоплення літаків, кораблів або інших засобів громадського чи вантажного транспорту*

ВИВЧЕННЯ ПРОБЛЕМИ 25
Міжгалузевий підхід до криміналізації: Канада

Кримінальне законодавство Канади визначає набір правопорушень, що включає поведінку, спрямовану на пошкодження, порушення та іншим чином втручання в «основну інфраструктуру», як це визначено в Законі про захист критичної інфраструктури 2020 року.:

Заборони

2. (1) *Жодна особа не має права без законного права, обґрунтування чи виправдання навмисно входити в будь-яку основну інфраструктуру.*

(2) *Жодна особа не має права без законного права, обґрунтування чи виправдання навмисно пошкоджувати чи руйнувати будь-яку важливу інфраструктуру.*

(3) *Жодна особа не має права без законного права, обґрунтування чи виправдання навмисно перешкоджати, переривати або втручатися в будівництво, технічне обслуговування, використання чи експлуатацію будь-якої основної інфраструктури таким чином, щоб зробити основну інфраструктуру небезпечною, марною, непрацездатною чи неефективний.*

(4) *Жодна особа не має права допомагати, консультувати чи спрямовувати іншу особу до вчинення правопорушення згідно з підпунктами (1), (2) або (3), незалежно від того, чи дійсно інша особа вчиняє правопорушення..*

(5) *Особа, яка проникає на будь-яку основну інфраструктуру, отримавши під неправдивим приводом дозвіл на вхід на основну інфраструктуру від власника або уповноваженого представника власника, вважається такою, що порушила пункт (1), якщо особа не мала законного право, обґрунтування чи виправдання входу в основну інфраструктуру..*

Правопорушення та покарання

3(1) *Особа, яка порушує розділ 2, є винною у вчиненні правопорушення та несе відповідальність*

(a) *у випадку фізичної особи,*

(i) *за перше правопорушення — до штрафу від 1000 доларів США до 10 000 доларів США або до позбавлення волі на строк не більше 6 місяців, або одночасно до штрафу та ув'язнення, і*

(ii) *за друге чи наступне правопорушення, пов'язане з тим самим приміщенням, до штрафу не менше 1000 доларів США та не більше 25 000 доларів США або до позбавлення волі на строк не більше 6 місяців, або*

одночасно до штрафу та ув'язнення, і

(b) у випадку корпорації, до штрафу не менше 10 000 доларів США та не більше $200 000.

(2) Якщо корпорація вчиняє правопорушення згідно з пунктом (1), будь-яка посадова особа, директор або агент корпорації, який керував, санкціонував, погоджувався, мовчазно погоджувався або брав участь у вчиненні правопорушення, є винним у цьому правопорушенні та несе відповідальність за покарання, передбачене за правопорушення, незалежно від того, чи була корпорація переслідувана або засуджена за це правопорушення чи ні.

(3) Кожен день, протягом якого триває порушення, є окремим правопорушенням.

Джерело: www.canlii.org/en/ab/laws/stat/sa-2020-c-c-32.7/latest/sa-2020-c-c-32.7.html.

[58] Рамкове рішення Європейського Союзу від 13 червня 2002 р. про боротьбу з тероризмом (2002/475/JHA), ст. 1

ВИВЧЕННЯ ПРОБЛЕМИ 26
Дві системи кримінального права щодо CIP: Південна Африка

Південна Африка передбачає кримінальні санкції за дії, спрямовані проти KI, як у своєму законодавстві про боротьбу з тероризмом 2004 року, так і в Законі про захист критичної інфраструктури 2019 року.[59]

2004 Закон про захист конституційної демократії від тероризму та пов'язаної з ним діяльності

«Терористична діяльність» розуміється як:

(a) *будь-які дії, вчинені в Республіці або за її межами, які*:

...
(vi) *призначений або розрахований на те, щоб спричинити серйозні перешкоди або серйозні збої в роботі основної послуги, об'єкта чи системи, або надання будь-якої такої послуги, об'єкта чи системи, державних чи приватних, включаючи, але не обмежуючись,*
(aa) *система, що використовується для електронної системи або використовується нею, включаючи інформаційну систему;*
(bb) *телекомунікаційна послуга або система;*
(cc) *банківська або фінансова служба або фінансова система;*
(dd) *система, що використовується для надання основних державних послуг;*
(ee) *система, яка використовується або використовується основною комунальною службою або транспортним постачальником;*
(ff) *важливий об'єкт інфраструктури; або*
(gg) *будь-які важливі екстрені служби, такі як поліція, медичні служби або служби цивільного захисту;*

(vi) *спричиняє будь-які серйозні економічні втрати чи значну дестабілізацію економічної системи чи значне руйнування національної економіки країни; або*

(vii) *створює серйозну надзвичайну ситуацію або загальне повстання в Республіці, незалежно від того, чи шкода, передбачена в пунктах* (a) (i) *до* (vii), *заподіяна або може бути заподіяна в Республіці чи за її межами, і чи дія, про яку йдеться у підпунктах* (ii) - (viii) *було вчинено за допомогою будь-яких засобів або методів; і*

(b) *який призначений або за своїм характером і контекстом може розумно розглядатися як призначений, повністю або частково, прямо чи опосередковано, для*

(i) *загрожувати єдності та територіальній цілісності Республіки;*

(ii) *залякувати, викликати або викликати почуття незахищеності в громадськості чи певної частини суспільства щодо їх безпеки, включаючи економічну безпеку, або викликати, викликати або поширювати відчуття жаху, страху чи паніки у цивільному населенні; або*

(iii) *неналежним чином примушувати, залякувати, примушувати, спонукати або спонукати особу, уряд, широку громадськість чи частину громадськості, національну чи міжнародну організацію чи орган чи міжурядову організацію чи орган робити чи утримуватись або утримуватися від виконання будь-яких дій, приймати чи відмовлятися від певної точки зору, чи діяти відповідно до певних принципів, чи то громадськість, чи особа, уряд, орган, організація чи установа, зазначені в підпунктах* (ii) *або* (iii), *залежно від обставин, знаходиться всередині або за межами Республіки; і*

(c) *яке вчинене, прямо чи опосередковано, повністю або частково, з метою просування індивідуального чи колективного політичного, релігійного, ідеологічного чи філософського мотиву, цілі, причини чи починання*

2019 Закон про захист критичної інфраструктури

За відсутності «терористичних намірів» або у випадках, не охоплених законодавством про боротьбу з тероризмом 2004 року, Закон про захист критичної інфраструктури 2019 року може забезпечити альтернативну правову основу для переслідування дій, спрямованих проти КІ.

[59] 7 Можливо, якщо поведінка, про яку йде мова, підпадає під дію обох правових рамок, антитерористичне законодавство застосовуватиметься як lex specialis, якщо буде доведено конкретний «терористичний намір», викладений у законі про боротьбу з тероризмом..

Що стосується застосованих покарань, вони змінюються Законом 2019 року залежно від того, чи стосується відповідна поведінка КІ, яка була віднесена до категорії низького ризику, середнього ризику або високого ризику. Категорізація відбувається в той момент, коли компетентні національні органи вирішують класифікувати певний актив як критичний. Оцінка повинна брати до уваги як ймовірність відмови, порушення або руйнування відповідної інфраструктури, так і загрозу цього; а також вплив і наслідки збою, порушення або руйнування інфраструктури або загрози цього (розділ 19).

(7) Відповідно до Закону 2019 року,[60] кримінальне покарання встановлено для особи, яка протиправно:

(a) надає, розповсюджує або публікує будь-яким способом будь-яку інформацію, що стосується заходів безпеки, які застосовуються в критичній інфраструктурі або стосовно неї, крім випадків, передбачених Законом про захищене розкриття інформації 2000 року (Закон № 26 від 2000 року), запобігання та Закон про боротьбу з корупцією 2004 року (Закон № 12 2004 року) або будь-який інший закон парламенту, який передбачає законне розкриття інформації;

(b) знімає або записує, або змушує робити або записувати, аналогове або цифрове фотозображення, відео чи плівку заходів безпеки в критичній інфраструктурі;

(c) перешкоджає, перешкоджає або не підкоряється особі, яка контролює критичну інфраструктуру, у здійсненні будь-яких заходів, необхідних або наказаних відповідно до цього Закону щодо безпеки будь-якої критичної інфраструктури;

(d) перешкоджає, перешкоджає або не підкоряється будь-якій особі під час виконання функцій або виконання будь-яких обов'язків згідно з цим Законом;

(e) входить або отримує доступ до критичної інфраструктури без згоди менеджера з безпеки або особи, яка контролює цю критичну інфраструктуру;

(f) входить або отримує доступ до критичної інфраструктури всупереч повідомленням, передбаченим у розділі 24(8) або 25(8);

(g) завдає шкоди, ставить під загрозу або порушує критичну інфраструктуру або загрожує безпеці критичної інфраструктури чи її частини;

(h) загрожує пошкодженням критичної інфраструктури; або

(a) (i) вступає в змову з іншою особою або допомагає іншій особі у вчиненні, здійсненні чи здійсненні діяльності, зазначеної в пунктах (a) - (h), вчиняє правопорушення та відповідно до підрозділів (3) і (4) несе відповідальність за засудженням до штрафу або позбавлення волі на строк до 3 років або одночасно до штрафу та позбавлення волі.

3.2.3 Неспецифічний підхід до КІ

У деяких випадках кримінальні дії, вчинені проти КІ, караються шляхом віднесення до категорії так званих «стандартних» або «класичних» правопорушень, таких як пошкодження майна, підпал,

посягання та інші.

Однією з переваг підходу, не пов'язаного з CI, є те, що держави-члени можуть покладатися на набір основних і добре встановлених правопорушень, коли недоступні більш цілеспрямовані кримінально-правові рамки. Крім того, працівники кримінальної юстиції деяких країн можуть бути краще обізнані із застосуванням класичних злочинів, ніж з новими режимами, пов'язаними з CI. Більше того, набагато більш імовірно, що певні основні правопорушення – у тому числі ті, що вкорінені в традиції загального права – можуть супроводжуватися набагато більш надійною та консолідованою судовою практикою та прецедентами.

Недоліки цього підходу включають відсутність диференціації між основними та неосновними активами, що може призвести до застосування штрафів, які не відображають більш серйозні наслідки – або потенційні наслідки – спричинені порушенням критичної інфраструктури. Крім того, заборона застосовувати кримінальні закони за аналогією може викликати питання щодо можливості віднесення правопорушень до кібердомену, які були задумані лише для фізичного світу (наприклад, використання традиційних правопорушень для протидії несанкціонованому доступу до комп'ютерних систем)[61]

[60] Розділ. 5, Правопорушення та покарання, розд. 26.

[61] З практичної точки зору, розслідування кіберзлочинів створює особливі проблеми з точки зору приписування відповідної поведінки.

3.3 Діяльність кримінального законодавства, пов'язаного з КІ

Під час розробки проекту кримінального законодавства, пов'язаного з КІ, слід ретельно розглянути сферу його застосування. Зокрема, національні органи влади повинні забезпечити, щоб компетентні національні суди могли здійснювати свою юрисдикцію в наступних сценаріях:

- Атака, скоєна проти КІ, розташованих на території держави, коли атака спричиняє істотні наслідки в іншій державі. Наприклад, промислова система контролю, розташована в Країні А, регулює постачання газу в Країну В. Після маніпулювання системою промислового контролю збої відчуваються в Країні В, але не в Країні А. Остання, тим не менш, повинна бути в змозі викликати притягнення ймовірних винних до відповідальності.

  Після нападу на СІ, розташовану в країні А, ймовірний злочинець втікає до країни В. Універсальна правова база проти тероризму вимагає, щоб сторони встановлювали свою екстериторіальну юрисдикцію щодо дій, вчинених за кордоном, принаймні у двох випадках:

  - Злочин скоєно одним із їхніх громадян (принцип активного громадянства).
  - Ймовірний злочинець знайдений на території держави та не екстрадований жодній державі, яка вимагає екстрадиції за таку саму поведінку (так званий принцип «aut dedere aut judicare»).

Вміст 15
Обов'язкова та необов'язкова юрисдикція відповідно до універсальної правової бази проти тероризму

Більшість універсальних договорів про боротьбу з тероризмом встановлюють конкретні критерії юрисдикції. Наприклад, у випадку злочину, пов'язаного з повітряним судном, згідно з Конвенцією про боротьбу з незаконним захопленням повітряних суден 1970 року та Конвенцією про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації 1971 року, національні суди встановлюють юрисдикцію щодо правопорушень на борту повітряне судно, якщо повітряне судно приземляється на території держави з передбачуваним правопорушником, який все ще перебуває на борту, і жодна інша держава-учасниця не вимагає його або її

CASE STUDY 27
Забезпечення належного формування та застосування кримінального законодавства у сфері безпеки

У грудні 2014 року кримінальний відділ Міністерства юстиції Сполучених Штатів створив відділ кібербезпеки в рамках відділу комп'ютерних злочинів та інтелектуальної власності. Одним із завдань підрозділу є забезпечення ефективного використання правоохоронних органів для притягнення винних до відповідальності, одночасно захищаючи приватне життя звичайних громадян. Переслідуючи цю мету, підрозділ також допомагає формувати законодавство про кібербезпеку для захисту комп'ютерних мереж країни та окремих жертв від кібератак. Підрозділ також бере участь у інформаційно-роз'яснювальній діяльності з приватним сектором з метою просування законної практики кібербезпеки. Підрозділ кібербезпеки очолює спеціальний радник з національної безпеки відділу комп'ютерних злочинів та інтелектуальної власності.

Джерело: www.justice.gov/criminal-ccips/cybersecurity-unit.

3.4 Санкції за порушення нормативної бази CIP

КІ потрібно захищати не лише від тих, хто навмисно намагається порушити його роботу, але й від ризику того, що особи, відповідальні за їхню безпеку, не дотримуються встановленої нормативної бази. Наприклад, законодавство низки держав-членів, зокрема тих, які переважно застосовують обов'язковий підхід до CIP (див. розділ 2.5.1), вимагає від операторів КІ готувати детальні плани безпеки, що стосуються критичних активів або процесів, які знаходяться під їх контролем. Ці плани, як правило, потрібно подати в певні часові рамки. Національне законодавство може також вимагати, щоб компетентні органи проводили інспекції на конкретних об'єктах КІ, щоб переконатися, що представлені плани безпеки були належним чином реалізовані. Інші потенційні порушення зобов'язань щодо безпеки стосуються розповсюдження або публікації конфіденційної інформації про вразливі місця активів, прийняті або заплановані заходи пом'якшення, тощо.

У всіх цих випадках держави-члени повинні забезпечити наявність належного режиму санкцій; це досягається, як правило, шляхом поєднання адміністративних і кримінальних санкцій, залежно від тяжкості (або повторності) відповідної поведінки.

ВИВЧЕННЯ ПРОБЛЕМИ 28
Режим перевірки та санкцій для операторів КІ: Франція

Франція приймає те, що можна назвати «поступовим» підходом до накладення санкцій на операторів, які не відповідають вимогам. Цей підхід спрямований на те, щоб спочатку залучити операторів до постійного діалогу у випадку, якщо інспекції об'єктів виявлять потенційні проблеми з безпекою.

Завдання контролю рівня безпеки на певному об'єкті СІ покладається на міжміністерський комітет з питань оборони та безпеки та місцеву комісію з питань оборони та безпеки, які підтримуються префектами департаментів. Інспекційні звіти мають на меті висвітлити вразливі місця по відношенню до виявлених загроз і рекомендувати заходи, яких необхідно вжити для посилення стійкості. Негайна оцінка проводиться після закінчення перевірки в присутності особи, відповідальної за безпеку КІ. Ця зустріч має на меті представити не лише початкову оцінку інспекційної групи, а й з'ясувати точку зору оператора.

Другим кроком є складання звіту про перевірку, який містить рекомендації щодо покращення захисту відповідної КІ щодо її контексту та її довідкової системи безпеки. У звіті висвітлюються вразливості КІ перед обличчям виявлених загроз і заходи, які необхідно вжити для пом'якшення ризиків і зменшення ймовірності атак. Наглядовий орган, а також префект департаменту інформуються про подальші дії, вжиті за звітом перевірки.

У разі повідомлень про проблеми вищезазначений процес може призвести до перегляду плану оператора або офіційного повідомлення про вжиття заходів безпеки протягом періоду від одного до трьох місяців, які не були виконані. Лише в крайніх випадках невиконання процес може призвести до передачі до судового органу для застосування кримінальних санкцій.

Джерело: www.legifrance.gouv.fr/download/pdf/circ?id=37828.

4. Обмін інформацією та досвідом

Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки

...

4. Закликає держави-члени досліджувати способи обміну відповідною інформацією та активно співпрацювати у запобіганні, захисті, пом'якшенні наслідків, забезпеченні готовності, розслідуванні, реагуванні на терористичні атаки або відновлення після терористичних атак, запланованих або скоєних проти критичної інфраструктури;

5. Далі закликає держави встановити або зміцнити національне, регіональне та міжнародне партнерство із зацікавленими сторонами, як державними, так і приватними, у відповідних випадках для обміну інформацією та досвідом з метою запобігання, захисту, пом'якшення, розслідування, реагування та відновлення після збиток від терористичних атак на об'єкти критичної інфраструктури, в тому числі шляхом спільного навчання, а також використання або встановлення відповідних мереж зв'язку чи оповіщення про надзвичайні ситуації;

...

7. Закликає ООН, а також ті держави-члени та відповідні регіональні та міжнародні організації, які розробили відповідні стратегії щодо захисту критичної інфраструктури, співпрацювати з усіма державами та відповідними міжнародними, регіональними та субрегіональними організаціями та установами для виявлення та обміну добром практики та заходів щодо управління ризиком терористичних атак на критичну інфраструктуру.

Додаток до Мадридських керівних принципів

Керівний принцип 50

У своїх зусиллях щодо розробки та впровадження заходів для захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевими органами влади, повинні:

...

(g) Створити або зміцнити механізми для обміну інформацією, досвідом (такими як інструменти, вказівки) та досвідом між державними та приватними зацікавленими сторонами для розслідування та реагування на терористичні атаки на такі цілі.

Керівний принцип 51

У своїх подальших зусиллях щодо захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевою владою, повинні також

розглянути:

...

(b) Впровадження національних рамок і механізмів для підтримки прийняття рішень на основі ризиків, обміну інформацією та державно-приватного партнерства як для уряду, так і для промисловості, в тому числі з метою спільної роботи для визначення пріоритетів, ...

...

(d) Встановлення процесів для обміну відповідною інформацією з партнерами в промисловості та приватному секторі шляхом, наприклад, видачі дозволів безпеки та підвищення обізнаності

4.1 Обмін інформацією в контексті стратегій CIP

Розвиток добре функціонуючих каналів для обміну інформацією між усіма зацікавленими сторонами, залученими до зусиль CIP, є важливою складовою успіху та ключовим фактором, на якому слід будувати ДПП (див. розділ 2.4.2). Міжвідомча координація також ґрунтується на надійних протоколах і практиках обміну інформацією (див. розділ 7). Крім того, обсяг і якість міжнародного співробітництва з КІ визначаються здатністю та готовністю держав обмінюватися інформацією через кордони (див. розділ 8).

4.2 Розміри обміну інформацією для CIP

Встановлюючи широку оперативну структуру для обміну інформацією, стратегії CIP та відповідні плани впровадження повинні розглядати три основні питання:

- Якою інформацією необхідно обмінюватися.
- Як потрібно ділитися інформацією для будь-якого завдання.
- Між якими суб'єктами має ділитися інформацією та на яких рівнях конфіденційності вона має базуватися

Необхідно обмінюватися інформацією для CIP на стратегічному, технічному та тактичному рівнях. З іншої точки зору, інформація може бути випадковою або не пов'язаною з подією. Він також може приймати форму обміну інформацією в режимі реального часу в контексті неминучої або триваючої кризи, коли очікується, що одержувач вживе негайних дій. Що стосується цього останнього типу інформації, платформи для обміну інформацією (з пов'язаними функціями безпеки) будуть структуровані зовсім інакше, ніж ті, які прагнуть передавати найкращі практики, стратегічні поради чи інші переваги.

Обмін інформацією може (і повинен) відбуватися між різними типами зацікавлених сторін:

- Між компетентними державними органами та операторами KI (як у межах певного сектора, так і між секторами)
- Між одним або декількома операторами KI та іншими операторами KI (як у певному секторі, так і між секторами)
- Між 1 або кількома державними органами та іншими державними органами (міжвідомчий обмін інформацією)

Усі вищезазначені типи каналів обміну інформацією можуть – і, дійсно, повинні – бути встановлені як між внутрішніми зацікавленими сторонами, так і між суб'єктами, що належать до двох або більше країн.

Інструмент 22

Портал знань (Cybil) – Глобальний форму кіберекспертизи

https://cybilportal.org/

Створений за підтримки Глобального форуму з кіберекспертизи, портал Cybil *є порталом для обміну знаннями для міжнародної спільноти з розбудови кіберпотенціалу. Портал дає змогу урядам, спонсорам та установам-виконавцям знаходити та ділитися найкращими практиками та практичною інформацією для підтримки розробки та реалізації проектів і заходів із розбудови потенціалу. Він також виступає джерелом інформації щодо кібербезпеки та нарощування потенціалу у сфері запобігання кіберзлочинності для громадянського суспільства, академічного сектору та технічної спільноти.*

Загальною метою порталу є створення нейтральної, відкритої та глобальної платформи для обміну знаннями з багатьма зацікавленими сторонами, яка робить можливим таке::

- *Обмін даними, інформацією та результатами глобальних зусиль із розбудови кіберпотенціалу*
- *Забезпечення прозорого доступу до даних та інформації про інструменти розвитку кіберпотенціалу за допомогою простого інтерфейсу користувача*
- *Інтеграція наявних ресурсів та інформації, яка вже є*

4.2.1 Обмін інформацією між державними органами та операторами KI

Обмін інформацією між державними установами з обов'язками CIP та операторами CI – незалежно від того, чи є останні державними чи приватними організаціями62 – має відбуватися в обох напрямках і охоплювати, зокрема:

- Оцінка загроз: правоохоронні органи та розвідувальні служби повинні надавати операторам KI національні оцінки загроз, що впливають на конкретні критичні активи та процеси та критичні сектори. Цю інформацію необхідно включити в оцінки ризиків, які оператори KI повинні проводити, часто відповідно до нормативних вимог, які зобов'язують їх підготувати та поширювати плани безпеки на рівні KI. І навпаки, для окремих операторів KI важливо ділитися своїми власними оцінками загроз з компетентними державними органами, щоб останні могли скласти точну картину загрози як у певному секторі KI, так і на міжгалузевому рівні..
- Підозріла діяльність: оператори KI відіграють важливу роль у спостереженні та звітуванні про незвичайні дії, що відбуваються в межах або навколо активів і процесів, за які вони відповідають. Це завдання має бути обов'язком не лише тих, хто відповідає за безпеку, а й тих, хто контактує з активами, процесами та системами CI як співробітників, підрядників, постачальників та інших зацікавлених сторін. Слід запровадити відповідні програми підвищення обізнаності та навчальні заходи, щоб гарантувати, що ці люди зможуть розпізнавати підозрілу поведінку та знати, кому про це повідомляти.
- Дані та перспективи, пов'язані з інцидентами: уроки, отримані з минулих інцидентів (включно з успішними практиками, втручаннями та невдачами), пропонують важливе розуміння способів запобігання повторенню тієї самої ситуації. Це, у свою чергу, створює основу для більш ефективного управління ризиками та заходів щодо відновлення.

Вміст 16
Публічно-приватний обмін інформацією про загрози кібертероризму

ОБСЄ склала таблицю де узагальнено основні типи інформації, пов'язаної з KI, якою державний сектор має обмінюватися з приватним сектором (і навпаки) для протидії терористичним загрозам, пов'язаним з кібернетичною мережею. Хоча таблиця зосереджена на енергетичному секторі, інформація, що в ній міститься, стосується також інших критичних секторів.[63]

Інформація про Державний сектор[64]	Інформація про приватний сектор

• Відомості про кіберможливості ключових терористичних організацій	• Інформація про основні категорії активів в енергетичному секторі (дані про газ, нафту, електроенергію, відновлювані джерела енергії; показники надійності; інформація з енергетичних бірж)
• Інформація про зв'язки між різними терористичними та нетерористичними групами	• Інформація про технічну вразливість для певних апаратних і програмних продуктів, що використовуються операторами енергетичної інфраструктури
• Стаття про минулі вектори атак	• Анонімна інформація про вплив минулих атак
• Уявлення про можливі майбутні вектори атак, отримані з аналізу підпільних веб-сайтів кіберзлочинців	• Уявлення про відновлення потребують боротьби з різними формами атак
	• Аналіз моделей атак в інших секторах критичної інфраструктури, які можуть служити індикаторами раннього попередження для енергетичного сектора

Обмін інформацією з компетентними державними органами може становити особливу проблему через часті прояви взаємної підозри, зокрема, коли критично важливі активи управляються суб'єктами приватного сектора.

---

[62] *Процес приватизації кількох секторів і підсекторів KI, таких як газ, поштові системи та телекомунікаційні послуги, який історично відбувався в багатьох країнах, призвів до того, що кілька операцій KI потрапили в приватні руки. Це, у свою чергу, породило потребу в міцному державно-приватному партнерстві. Обмін інформацією для цілей CIP є життєво важливим завданням, яке необхідно виконувати в рамках такого партнерства.*

[63] *Дивіться* www.osce.org/files/f/documents/4/b/103500.pdf.

[64] *Посилання на «державний сектор» у таблиці стосується державних установ.*

За даними ОБСЄ, «з точки зору обізнаності про безпеку все ще існує велика розбіжність між реальною потенційною загрозою цілеспрямованих атак і тим, як вони сприймаються. В основному це пов'язано з тим, що більшість атак, які відбуваються в сферах енергопостачання та промисловості, не оприлюднюються, оскільки оператори постраждалих установок не мають бажання оприлюднювати ці інциденти. Такий підхід створює ситуацію (інциденти сприймаються як окремі події), що посилює цю тенденцію до збереження інцидентів у таємниці. Промисловість у деяких країнах просять, заохочують, а іноді й зобов'язують повідомляти про ці випадки[65]

Зрештою, налагодження безперебійного обміну інформацією між приватними KI та компетентними державними органами можна розглядати як самостійну мету, яка допомагає створити справжнє відчуття спільноти навколо питань CIP.

ВИВЧЕННЯ ПРОБЛЕМИ 29
Стимули для приватного сектору ділитися інформацією в рамках стратегії кібербезпеки: Японія

Японська стратегія кібербезпеки 2015 року мала на меті подолати небажання компаній ділитися інформацією з державними органами через страх втратити довіру чи частку ринку. Згідно з цією стратегією, щоб зробити обмін інформацією більш активним, важливо зняти психологічний тягар операторів ICI щодо потенційної втрати кредиту чи руйнування репутації свого бізнесу в разі надання інформації відповідній стороні та дозволити їм визнати переваги така дія замість цього. Уряд заохочуватиме операторів ICI досягти спільного розуміння щодо внесення відповідних змін до інформації, яка надається, ~~наприклад, приховувати особистість інформаторів і вказувати обсяг і обмеження інформації, яка буде передаватись, і~~ створюватиме середовище, в якому інформатори не зазнають будь-яких необґрунтованих дій. втрати або збитки від надання інформації.

Джерело: www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

ВИВЧЕННЯ ПРОБЛЕМИ 30
Автоматизований обмін індикаторами, CISA: США

Автоматизований обмін індикаторами (надалі «AIS») — це функція, розроблена CISA. Він дає змогу обмінюватися в режимі реального часу машиночитаними індикаторами кіберзагрози та заходами захисту, щоб допомогти захистити учасників спільноти AIS і, зрештою, зменшити поширеність кібератак. Індикатори загрози та захисні заходи можуть включати, наприклад, інформацію про спроби компрометації супротивника, коли вони спостерігаються, щоб допомогти захистити інших учасників спільноти AIS і обмежити використання супротивником методу атаки.

Спільнота AIS включає організації приватного сектору, федеральні департаменти та агентства, державні, місцеві, племінні та територіальні органи влади, центри та організації з обміну інформацією та аналізу, а також іноземних партнерів і компанії. AIS пропонується безкоштовно для учасників у рамках місії CISA для роботи з державними та приватними партнерами з метою виявлення та пом'якшення кіберзагроз шляхом обміну інформацією.

AIS використовує два відкриті стандарти: Structured Threat Information Expression (відомий як «STIX™») для індикаторів кіберзагрози та інформації про заходи захисту та Trusted Automated Exchange of Indicator Information («TAXII™») для міжмашинної комунікації. комунікації. Цінуючи конфіденційність організації, AIS за замовчуванням анонімізує подання під час їх передачі, тобто особи подавців не розкриваються без їхньої попередньої чіткої згоди.

У майбутньому CISA має намір надати додаткові функції AIS, щоб дозволити учасникам ідентифікувати

[65] Дивіться www.osce.org/files/f/documents/4/b/103500.pdf.

Інструмент 23
Керівні принципи обміну інформацією про загрози ІСАО

ІСАО розробила загальні керівні принципи щодо обміну інформацією про загрози між державою та операторами критичної інфраструктури. Вони передбачають, що лінії зв'язку, як офіційні, так і неофіційні, між офіційними особами авіаційної безпеки держав повинні сприяти швидкому обміну інформацією, включаючи будь-яке підвищення рівня загрози. Обмін інформацією про методи, які використовуються для спроб порушити безпеку, досвід роботи з обладнанням безпеки та методи роботи також є надзвичайно корисним. Для спілкування під час серйозного інциденту.

Штати повинні розробити процедури для аналізу та розповсюдження інформації про загрози та забезпечити вжиття відповідних заходів операторами повітряних суден та аеропортів для протидії виявленій загрозі. Інформацію слід поширювати, коли вона потрібна особам для ефективного виконання своїх обов'язків, із застосуванням принципу «необхідно знати».

Проводячи оцінку ризику, держави-члени повинні отримати інформацію про загрозу, зокрема про можливі цілі та способи дії. Така інформація може надходити з різних джерел, зокрема з наведених нижче:

- Фактичні інциденти, включаючи успішні чи невдалі атаки на авіацію, які надають інформацію про терористичні цілі та методику (держави-члени ІКАО можуть знайти відповідну інформацію про акти незаконного втручання та інші інциденти безпеки в базі даних ІКАО про акти незаконного втручання)
- Закриті джерела, насамперед антитерористична розвідка та оцінки, які можуть бути зібрані або підготовлені розвідувальними, правоохоронними та іншими органами держав
- Відкриті джерела, які можуть включати загальнодоступну інформацію про незвичайні або підозрілі випадки та наявність предметів, які можуть бути використані в терористичних цілях, а також будь-яку іншу інформацію, яка може сприяти створенню картини загрози

Більше інформації щодо обміну інформацією та культури безпеки в авіації можна знайти в Керівництві ІСАО *з авіаційної безпеки* (Doc 8973-Restricted).

4.2.2 Обмін інформацією між операторами КІ

Надання найбільш важливих послуг суспільству є результатом складних ланцюгів поставок, які вимагають участі різних організацій, що працюють у багатьох секторах інфраструктури та галузевих сегментах. Залежність ланцюга постачання показує важливість наявності відповідних каналів між операторами для потоків інформації між секторами.

Необхідність мати адекватні механізми обміну інформацією також стосується різних операторів КІ, які виробляють або постачають той самий тип товарів чи послуг у межах одного сектора. Це особливо актуально з метою обміну передовою практикою, інформацією про методології оцінки ризиків, порадами щодо корисності певних прийнятих заходів пом'якшення, уроками, отриманими після інцидентів, та іншими цінними матеріалами. Досвідчені оператори з багаторічною практикою захисту КІ можуть з користю передати свої знання іншим, які менш знайомі з застосовною нормативною базою та стратегіями відповідності КІ. У той же час важливо усвідомлювати суттєву складність забезпечення безперебійних потоків інформації між двома або більше приватними організаціями КІ, які є ринковими конкурентами. Хоча ці суб'єкти можуть побоюватися співпраці один з одним, особливо в обміні конфіденційною

інформацією, важливо, щоб стратегії CIP вирішували це питання з метою обмеження потенційних недоліків.

ВИВЧЕННЯ ПРОБЛЕМИ 31
Ініціатива приватного сектора щодо обміну інформацією між КІ у фінансовому секторі

Центр обміну та аналізу інформації про фінансові послуги (іменований «FS-ISAC») – це глобальна спільнота з обміну кіберрозвідувальними даними, яка зосереджена виключно на фінансових послугах. Обслуговуючи фінансові установи та, у свою чергу, їхніх клієнтів, організація використовує свою інтелектуальну платформу, ресурси стійкості та надійну однорангову мережу, щоб передбачати, пом'якшувати та реагувати на кіберзагрози.

Організація зі штаб-квартирою в Сполучених Штатах Америки має представництва у Великій Британії та Сінгапурі та членські фінансові установи приблизно в 70 країнах. Його учасники представляють активи на 100 трильйонів доларів і 16 000 активних користувачів.

Центр обміну інформацією та аналізу фінансових послуг забезпечує конфіденційність і конфіденційність

4.2.3 Обмін інформацією між державними установами

Створення міжвідомчих механізмів обміну інформацією (за участю як національного, так і місцевого рівнів управління) є життєво важливим, оскільки державні установи мають повноваження координувати та впроваджувати дії, пов'язані з CIP, як горизонтально, так і вертикально. Прикладом, так би мовити, «горизонтального» обміну інформацією є ситуація, коли декілька міністерств і відомств відповідають за конкретні сектори та потребують співпраці для вирішення питань, що становлять взаємний інтерес, наприклад, оцінити вплив залежностей між секторами або керувати кризою, яка вражає декілька секторів одночасно. Прикладами домовленостей вертикального типу є ті, які необхідні для підтримки розподілу праці між муніципальними, регіональними та національними органами влади.

Цей вимір обміну інформацією є частиною ширшої міжвідомчої координації, яка детальніше розглядається в розділі 5.

ВИВЧЕННЯ ПРОБЛЕМИ 32
Обмін інформацією на рівні міста: мережа боротьби з тероризмом

Мережа підготовки до боротьби з тероризмом, яка наразі фінансується містом Стокгольм, є яскравим прикладом міжнародної платформи обміну інформацією, яка об'єднує державні організації на рівні міста. Місія Мережі полягає в тому, щоб об'єднати стратегічних лідерів, практиків і науковців для інформування про місцеву політику та методи, які створюють стійкість, щоб захистити наші міста та громади від тероризму. Ця загальна мета переслідується з встановленням ряду конкретних цілей:

- Розвивайте та підтримуйте відносини між містами-партнерами в Мережі.
- Забезпечте містам безпечну та конструктивну платформу для обміну досвідом.
- Обмінюйтеся уроками, практиками та матеріалами, які можуть посилити стійкість міста до тероризму.
- Проведіть дослідження, щоб вплинути на заходи, заходи та політику на рівні міста та поінформувати про них.
- Підтримувати впровадження рекомендацій і контролювати їх подальший вплив.
- Переглядайте звіти мережі в міру виявлення нових стратегічних уроків, досліджень або практики.
- Співпрацюйте шляхом постійного обміну досвідом та залучайте інших відповідних зацікавлених сторін, щоб забезпечити зв'язок із паралельними проектами, ініціативами та планами денними.

Мережа підготовки до боротьби з тероризмом керується міжнародною радою, якій сприяє London Resilience Group і

ВИВЧЕННЯ ПРОБЛЕМИ 33
Захист потоку інформації: телекомунікаційна система високої інтеграції Сполученого Королівства

Технології можуть суттєво допомогти агентствам у забезпеченні надходження важливої інформації в надзвичайних ситуаціях. У Сполученому Королівстві цю мету переслідує Телекомунікаційна система високої інтеграції (HITS). Розроблена урядом Сполученого Королівства HITS є незалежною системою, яка продовжуватиме функціонувати, коли звичайні стаціонарні та мобільні зв'язки стануть недоступними або погіршаться. Базуючись на військовій супутниковій мережі Skynet 5, він доступний для поліції та іншого персоналу екстрених служб на стаціонарних об'єктах, розташованих по всій території Сполученого Королівства, з додатковими мобільними одиницями, які дозволяють розгортати HITS будь-де та коли виникає потреба. Забезпечуючи передачу голосу та даних, а також

4.3 Передумови для ефективного обміну інформацією

Досвід показує, що ефективність обміну інформацією про CIP залежить від двох основних факторів:

- Здатність створити загальне розуміння того, яким типом інформації необхідно ділитися та чому, таким чином сприяючи умовам довіри між залученими зацікавленими сторонами.
- Забезпечення належного рівня захисту конфіденційної інформації, передача якої заохочується або вимагається згідно з угодами CIP.

Розробникам стратегій CIP (і тим, хто покликаний їх реалізувати) важливо розуміти, як ці два фактори взаємодіють один з одним. Хоча рівень довіри знизиться, якщо інформація не захищена належним чином, суворі рівні захисту інформації самі по собі не створять більшої довіри серед учасників.

4.3.1 Довіра

Створення справжньої довіри між учасниками певної домовленості щодо обміну інформацією може зайняти багато часу та потребуватиме активної участі всіх зацікавлених сторін. Значною мірою встановлення належного рівня довіри залежить від спільного усвідомлення доданої вартості кожного агентства-учасника. Після встановлення довіри потоки інформації значно збільшаться як в якісному, так і в кількісному плані.

Вміст 17
Фактори успіху в обміні інформацією CIP

На основі дослідження методологій CIP, *зосереджених переважно на європейських країнах, проект, що фінансується Європейським Союзом щодо рекомендованих елементів захисту критичної інфраструктури для політиків у Європі* (RECIPE), *склав список основних факторів успіху в обміні інформацією. Відповідно, як зазначено в рекомендаціях* RECIPE, *Рекомендовані елементи захисту критичної інфраструктури для політиків у Європі*:

"Досвід показує, що довіра найкраще розвивається на невеликих особистих зустрічах.

"Загалом, є деякі основні речі, які можна і чого не можна робити. Як правило, обмін інформацією найкраще починати на не надто детальному рівні. Не завжди необхідно ділитися інформацією, яка є надто конкретною, наприклад, знаннями про критичні об'єкти та їх розташування, або конкретною інформацією про вразливі місця чи інциденти. Декілька успішних обмінів інформацією підкреслюють, що починаючи з малого, можна встановити необхідний рівень довіри.

"Для встановлення довіри між людьми, які відвідують зустрічі з обміну інформацією, має бути спадкоємність. Учасники повинні бути призначені на особистому рівні з достатнім мандатом і відповідальністю у своєму власному середовищі. Як правило, заміни не допускаються.

"Зустрічі з обміну інформацією зосереджені на обміні інформацією: усі залучені організації повинні (в принципі) надавати інформацію.

"Постачальник інформації повинен гарантувати, що надана інформація має належний рівень змісту та фону. На основі інформації одержувачі інформації повинні мати можливість вжити відповідних заходів у своїх відповідних організаціях або отримати сповіщення про нову загрозу. Перш за все, постачальник інформації залишається власником спільної інформації та її класифікації конфіденційності.

"Більшість прикладів успішного обміну інформацією відбувається на добровільній основі, заснованій на довірі.

"Однак є також деякі обов'язкові приклади, коли інформація про оцінку ризиків та інциденти повинна бути спільною, напр. звітування про значні збої в мережах зв'язку загального користування відповідно до статті 13a телекомунікаційного пакету ЄС. У мандатному підході часто важко гарантувати якість обмінюваної інформації. Таким чином, навіть обов'язкові підходи наголошують на тому, що ключем до успіху їх схеми все ще є зміцнення довіри та духу добровільної співпраці» (с. 52).);

та

«Досвід показує, що засоби електронного обміну інформацією найкраще використовувати як додатковий інструмент для існуючих довірених спільнот обміну інформацією. Якщо немає рівня довіри, то дуже важко створити високий рівень довіри в електронному середовищі» (с. 58).

Джерело: www.researchgate.net/publication/261987293_RECIPE_Good_Practices_Manual_for_CIP_Policies.

4.3.2 Захист конфіденційної інформації

Зацікавлені сторони, яких закликають співпрацювати з питань CIP, часто потребують обробки конфіденційної інформації. Як наслідок, стратегії CIP повинні передбачати механізми роботи з інформацією, обіг якої обмежено на різних підставах, включаючи, наприклад, законодавство про права людини, національну безпеку та права інтелектуальної власності. Наприклад, більшість операторів приватних KI, ймовірно, нададуть дані про інциденти або фактори вразливості, лише якщо вони отримають відповідні гарантії того, що оприлюднення конфіденційної інформації не матиме негативного впливу на їхній бізнес (наприклад, інформація не буде забезпечить конкурентам ринкову перевагу, а також не буде використано проти них державними установами для інших цілей, окрім захисту KI). Таким чином, головна проблема полягає в тому, щоб якомога більше інформації

передавалося між різними зацікавленими сторонами, захищаючи її конфіденційний характер. Це може бути як конфіденційна бізнес-інформація, якою володіють компанії, або секретна інформація, якою володіють штатні установи.

Створення довірчого середовища для обміну інформацією залежить від встановлення чітких правових та операційних рамок для захисту конфіденційної природи спільних даних. При розробці таких рамок головна мета сприяння обігові інформації для цілей CIP завжди повинна враховувати відповідні режими прав людини та захисту даних. Відповідно до Хартії основних прав Європейського Союзу, наприклад, персональні дані «повинні оброблятися справедливо для визначених цілей і на основі згоди відповідної особи або на іншій законній підставі, встановленій законом. Кожен має право на доступ до даних, які були зібрані стосовно нього, і право на їх виправлення.''.[66]

Вміст 18
Конфіденційна інформація, пов'язана з CIP, у правовій базі Європейського Союзу

Директива Ради Європейського Союзу 2008/114/ЕС щодо «ідентифікації та позначення європейської критичної інфраструктури» містить таке визначення «чутливої інформації, пов'язаної із захистом критичної інфраструктури»: «Факти про критичну інфраструктуру, які у разі розголошення можуть бути використані для планування та діяти з метою спричинити збій або руйнування об'єктів критичної інфраструктури».[67]
Ця ж Директива встановлює «спеціальний принцип», відповідно до якого «держави-члени, Комісія та відповідні наглядові органи повинні гарантувати, що конфіденційна європейська інформація, пов'язана із захистом критичної інфраструктури, яка надана державам-членам або Комісії, не використовується для будь-яких інших цілей, окрім захист КІ. Ця стаття також поширюється на неписьмову інформацію, якою обмінюються під час зустрічей, на яких обговорюються чутливі теми».[68]

Не вся інформація, пов'язана з КІ, повинна бути конфіденційною. Таким же чином, не вся інформація, яка вважається «делікатною», заслуговує на такий самий ступінь захисту. Обмеження на обіг інформації, пов'язаної з КІ, можуть набувати різних форм і бути більш-менш суворими залежно від конкретних обставин і цілей певного типу обміну інформацією. Нова Зеландія, наприклад, встановила основний принцип, згідно з яким інциденти повинні розглядатися на найнижчому можливому рівні класифікації як засіб забезпечення раннього та ефективного розповсюдження важливої інформації всім особам, відповідальним за зменшення впливу.[69]

З операційної точки зору можна використовувати кілька підходів для захисту обігу конфіденційної інформації, і вони часто доповнюють один одного. Як правило, ці підходи зосереджені навколо таких питань: допуски та процедури перевірки; системи кольорового кодування; та електронні інструменти, як описано нижче.

4.3.2.1 Допуски та перевірка

Уряди можуть надавати дозволи безпеки для ключових зацікавлених сторін, яким потрібен доступ до конфіденційної інформації, пов'язаної зКСІ. Відповідно до Директиви Ради Європейського Союзу 2008/114/ЕС, «будь-яка особа, яка працює з секретною інформацією відповідно до цієї Директиви від імені держави-члена або Комісії, повинна мати відповідний рівень перевірки безпеки».[70]

Платформи обміну інформацією можуть також прийняти конкретні критерії відбору для прийому нових учасників на основі, наприклад, необхідності схвалення існуючими учасниками включення нових організацій, перевірки довідкових даних, співбесід з державними органами, відповідальними за платформу, та інші вимоги.

У деяких випадках приватному сектору може бути складно залучити членів правоохоронного співтовариства через побоювання, що розкриття певних типів інформації може спровокувати дії з їхнього боку, які зашкодять бажанню учасників ділитися інформацією взагалі. Важливо, щоб стратегії CIP враховували ці потенційні труднощі та знаходили шляхи їх подолання.

---

66 Art. 8 (2).

67 Art. 2 (d).

68 Art. 9.

69 See https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf.

70 Art. 9.

4.3.2.2 Системи кольорового кодування

Ці системи засновані на принципі, згідно з яким той, хто надає інформацію, визначає, якою мірою сама інформація може поширюватися. Протокол світлофора застосовує цю концепцію, оскільки джерело інформації позначає її одним із чотирьох кольорів:

Червоний: обмежено лише для названих одержувачів.

Жовтий: обмежений обіг, причому автор повинен визначити межі та умови обміну інформацією.

Зелений: інформація може поширюватися в певній спільноті, але не може бути загальнодоступною (наприклад, в Інтернеті) або оприлюднена за межами спільноти.

Білий: необмежений обіг.

Однією з переваг протоколу «Світлофор» є його зручність для користувача та чіткі межі, які він встановлює між обов'язками емітента та одержувача.

4.3.2.3 Електронні інструменти

Щоб забезпечити обмін інформацією, деякі платформи використовують електронні інструменти, такі як екстранет, для обміну документами. Екстранет — це телекомунікаційна мережа, яка використовує Інтернет-технології та мета якої — полегшити обмін між головною організацією та двома чи більше партнерами, які географічно віддалені. Щоб отримати доступ до інформації про мережу, партнери повинні пройти автентифікацію.

ВИВЧЕННЯ ПРОБЛЕМИ 34
Національні підходи до захисту конфіденційної інформації, пов'язаної з КІ: Австралія, Франція, США

Австралія

Мережа довіреного обміну інформацією, заснована урядом Австралії в 2003 році, є основним механізмом залучення в країні для обміну інформацією між бізнесом і державою та ініціатив з підвищення стійкості. Мережа забезпечує безпечне середовище, в якому власники та оператори КІ з семи галузевих груп регулярно зустрічаються для обміну інформацією та співпраці всередині та між секторами для вирішення проблем безпеки та безперервності бізнесу. Групи секторів у Мережі включають банківську справу та фінанси, комунікації, енергетику, харчування та бакалію, охорону здоров'я, транспорт і водопостачання. Крім того, існують спеціалізовані форуми (відомі як «міжгалузеві групи інтересів»), які допомагають у тимчасовому дослідженні наскрізних проблем, а також «консультативна група експертів із стійкості», яка приділяє значну увагу організаційній стійкості. Координацію та стратегічне керівництво Мережею забезпечує Консультативна рада з питань критичної інфраструктури, яка складається з голів кожної з груп Мережі, вищих урядових представників відповідних установ, а також вищих представників уряду штатів і територій..

Франція

Директиви та плани, прийняті в рамках національної системи безпеки життєдіяльності (відомої під французькою абревіатурою «SAIV»), класифікуються на рівні «конфіденційної оборони». Незалежно від того, чи є вони емітентами чи одержувачами, оператори КІ забезпечують знищення секретних документів, які їм більше не потрібні, особливо коли:

- Секретний документ переглядається або скасовується.
- «Життєва точка» скасовується.
- Скасовується «життєва зона».
- Оператор втрачає статус «життєвого оператора».

«Життєво важливі оператори» можуть не захотіти розкривати деяку дуже конфіденційну інформацію, пов'язану з управлінням ризиками та кризою. У такому випадку вони повинні застосувати спеціальні процедури. Компетентні адміністративні органи, які контролюють плани безпеки операторів, можуть обговорити питання з операторами, якщо це необхідно для виконання їхньої ролі. Такі органи можуть взяти до відома інформацію, яку оператори бажають приховати, не обов'язково використовуючи її за своїм бажанням.

США

Інформаційна мережа внутрішньої безпеки — це офіційна система, яку використовує Департамент внутрішньої безпеки для довіреного обміну конфіденційною, але несекретною інформацією між федеральними, державними, місцевими, територіальними, племінними, міжнародними та приватними партнерами. Оператори використовують Мережу для отримання даних внутрішньої безпеки, безпечного надсилання запитів між агентствами, керування операціями, координації запланованих заходів безпеки та безпеки, реагування на інциденти та обміну інформацією, необхідною для виконання своїх завдань..

У Мережі платформа, відома як «HSIN-CI», є основною системою, за допомогою якої власники та оператори приватного сектору, Міністерство внутрішньої безпеки та інші федеральні, державні та місцеві урядові установи співпрацюють для захисту критично важливої інфраструктури країни. HSIN-CI надає інструменти для співпраці в режимі реального часу, включаючи віртуальний простір для зустрічей, обмін документами, сповіщення та обмін миттєвими повідомленнями безкоштовно.

Завдяки HSIN-CI *користувачі можуть*:

- Отримувати, надсилати та обговорювати своєчасну, дієву та точну інформацію.
- Підтримуйте прямий надійний зв'язок із Міністерством внутрішньої безпеки та іншими перевіреними зацікавленими сторонами.
- Передавати інформацію про загрози, вразливі місця, безпеку, заходи реагування та відновлення, що впливають на секторальні та міжгалузеві операції.

Джерело: www.cisc.gov.au/engagement/trusted-information-sharing-network; www.legifrance.gouv.fr/download/pdf/circ?id=37828; *та* www.dhs.gov/hsin-critical-infrastructure.

ВИВЧЕННЯ ПРОБЛЕМИ 35
Інформаційний шлюз критичної інфраструктури* (CI Gateway): *Канади

Однією з цілей Національної стратегії та Плану дій щодо критичної інфраструктури є своєчасне просування обміну інформацією та захисту між партнерами KI. Щоб досягти цього, Стратегія передбачає розробку шлюзу KI, веб-порталу для обміну інформацією про критичну інфраструктуру, який буде розміщено на домені Міністерства громадської безпеки Канади.

У Плані дій щодо критичної інфраструктури на 2014-2017 рр. визнається, що в рамках початкового Плану дій було розроблено кілька домовленостей щодо обміну інформацією, які ґрунтувалися на цих досягненнях шляхом подальшого розширення можливостей обміну інформацією різними засобами, включаючи офіційні угоди, віртуальні та фізичні механізми та створення та розповсюдження інформаційних продуктів.

Відповідно до Плану дій на 2014-2017 рр. ключові завдання у цій сфері включено:

- Розширення членства та участі зацікавлених сторін у канадському шлюзі критичної інфраструктури та використання можливостей шлюзу CI для покращення обміну інформацією та співпраці в конкретних проектах: Міністерство громадської безпеки Канади прагне розвивати успішний запуск шлюзу CI, гарантуючи, що його членство охоплює десять секторів та інших ключових зацікавлених сторін, заохочуючи активну участь членів і сприяючи його використанню галузевими мережами та спільнотами практиків для обміну інформацією та передовим досвідом, а також для спільної роботи над конкретними проектами.
- Спонсорування дозволів безпеки серед зацікавлених сторін у приватному секторі з метою розширення обміну конфіденційною інформацією: деяка інформація, зібрана канадською спільнотою безпеки та розвідки, є конфіденційною та може надаватися лише особам, які мають відповідний дозвіл безпеки. Міністерство громадської безпеки Канади прагне співпрацювати з провідними федеральними департаментами та агенціями, щоб збільшити кількість зацікавлених сторін, які пройшли перевірку безпеки в приватному секторі..

Відповідно до попередніх планів дій, План дій на 2021-2023 рр. передбачав залучення зацікавлених сторін до «продовження зусиль з модернізації CI Gateway для задоволення мінливих потреб спільноти критичної інфраструктури та сприяння використанню CI Gateway для збільшення кількості користувачів і відвідування сайту».

Джерело: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx та www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.

Інструмент 24

Захист конфіденційної інформації авіаційної безпеки – ICAO

ICAO розробила загальні керівні принципи щодо захисту інформації, пов'язаної з авіаційною безпекою. Це повинно бути обмежено тими особами, які потребують такої інформації під час виконання своїх обов'язків і, отже, мають право мати доступ до такої інформації та використовувати її (це відоме як принцип «необхідності знати»). До конфіденційної інформації щодо авіаційної безпеки слід застосовувати заходи захисту, а ступінь захисту має визначати або держава, або відповідні організації, беручи до уваги національні вимоги щодо захисту конфіденційної інформації, встановлені відповідними органами. Захисні заходи повинні застосовуватися до ідентифікації, обробки, обміну або утилізації конфіденційної інформації авіаційної безпеки.

Держави повинні розробити письмову політику, процедури та вказівки щодо ідентифікації, обробки, обміну (усними, фізичними та електронними засобами) та утилізації конфіденційної інформації щодо авіаційної безпеки, щоб уникнути будь-якого несанкціонованого розголошення. Такі політики, процедури та вказівки також мають стосуватися несанкціонованого розголошення за допомогою захисного маркування.

При роботі з конфіденційною інформацією щодо авіаційної безпеки держави або відповідні організації повинні захищати таку інформацію від несанкціонованого доступу або розголошення. Держави або відповідні організації повинні враховувати, що доступ до конфіденційної інформації з питань авіаційної безпеки має бути обмежений тими, кому це необхідно знати; уповноважений персонал повинен мати доступ та використовувати конфіденційну інформацію з питань авіаційної безпеки лише у міру необхідності виконання своїх обов'язків; конфіденційну інформацію про авіаційну безпеку не слід копіювати без потреби; конфіденційну інформацію про авіаційну безпеку слід належним чином зберігати в надійному місці, наприклад у закритій шафі або ящику, коли вона не використовується; і електронні файли, що містять конфіденційну інформацію про авіаційну безпеку, повинні зберігатися в безпечний спосіб, наприклад за допомогою шифрування, захисту паролем і безпечних серверів. Такі електронні файли, якщо вони зберігаються на захищеному портативному електронному пристрої, повинні бути замкнені в шафі або закритій шухляді, коли вони не використовуються.

При обміні конфіденційною інформацією про авіаційну безпеку держави або відповідні організації повинні захищати таку інформацію від несанкціонованого доступу або розголошення шляхом застосування захисних заходів під час передачі конфіденційної інформації з авіаційної безпеки, наприклад надання одержувачу відповідних інструкцій щодо поводження з використанням авторизованих методів доставки, таких як авторизовані кур'єри та безпечні способи пакування. Електронні файли, що містять конфіденційну інформацію про авіаційну безпеку, повинні передаватися з використанням шифрування або захисту паролем. Якщо використовується пароль, він має бути достатньо надійним і передаватися окремо від оригінального електронного файлу. Перш ніж надавати конфіденційну інформацію з питань авіаційної безпеки, з одержувачем необхідно попередньо домовитися про спосіб транспортування, а також підтвердити отримання, а також укласти угоду про нерозголошення. Усні обговорення (телефоном, під час відеоконференцій або особисто) щодо конфіденційної інформації щодо авіаційної безпеки слід проводити лише з особами, яким це необхідно знати, і в умовах, де такі обговорення не можуть бути підслухані особами, які не мають на це повноважень.

Держави або відповідні організації також повинні встановити національні закони або політику зберігання записів, щоб гарантувати, що конфіденційна інформація з авіаційної безпеки не зберігається довше, ніж це необхідно. При знищенні конфіденційної інформації з питань авіаційної безпеки держави або відповідні організації повинні знищити матеріал у спосіб, який гарантує, що така інформація не підлягає відновленню та не може бути реконструйована для запобігання несанкціонованому доступу або розголошенню. Держави або відповідні

організації повинні гарантувати, що будь-яка третя сторона, з якою передається конфіденційна інформація про авіаційну безпеку, дотримується тих самих методів утилізації.

Щоразу, коли необхідний обмін інформацією між державами, вимога до інформації повинна бути встановлена письмовими угодами або домовленостями про обмін. Такі домовленості повинні включати положення щодо ідентифікації, обробки, обміну та розкриття конфіденційної інформації безпеки іншим державам. Останні повинні чітко ідентифікувати інформацію як конфіденційну інформацію з авіаційної безпеки та повідомляти про будь-які конкретні вимоги щодо захисних заходів, які мають бути застосовані до того, як надавати таку інформацію іншим державам. При отриманні конфіденційної інформації про авіаційну безпеку держави повинні застосовувати необхідні захисні заходи для запобігання несанкціонованому використанню або розголошенню.

Джерело: ICAO Aviation Security Manual, Doc 8973-Restricted.

5.Забезпечення міжвідомчої координації

Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки,

...

6. *Наполегливо закликає всі держави забезпечити, щоб усі відповідні національні департаменти, агентства та інші організації тісно та ефективно співпрацювали разом у питаннях захисту критичної інфраструктури від терористичних атак*

5.1 Необхідність та виклики міжвідомчого підходу до CIP

Існує безліч норм, правил і стандартів щодо питань безпеки в різних секторах KI, встановлених різними державними установами. Розвідувальна інформація, пов'язана з тероризмом, необхідна для оцінки поточних типів і рівнів загрози KI, часто збирається кількома відомствами, підпорядкованими різним міністерствам. Управління кризою та заходи з відновлення є складними процесами, у які втручаються декілька державних організацій (на місцевому, муніципальному, регіональному та національному рівнях) (служби швидкого реагування, правоохоронні органи та інші). Крім того, у багатьох випадках кілька організацій можуть бути залучені до певної функції безпеки в одному критичному секторі. Таким є випадок авіаційного сектору, де компетентний орган, керівництво аеропорту та правоохоронні органи можуть розділити відповідальність за захист аеропортів, аеронавігаційних засобів і послуг..

Широка міжвідомча координація є ключовою передумовою впровадження відповідних рівнів CIP. Міжгалузеві національні стратегії мають, так би мовити, з'єднати крапки між різноманітними національними агенціями, відповідальними за дії, пов'язані з CIP. Слід досягти координації між зацікавленими сторонами, такими як міністерства (таких як міністерства зв'язку, економіки, безпеки, юстиції, внутрішніх справ, оборони та офіс Кабінету Міністрів),

регіональні органи та регулятори, які співпрацюють на стратегічному, тактичному та оперативному рівнях. Однак досягнення цієї головної мети не завжди є простим. Використання різної термінології та жаргону різними суб'єктами, залученими до заходів із запобігання, реагування та відновлення, разом із відсутністю єдиних процедур і каналів зв'язку потенційно може вплинути на якість загальних зусиль CIP. До того ж, «у деяких випадках органи державної влади, як правило, дотримуються різних планів, коли йдеться про CIP. Деякі з них дотримуються влади ринкових сил, тоді як інші твердо вірять у законодавчу роль уряду. Однак ці розбіжності можуть стати серйозними каменями спотикання для співпраці при взаємодії з приватним сектором».[71]

---

[71] ОБСЄ, Посібник із належної практики щодо захисту критично важливої неядерної енергетичної інфраструктури (NNCEIP) від терористичних атак із зосередженням на загрозах, що виходять із кіберпростору, Відень, 2013 р. Доступно за адресою www.osce.org/atu/103500?download=true.

ВИВЧЕННЯ ПРОБЛЕМИ 36
Федерально-провінційно-територіальна робоча група з критичної інфраструктури: Канада

Поряд із галузевими мережами та міжгалузевим форумом країни, у рамках канадської національної стратегії та плану дій було створено Федерально-провінційно-територіальну робочу групу з критичної інфраструктури. Цей орган є прикладом вертикальної координації між органами влади у федеральній системі уряду. Його заявлені цілі полягають у тому, щоб:

- Підтримувати реалізацію Стратегії в рамках федеральних, провінційних і територіальних юрисдикцій
- Надавати керівництво та брати участь у розробці та реалізації Плану дій
- Дійте як центр обміну інформацією для урядів щодо критичних питань, пов'язаних з інфраструктурою, для федеральних, провінційних і територіальних високопосадовців, відповідальних за управління надзвичайними ситуаціями
- Сприяти федеральним, провінційним і територіальним мережам для підтримки обміну інформацією про критичну інфраструктуру, управління ризиками, планування критичної інфраструктури та навчань
- Визначте критичні питання інфраструктури, що мають регіональне чи юрисдикційне значення
- Розвивайте загальне розуміння ризиків критичної інфраструктури та взаємозалежностей
- Заохочуйте участь у навчаннях для перевірки робочих планів у конкретних секторах та виявлення нових ризиків
- Надайте вказівки щодо поточних і майбутніх проблем, пов'язаних із критичною інфраструктурою
- Визначати зв'язки між федеральними, провінційними та територіальними програмами та ініціативами та сприяти обміну інформацією та найкращими практиками

Членство в Робочій групі відкрите для всіх урядів відповідно до їхніх потреб і можливостей. Рішення приймаються лише після обміну інформацією та надання всім членам можливості прокоментувати. Співголовами робочої групи є представник Відділу управління надзвичайними ситуаціями та національної безпеки Міністерства громадської безпеки Канади та представник провінції або території, визначений консенсусом групи.

У Плані дій на 2021-2023 роки підтверджено зобов'язання уряду Канади продовжувати співпрацю з Федерально-провінційно-територіальною робочою групою з критичної інфраструктури та займатися вирішенням поточних і нових проблем, з якими стикаються сектори критичної інфраструктури.

Джерело: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr/index-en.aspx та www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.

5.2 Координація агенцій у кризових сценаріях

Важливим аспектом міжвідомчої координації є здатність усіх зацікавлених сторін оперативно та ефективно діяти в кризових ситуаціях. Після визначення основних структур і процесів управління кризою стратегії CIP повинні гарантувати, що вони працюватимуть безперебійно в разі потреби. Нижче наведено деякі основні передумови для плавного та швидкого прийняття рішень:

- *Чіткий розподіл ролей і обов'язків із застереженням, що рішення мають прийматися на найнижчому відповідному рівні та що координація доступна на найвищому необхідному рівні. Можна стверджувати, що «тісна інтеграція операторів KI в управління кризами вимагає виконання великого набору вимог. Взаємне розуміння ролей, обов'язків, можливостей і здібностей – це тривалий процес, який вимагає вкладення часу, людської співпраці, вивчення сленгу один одного».*[72]

- Повне розуміння наслідків порушення КІ, включаючи його каскадні ефекти. Було зазначено, що «поточний акцент у врегулюванні кризових ситуацій у більшості країн набагато більше зосереджений на одному зриві КІ та його потенційних наслідках, напр. планування перебоїв у постачанні питної води, аніж у каскадних збоях і збоях у загальному режимі, як-от сильний шторм, що порушує кілька КІ одночасно.

---

[72] Посібник із належної практики щодо політики CIP для політиків у Європі, RECIPE, 2011. Доступно за адресою www.researchgate.net/publication/261987293_RECIPE_Good_ Practices_Manual_for_CIP_Policies.

Рекомендується підготуватися до збоїв загального режиму та ефектів каскадних збоїв, що впливають на декілька KI одночасно».[73]

- *Призначення координаторів у всіх залучених установах з доступністю 24/7.*
- *Створення адекватних систем управління інформацією для підтримки ефективного збору, аналізу та поширення даних для підтримки прийняття рішень одним і кількома відомствами, а також надання інформації громадськості. Комунікаційні заходи повинні бути розроблені таким чином, щоб звести до мінімуму ситуації, коли надходять суперечливі інструкції. Крім того, в ідеалі системи управління інформацією підтримуються захищеними лініями зв'язку.*

ВИВЧЕННЯ ПРОБЛЕМИ 37
Управління кризою після теракту в Лондоні 2005 року

7 липня 2005 року внаслідок вибуху чотирьох бомб на транспортній системі Лондона загинуло 52 громадянина. Обставини аварії особливо ускладнили координацію реагування на надзвичайні ситуації. Як підкреслюється в звіті Коронер після розслідування подій, «розташування трьох вибухів у тунелях означало, що було обмежено кількість очевидців того, що сталося. По-друге, комунікації в тунелях були обмежені. По-третє, масові збої, спричинені вибухами, призвели до лавини вхідних дзвінків, які перевантажили радіооператорів і спричинили перевантаження всіх радіо- та телефонних комунікацій. Знадобився час, щоб визначити та витягнути найважливішу та важливу інформацію з безлічі отриманих повідомлень (на додаток до звичайних щоденних запитів до екстрених служб і лондонського метро), щоб агентства могли реагувати належним чином».

Коронер виявив низку недоліків у реагуванні на надзвичайні ситуації та надав кілька рекомендацій. Зокрема, «докази виявили не просто збої в існуючих на той час системах зв'язку, але й деякі базові непорозуміння між службами екстреної допомоги щодо їхніх відповідних ролей та операцій, наприклад, нездатність деяких працівників екстреної допомоги оцінити та зрозуміти зобов'язання щодо частина першого присутнього персоналу LAS [Лондонської служби швидкої допомоги], щоб діяти як офіцери швидкої допомоги, а не брати участь у лікуванні постраждалих... Окремі служби екстреної допомоги зіткнулися із затримками та труднощами, намагаючись визначити характер інцидентів, або які ресурси були потрібні, і були значні відмінності в тому, як кожен аварійний рятувальник намагався вирішувати загальні проблеми, такі як використання радіостанцій, де існував можливий ризик детонації вторинних пристроїв... Отже, дані демонструють необхідність перегляд обсягу та обсягу міжвідомчого навчання. Таке навчання має життєво важливе значення для того, щоб допомогти зменшити плутанину та сприяти кращому розумінню відповідних ролей екстрених служб»

У доповіді коронера зазначено, що, незважаючи на те, що навчання (у формі так званих «настільних» або «реальних» вправ) вже широко проводилося для вищого керівництва, «докази також показали, що було значно менше міжвідомче навчання, доступне для тих «перших» співробітників екстрених служб, яким доручено реагувати на початковий хаос, бійню та плутанину великого інциденту».

- Розглянуто інші рекомендації:
- Міжвідомча підготовка персоналу на передовій з серйозних інцидентів;
- Протоколи для обміну інформацією про надзвичайні ситуації між транспортом Лондона та екстреними службами
- Встановлення та комплектування пунктів зустрічі
- Процедури підтвердження та передачі інформації про те, що тяговий струм вимкнено в лондонському метро
- Забезпечення засобами першої медичної допомоги та ношами в поїздах та станціях метро
- Процедури сортування кількох постраждалих
- Невідкладна допомога типу, що надається Лондонською бригадою швидкої медичної допомоги та екстреного реагування на інциденти

У звіті коронер також торкався таких питань, як регулювання постачання перекису водню; ефективний міжвідомчий зв'язок; хороший зв'язок і обмін інформацією; Базові радіостанції Airwave *та їх потужність у разі великого інциденту; і прозорість між різними службами екстреного реагування.*

Джерело: http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06/rule43-report.pdf.

[73] mam же

ВИВЧЕННЯ ПРОБЛЕМИ 38
Національний посібник із сповіщення та управління кіберінцидентами, 2019: Іспанія

Уряд Іспанії наділяє різні державні інституції повноваженнями щодо питань кібербезпеки, пов'язаних із знанням, управлінням і реагуванням на інциденти кібербезпеки, що впливають на різні інформаційні та комунікаційні мережі країни. Установи державного сектору, громадяни, компанії, оператори критичної інфраструктури, академічні та дослідницькі мережі мають у своєму розпорядженні низку довідкових органів, на яких базується спроможність уряду реагувати на інциденти кібербезпеки.:

- CCN-CERT: Спроможність реагування на інциденти інформаційної безпеки Національного криптологічного центру, який має загальну компетенцію щодо державного сектору та систем, які обробляють секретну інформацію.
- INCIBE-CERT: належить до Національного інституту кібербезпеки, який має компетенцію щодо громадськості та приватного сектору. INCIBE-CERT також надає послуги реагування на інциденти установам, пов'язаним з іспанською академічною та дослідницькою мережею, у координації з CCN-CERT щодо державних органів.
- CNPIC: Національний центр захисту інфраструктури та кібербезпеки, який має компетенцію щодо критичної інфраструктури та критичних операторів.
- ESP-DEF-CERT: належить Об'єднаному командуванню кіберзахисту, яке має компетенцію над мережами та інформаційними та телекомунікаційними системами Збройних Сил, а також іншими мережами та системами, спеціально довіреними йому, які впливають на національну оборону.

Національний посібник є офіційним довідником для сповіщень про кіберзлочини (обов'язкових або необов'язкових), а також для запитів щодо реагування на інциденти кібербезпеки. Документ є посібником, який дозволяє будь-якій організації - державній чи приватній - а також окремим громадянам знайти точні вказівки щодо того, кому та як повідомляти про інцидент кібербезпеки. Посібник відповідає нормативним базам Іспанії та Європейського Союзу та вказівкам відповідних міжнародних організацій, які прагнуть узгодити можливості реагування на інциденти кібербезпеки.

Джерело: https://cybilportal.org/wp-content/uploads/2020/04/SPAIN-CYBERINCIDENTS-NATIONAL-GUIDE.pdf.

5.3 Спільні навчання та тренувальні заходи

Додаток до Мадридських керівних принципів

Керівний принцип 51

У своїх подальших зусиллях щодо захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевою владою, повинні також розглянути:

...

У контексті CIP міжвідомчі навчання та навчальні заходи загальновизнані як важливі інструменти сприяння та консолідації міжвідомчої координації. На практиці необхідно реалізовувати різні форми навчань залежно від поставлених цілей, кількості залучених суб'єктів та учасників, наявності ресурсів та інших факторів. У більшості випадків переслідуються цілі:

- *Досягніть спільного розуміння застосовних процесів і методологій.*
- *Уточнити взаємні ролі та відповідальність у циклах захисту KI.*

- Створіть у персоналу впевненість у виконанні інструкцій і політик захисту, пов'язаних із KI (важливо під час стресових фаз справжньої кризи).
- Визначте слабкі місця та внесіть будь-які зміни, необхідні для безпечного завершення фактичної надзвичайної ситуації.
- Забезпечення робочої надійності та сумісності всього комунікаційного обладнання, призначеного для використання під час кризи.

Вміст 19
Підготовка, тренування відповідно до Міжнародного кодексу охорони суден та портових засобів

Міжнародний кодекс охорони суден і портових засобів (Кодекс ISPS), *який діє з* 2004 *року, є поправкою до Конвенції про безпеку життя на морі* (SOLAS). *Його метою є покращення виявлення та пом'якшення загроз безпеці, з якими стикаються судна, які здійснюють міжнародні рейси, та портові засоби, що обслуговують такі судна. Кодекс зв'язує уряди країн-учасниць і судноплавну галузь у структуроване партнерство, засноване на розвитку сильної культури, заснованої на безпеці, і методології оцінки ризиків.*

Виходячи з цього, Кодекс передбачає обов'язкове навчання та тренування в рамках заходів, спрямованих на покращення розуміння зацікавленими сторонами своїх обов'язків та відповідальності, пов'язаних із безпекою (розділи 13 та 18 Кодексу). Зокрема, необхідно передбачити проведення тренувань через відповідні проміжки часу. Що стосується охорони судна, під час навчань слід враховувати «тип судна, зміни в персоналі судна, портові засоби, які необхідно відвідати, та інші

ВИВЧЕННЯ ПРОБЛЕМИ 39
Кібер Європа

Керований Агентством ЄС з кібербезпеки (ENISA), Cyber Europe – *це серія навчань з управління кіберінцидентами та кризами для державного та приватного секторів з країн Європейського Союзу та ЄАВТ. Навчання є моделюванням масштабних інцидентів у сфері кібербезпеки, які переростають у повноцінну кіберкризу. Вони пропонують командам з IT-безпеки, безперервності бізнесу та управління кризовими ситуаціями можливість аналізувати передові технічні інциденти кібербезпеки та мати справу зі складними ситуаціями безперервності бізнесу та управління кризовими ситуаціями.*

Навчання Cyber Europe *почалися в* 2010 *році і проводяться кожні два роки. В останніх навчаннях серії* Cyber Europe 2018 *взяли участь понад* 1000 *учасників з усієї Європи. Наступні навчання відбулися влітку* 2022 *року, під час яких було розроблено сценарій, що стосується охорони здоров'я, за участю національних і державних груп реагування на інциденти комп'ютерної безпеки, органів кібербезпеки, міністерств охорони здоров'я, медичних організацій*

ВИВЧЕННЯ ПРОГРАМИ 40
Збірник вправ Інституту стратегічних досліджень: Україна

Український інститут стратегічних досліджень склав інвентаризацію найпоширеніших типів вправ та основних напрямків їх використання:

- Семінари: для надання загальних вказівок щодо існуючих стратегій, планів, політики, процедур, протоколів, ресурсів і концепцій.
- Настільні вправи: для обговорення гіпотетичної, змодельованої надзвичайної ситуації. Настільні вправи корисні для полегшення концептуального розуміння, визначення сильних сторін і областей для вдосконалення та досягнення змін у сприйнятті.
- Симуляції (ігри): для вивчення наслідків рішень і дій гравців. Цей тип вправ часто базується на створенні конкурентного середовища, де дві або більше команд стикаються одна з одною в реальних ситуаціях.
- Тренування: провести навчання на новому обладнанні, перевірити процедури або практикувати та підтримувати поточні здібності. Тренування базуються на понятті навчання та вдосконалення навичок шляхом повторення завдань.
- Повномасштабний (в прямому ефірі): зіткнути учасників зі сценаріями, призначеними для відображення реальних ситуацій, вимагаючи від них дій і реагування в реальному часі.

Оскільки деякі з вищезгаданих навчань включають велику кількість учасників і базуються на складних симуляціях у реальному часі, вони вимагають ретельного планування та часто місяців, якщо не років,

Інструмент 25
Навчання з кібербезпеки: ініціативи CISA (США)

CISA покладається на два основні ресурси для вдосконалення навичок зацікавлених сторін у захисті кібербезпеки КІ:

- Навчальний посібник з кібербезпеки

www.cisa.gov/publication/cybersecurity-workforce-training-guide

Посібник, випущений у 2021, адресований нинішнім і майбутнім федеральним, державним, місцевим, племінним і територіальним працівникам. Це допомагає їм розробити план навчання на основі їх поточного рівня навичок і бажаних кар'єрних можливостей.

- Настільні пакети вправ CISA (іменовані «CTEPs»)www.cisa.gov/cisa-tabletop-exercises-packages

Це повний набір ресурсів, призначених для допомоги зацікавленим сторонам у проведенні власних навчань. Партнери можуть використовувати CTEP, щоб ініціювати обговорення у своїх організаціях щодо їх здатності реагувати на різні сценарії загроз. Кожен пакет можна налаштувати та містить шаблонні цілі вправ,

5.4 Сприяння сумісним процесам і рішенням

Додаток до Мадридських керівних принципів

Керівний принцип 50

У своїх зусиллях щодо розробки та впровадження заходів для захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевими органами влади, повинні:

Ключовим поняттям міжвідомчої координації є «сумісність». У контексті міжвідомчої координації можливість покладатися на сумісні процеси набуває особливого значення для зв'язку реагування на надзвичайні ситуації. У зв'язку з цим було помічено, що

ця проблема ... викликає занепокоєння майже до тих пір, поки радіостанції використовуються службами швидкого реагування та іншими посадовими особами громадської безпеки. Однак лише після терористичної атаки у Всесвітньому торговому центрі 11 вересня оперативна сумісність була піднесена з давнього занепокоєння до критичного національного пріоритету.

Одна з найбільших трагедій катастрофи 11 вересня сталася через неможливість ефективно передати попередження пожежно-рятувальному персоналу про те, що вежі ось-ось впадуть і що їм потрібно негайно евакуюватися. Багато експертів сходяться на думці, що ця нездатність радіосистеми пожежної служби ефективно зв'язуватися з іншими службами або навіть між новими та старими моделями радіостанцій, головною причиною смерті 343 пожежників.[74]

Використання взаємосумісних систем має ключове значення не тільки для того, щоб поліція та інші служби реагування (поліція, пожежно-рятувальні служби, служби швидкої допомоги) могли спілкуватися один з одним для координації дій, але й щоб вони могли оптимізувати ресурси для формування бюджету та планування на випадок стихійного лиха. зусилля з надання допомоги та відновлення.

---

[74] Основа взаємодії для екстреного зв'язку, Federal Signal, 2013. Доступно за адресою www.fedsig.com/sites/default/files/news/pdf/The%20bais%20of%20Interoperability%20for%20Emergency%20Communications.pdf.

Вміст 20

Взаємосумісність відповідно до Стратегії стійкості до хімічних, біологічних, радіологічних, ядерних і вибухових речовин: Канада

Канадська стратегія стійкості до хімічних, біологічних, радіологічних, ядерних і вибухових речовин визначає оперативну сумісність як операційну/функціональну або технічну природу.

«(1) Оперативна/функціональна сумісність – це здатність ефективно працювати разом. Зокрема, це здатність різних юрисдикцій або дисциплін надавати послуги та приймати послуги з інших юрисдикцій або дисциплін узгоджено, а також використовувати ці послуги для більш ефективної спільної роботи в надзвичайних ситуаціях. З практичної точки зору оперативна сумісність означає, що персонал з різних юрисдикцій або служб працює як команда в рамках спільної командно-контрольної структури.

«(2) Технічна сумісність – це здатність спілкуватися та обмінюватися інформацією, а також інтегрувати обладнання та технічні можливості. Це здатність систем забезпечувати динамічний інтерактивний обмін інформацією та даними між командними, контрольними та комунікаційними елементами для планування, координації, інтеграції та виконання операцій реагування».

5.5 Подолання культурних бар'єрів

Незважаючи на те, що впровадження взаємосумісних рішень і спрощених, інтегрованих процесів може значною мірою допомогти усунути ізоляції та сприяти міжвідомчій координації, факт залишається фактом: захист KI залежить від повсякденної роботи людей з найрізноманітнішими технічними та професійними навичками. фони. Різні погляди можуть ґрунтуватися на різних термінах, методологічних підходах і способах організації роботи.

Поділ на приватний і державний сектор пропонує типовий сценарій, коли діють різні уявлення щодо того, де має бути баланс між витратами на безпеку (наприклад, для підвищення стійкості KI) та впровадженням зручних для бізнесу заходів економії. Крім того, вплив культурних бар'єрів і неоднакового сприйняття також можна спостерігати у тих, хто працює в різних гілках одного уряду.

Досвід та уявлення держав-членів можуть суттєво відрізнятися залежно від конкретних інституційних, соціальних та економічних структур, у яких працюють представники різних професій. Без обов'язкової мети уніфікувати глибоко вкорінені стилі поведінки, кожна держава-член може побажати розвинути обізнаність щодо цих проблем і знайти способи (наприклад, шляхом відкритого та регулярного обговорення їх під час спільних навчальних заходів), щоб гарантувати, що вони врешті-решт не залишаться шлях постійних зусиль для досягнення стійкості KI.

ВИВЧЕННЯ ПРОБЛЕМИ 41
Дослідження культурних прогалин серед зацікавлених

Ступінь, до якої культурні розриви між зацікавленими сторонами КІ можуть перешкоджати досягненню оптимального рівня співпраці, було розглянуто з особливою увагою в Швеції в рамках загальносуспільного підходу країни до стійкості КІ та на більш загальному рівні, соціальна безпека. Відповідно, дослідження, присвячене стійкості до катастроф, виокремило низку професійних стосунків, пов'язаних із захистом КІ, і проаналізувало специфічні культурні проблеми, пов'язані з кожним із них. Дослідження підкреслює, наприклад, прогалини між фахівцями з безпеки та безпеки в тому, як ці дві групи керують інформацією. У той час як співробітники служби безпеки звикли працювати з секретною інформацією в обмеженому колу людей, співробітники служби безпеки, як правило, покладаються на відкриті джерела і не бачать ролі конфіденційної інформації. Тим не менш, «із ускладненням загроз, коли подію спочатку важко визначити як очевидну «звичайну» аварію або як терористичну атаку, потрібна міцна співпраця між, наприклад, поліцією та службами екстреного реагування. розроблені завчасно» (Lindberg and Sundelius 2013, p. 1301).

Хоча певні поведінкові прогалини можна виявити вздовж розриву між цивільним і військовим, дослідження визначає більш виражені перешкоди для координації між цивільним і цивільним, основна причина полягає в тому, що «ролі та обов'язки в складній цивільній сфері часто менш чіткі, а іноді навіть збігаються. Оскільки загрози розвиваються, правила та процедури можуть бути відсутні або застаріти. Лінії юрисдикції можна розглядати як додаткові або конкуруючі. Можна виявити певний опір координації, і одна з причин, ймовірно, полягає в тому, що взаємодії з метою зміни поведінки можуть бути дуже чутливими серед гордих професіоналів».

Джерело: www.semanticscholar.org/paper/Whole-of-Society-Disaster-Resilience-%3A-The-Swedish-Lindberg-Sundelius/9524aa4182828716ba- 5834c40ee6128f8674f54f.

6. Розширення міжнародного співробітництва для CIP

Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки,

...

8. Підтверджує, що ініціативи регіонального та двостороннього економічного співробітництва та розвитку відіграють життєво важливу роль у досягненні стабільності та процвітання, і у зв'язку з цим закликає всі держави посилити їхню співпрацю для захисту критично важливої інфраструктури, включаючи проекти регіонального зв'язку та пов'язану з ними мережу - прикордонна інфраструктура, від терористичних атак и відповідних випадках за допомогою двосторонніх та

6.1 Розміри міжнародного співробітництва з CIP

Однією з найбільш характерних тенденцій у сучасному глобальному ландшафті є інтернаціоналізація ланцюгів постачання, незалежно від того, чи йдеться про постачання критичних чи некритичних продуктів і послуг. Взаємозалежність і взаємозв'язок KI проходять через кордони. Ризики для KI держав-членів можуть однаково виникати в сусідніх країнах (особливо у випадку спільної фізичної інфраструктури) або дуже віддалених країнах (особливо у випадку кіберінфраструктури). У разі атаки на критичну інформаційну інфраструктуру (KII) криза, що розгортається в одній країні, може бути спланованою та пілотованою на території іншої країни..

Потенційні сценарії, що ілюструють необхідність міцного розміщення міжнародного співробітництва в стратегіях CIP держав-членів, включають наступне:

- Дві або більше держав-членів спільно використовують однакову інфраструктуру (транскордонні KI).
- Одна держава-член залежить, повністю або частково, від продуктів, послуг, технологій та

інших предметів, що постачаються CI, розташованими в іншій державі-члені.

Сучасні форми та рівні міжнародного співробітництва з CIP суттєво відрізняються між країнами. Вони можуть бути більш чи менш широкими за обсягом і сформульованими залежно від конкретного типу існуючих домовленостей, ступеня економічної інтеграції країни з іншими та інших факторів. Розглядаючи плани щодо нових або зміцнених міжнародних партнерств щодо CIP, держави-члени повинні зосередитися на кількох тематичних областях. У більшості випадків, коли міжнародне співробітництво щодо CIP здійснюється, вони зосереджені навколо питань обміну інформацією, управління кризою та спільних навчань.

Важливим аспектом обміну, пов'язаного з CIP, є міжнародна співпраця в цілях кримінального правосуддя. Оскільки резолюція Ради Безпеки 2341 (2017) вимагає встановлення кримінальної відповідальності за напади на CI, притягнення підозрюваних до відповідальності часто залежить від активізації державами-членами та використання ефективних каналів для міжнародного співробітництва у сфері кримінального правосуддя.

Вміст 21

Глобальна платформа INTERPOL для спілкування з правоохоронними органами

Глобальна цілодобова платформа INTERPOL I-24/7 з'єднує співробітників правоохоронних органів у всіх 195 країнах-членах INTERPOL і дозволяє авторизованим користувачам ділитися в безпечному середовищі конфіденційною та терміновою поліцейською інформацією зі своїми колегами по всьому світу, 24 годин на день, 365 днів на рік. I-24/7 — це мережа, яка надає доступ до різноманітних баз даних злочинців, які підтримує Інтерпол. Авторизовані користувачі можуть здійснювати пошук і перехресну перевірку даних за лічені секунди, маючи прямий доступ до баз даних на такі предмети, як підозрювані злочинці або особи, які розшукуються, викрадені та втрачені проїзні документи, викрадені автомобілі, відбитки пальців, профілі ДНК, викрадені адміністративні документи та викрадені твори мистецтва.

На національному рівні I-24/7 надається безпосередньо для національних центральних бюро та, за умови дозволу цих бюро, для великої кількості національних установ. У зв'язку з цим все більше членів Організації вирішили розширити доступ до ексклюзивної

ВИВЧЕННЯ ПРОБЛЕМИ 42

Міжнародний обмін інформацією про загрози у сфері цивільної авіації

В авіаційному секторі важливим аспектом обміну інформацією є обмін інформацією про загрози.

Посібник ICAO з авіаційної безпеки (Doc 8973-Restricted) рекомендує встановити лінії зв'язку, як офіційні, так і неофіційні, між посадовими особами авіаційної безпеки держав для сприяння швидкому обміну інформацією, включаючи будь-яке збільшення рівня загрози. Обмін інформацією про методи, які використовуються для спроб порушити безпеку, досвід роботи з обладнанням безпеки та оперативні практики також є надзвичайно корисним.

Офіційні процедури обміну інформацією між визначеними відповідальними посадовими особами, включаючи публікацію списку номерів телефонів, вуличних адрес, номерів телексу та факсу, а також адреси електронної пошти та адреси авіаційних фіксованих служб, мають бути доступними для зв'язку під час серйозного інциденту. Держави повинні розробити процедури для аналізу та розповсюдження інформації про загрози та забезпечити вжиття відповідних заходів операторами повітряних суден та аеропортів для протидії виявленій загрозі. Інформацію слід поширювати, коли вона потрібна особам для ефективного виконання своїх обов'язків, іншими словами, із застосуванням принципу «необхідно знати».

Держави з обмеженими ресурсами для боротьби з безпосередніми загрозами або актами незаконного втручання повинні розглянути можливість домовитися про правову та процедурну допомогу з суміжними державами, які краще оснащені для збору та поширення інформації про загрози та інциденти.

Запити держави про спеціальні заходи безпеки для конкретного рейсу слід задовольняти, коли це необхідно. Щоб гарантувати належну увагу таким запитам, держави повинні визначити процедури та представників уряду, повітряного судна та оператора аеропорту, які повинні знати інформацію про загрозу. Крім того, параметри спеціальних заходів безпеки, відповідальність за додаткові витрати та часові рамки для початку дії повинні бути узгоджені з відповідним оператором повітряного судна та аеропортами.

Терміновий зв'язок може бути полегшений за допомогою мережі контактних пунктів авіаційної безпеки ICAO, створеної для повідомлення про неминучі загрози для операцій цивільного повітряного транспорту, відповідно до поглядів, висловлених Групою восьми Ліон-Рома по боротьбі зі злочинністю та тероризмом. Відповідно до резолюції Асамблеї A39-18: «Консолідована заява про безперервну політику ICAO, пов'язану з авіаційною безпекою», держави, які ще не зробили цього, закликаються брати участь у Мережі контактних осіб ICAO з питань авіаційної безпеки. Метою Мережі є надання інформації

про міжнародні контакти з питань авіаційної безпеки в кожній державі, які призначені відповідним органом для надсилання та отримання повідомлень у будь-який час дня чи ночі щодо інформації про безпосередню загрозу, термінових запитів безпеки природи та вказівок щодо підтримки вимог безпеки, щоб протистояти неминучій загрозі. Контактні особи повинні бути доступними в будь-який час, брати участь у процесі оцінки загроз і бути близькими до процесу прийняття рішень щодо процедур авіаційної безпеки.

Джерело: ICAO, *Керівництво з авіаційної безпеки*, Doc 8973-Restricted.

6.2 Основні транскордонні ініціативи

Протягом останніх кількох років підвищення обізнаності про взаємозалежність КІ та їх транскордонні наслідки спричинило прийняття ряду міжнародних угод і партнерств. З огляду на економічну вагу залучених країн і наявність у них спільних мереж надзвичайно складної інфраструктури, у цьому розділі розглядається структура, що з'єднує країни-члени Європейського Союзу та домовленості про співпрацю між Сполученими Штатами та Канадою в цій галузі. Він також розглядає останній досвід та ініціативи, реалізовані скандинавськими країнами.

6.2.1 Європейський Союз

Поточний загальноєвропейський підхід до CIP закріплено в Директиві 2008 року, яка вводить поняття «європейська критична інфраструктура» (іменована в Союзі «ECI») як «критична інфраструктура, розташована в державах-членах, порушення або знищення що мало б значний вплив принаймні на дві держави-члени»[75]. Сфера застосування Директиви 2008 року обмежена енергетичним і транспортним секторами. Крім того, він призначений для доповнення, а не для заміни існуючих галузевих заходів, прийнятих на рівні ЄС або окремими державами-членами.

Процес призначення для європейської критичної інфраструктури включає різні кроки, які вимагають від держав-членів Європейського Союзу:

- Інформувати інші держави-члени про потенційну європейську критичну інфраструктуру, розташовану на їхній території та впливаючи на них, і залучати їх до двосторонніх або багатосторонніх обговорень.
- Призначити таку інфраструктуру як європейську критичну інфраструктуру після погодження з залученими державами-членами.
- Щороку інформувати Європейську комісію про кількість визначених об'єктів європейської критичної інфраструктури на сектор та кількість держав-членів, залежних від кожного призначеного об'єкта європейської критичної інфраструктури.
- Інформувати зацікавлених власників та операторів про те, що їхню інфраструктуру визначено як європейську критичну інфраструктуру.
- Переконайтеся, що визначені європейські об'єкти критичної інфраструктури мають план безпеки оператора та що цей план регулярно переглядається.

Переконайтеся, що кожен європейський об'єкт критичної інфраструктури призначає офіцера зв'язку з безпеки, який буде координувати роботу між європейською критичною інфраструктурою та відповідним національним органом.

- Провести оцінку загрози щодо підсекторів європейської КІ протягом одного року після визначення критичної інфраструктури на своїй території як європейської критичної інфраструктури в цих підсекторах.
- Звітувати зведені дані кожні два роки до Європейської комісії щодо типів ризиків, загроз і вразливостей, які виникли для кожного сектору об'єктів європейської критичної інфраструктури, у межах якого така інфраструктура була визначена.
- Призначити «Контактний пункт із захисту критичної європейської інфраструктури» для координації питань захисту європейської КІ всередині країни, по відношенню до інших держав-членів та Європейської Комісії.

У 2013 році оцінка стану виконання Директиви 2008 року виявила змішаний сценарій. Незважаючи на те, що держави-члени чітко продовжували усвідомлювати важливість створення пов'язаної з CIP рамки для всього Європейського Союзу, було виділено низку проблем. Зокрема, було зазначено, що «менше 20 європейських CI [було призначено] і, отже, було створено дуже мало нових планів безпеки операторів.

---

[75] Директива Ради 2008/114 від 8 грудня 2008 року про ідентифікацію та визначення європейських критичних інфраструктур та оцінку потреби у покращенні їх захисту. Доступний на https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG.

Деякі чіткі КІ європейського виміру, такі як основні мережі передачі енергії, [не були] включені. Незважаючи на сприяння розвитку європейської співпраці в процесі CIP, Директива в основному заохочувала двосторонню співпрацю держав-членів замість справжнього європейського форуму для співпраці. Орієнтований на галузь підхід Директиви також є проблемою для низки держав-членів, оскільки на практиці аналіз критичних моментів не обмежується галузевими межами та дотримується скоріше «системного» або «сервісного» підходу (наприклад, лікарні, фінансові послуги)[76]».

Ґрунтуючись на результатах своєї оцінки, у 2013 році Європейська комісія розпочала процес переорієнтації дій CIP у масштабах Європейського Союзу шляхом вивчення нового, більш практичного підходу, який суттєво змінить секторну модель до системної. Необхідність змін була додатково підтверджена оцінкою Директиви 2008 року, проведеною у 2019 році, яка підкреслила, як існуючі європейські та національні заходи стикаються з обмеженнями в допомозі операторам протистояти операційним викликам, з якими вони зараз стикаються, і вразливостям, які тягне за собою їх взаємозалежний характер.[77]

У 2020 році новий підхід був викристалізований у пропозиції Комісії Європейського Союзу щодо директиви щодо стійкості критично важливих об'єктів.[78] Пропозиція повторює необхідність фундаментального переходу від захисту конкретних активів до посилення стійкості критично важливих організацій, які ними керують. Таким чином, він відображає концепцію «стійкого оператора», закріплену в Порядку денному Європейського Союзу з боротьби з тероризмом на 2020 рік.[79]

Вміст 22

Від захисту критичних активів до стійкості системи: нова парадигма Комісії ЄС

Пропозиція Комісії Європейського Союзу 2020 року щодо нової директиви щодо стійкості критично важливих об'єктів відображає пріоритети Стратегії Комісії щодо Союзу безпеки Європейського Союзу. Останнє вимагає перегляду підходу до стійкості критичної інфраструктури, який краще відповідає поточному та очікуваному майбутньому ландшафту ризиків, постійно тісній взаємозалежності як між критичними секторами, так і між фізичною та цифровою інфраструктурою.

Запропонований інструмент розроблено для заміни Директиви 2008/114 *про європейську критичну інфраструктуру, яка стосується лише енергетичного та транспортного секторів, зосереджена виключно на захисних заходах і забезпечує процедуру ідентифікації та призначення європейської критичної інфраструктури через транскордонний діалог. Відступаючи від існуючого підходу, запропонована директива*:

- Має ширшу сферу застосування, оскільки охоплює десять критичних секторів, а саме енергетику, транспорт, банківську справу, інфраструктуру фінансового ринку, охорону здоров'я, питну воду, стічні води, цифрову інфраструктуру, державне управління та космос.
- Встановлює процедуру для держав-членів ідентифікації критичних об'єктів за допомогою спільних критеріїв на основі національної оцінки ризику.

- Встановлює конкретні зобов'язання для держав-членів та визначених критично важливих суб'єктів, у тому числі тих, що мають особливе європейське значення, а саме критично важливі суб'єкти, які надають основні послуги більш ніж одній третині держав-членів, які підлягатимуть спеціальному нагляду.

Комісія також передбачає підтримку як компетентних органів, так і критично важливих суб'єктів у їхніх зусиллях щодо дотримання своїх зобов'язань згідно з директивою. Крім того, очікується, що група експертів Комісії - надаватиме консультації Комісії та сприятиме стратегічній співпраці та обміну інформацією. Нарешті, запропонована директива передбачає можливість співпраці з країнами-партнерами, наприклад, у сфері оцінки ризиків..

Джерело: https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_ en.pdf.

---

[76] *Робочий документ щодо нового підходу до Європейської програми захисту критичної інфраструктури, Європейська комісія, 2013 р. Доступно за адресою: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.*

[77] *Дивіться https://ec.europa.eu/home-affairs/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf.*

[78] *Дивіться https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0829&from=EN. In December 2021, the Council approved a general approach on the new draft directive.*

[79] *Дивіться https://ec.europa.eu/home-affairs/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.*

ВИВЧЕННЯ ПРОБЛЕМИ 43
AIRPOL and RAILPOL

Транскордонне співробітництво щодо захисту КІ в європейських країнах не обмежується рамками, встановленими Директивою 2008 року. Це також відбувається на форумах, які, хоч і не присвячені спеціально захисту КІ, відіграють важливу роль у досягненні цієї мети. Транспортний сектор, завдяки діяльності AIRPOL і RAILPOL, пропонує два відповідні приклади.

Створена в 2011 році авіаційна мережа, відома як «AIRPOL», є координаційним органом підрозділів правоохоронних органів в європейських аеропортах. Його місія полягає в тому, щоб підвищити загальну безпеку в сфері цивільної авіації:

- Оптимізація ефективності та результативності правоохоронних і прикордонних питань, пов'язаних з аеропортами та авіацією.
- Сприяння більш узгодженому підходу до правозастосування в цій сфері.

AIRPOL працює навколо трьох результатів:

- Розробка постійної та функціональної мережі, зосередженої на обміні передовим досвідом, розвідкою, загальною інформацією та обміні персоналом у майбутньому в кількох сферах.
- Координація транскордонних дій із високим ступенем впливу.

Встановлення дорадчої ролі як представницького органу експертів.

Аналогічний орган у залізничному секторі, відомий як «RAILPOL», є міжнародною мережею організацій, відповідальних за контроль залізниць у державах-членах Європейського Союзу. Його мета полягає в посиленні та інтенсифікації міжнародного співробітництва залізничної поліції в Європі, щоб запобігати загрозам і гарантувати ефективність заходів проти транскордонної злочинності. RAILPOL складається з представників організацій, відповідальних за виконання обов'язків

6.2.2 Канадсько-американське співробітництво

Мало того, що канадсько-американський кордон є найдовшим у світі, понад 90% населення Канади проживає в межах 160 км від цього кордону. Крім того, поблизу кордону розташовано кілька нафтопереробних заводів, атомних електростанцій, великих виробничих потужностей та інших критичних об'єктів. Основним наслідком є наявність великої кількості залежностей і транскордонних КІ, захист яких у вирішальній мірі залежить від ініціатив двосторонньої співпраці.

Основним інструментом транскордонного співробітництва щодо CIP є Канадсько-Сполучені Штати дій 2010 року[80]. Хоча План базується на існуючих галузевих угодах про співпрацю між двома країнами, стимул для інтегрованого підходу в основному випливає з:

- *Необхідність підтримки тісної співпраці приватного сектору через кордон*
- *Необхідність уникати дублювання зусиль, яке є неминучим при суто галузевих підходах*
- *Необхідність підвищити своєчасність і точність спілкування з зацікавленими сторонами КІ як усередині країни, так і за кордоном*

План дій між Канадою та Сполученими Штатами побудовано навколо трьох цілей: партнерство для забезпечення стійкості критичної інфраструктури КІ; обмін інформацією; та управління ризиками, як зазначено нижче.

6.2.2.1 Партнерство для забезпечення стійкості критичної інфраструктури

Методологія, яка використовується для досягнення цієї мети, полягає у використанні існуючих організаційних і партнерських структур. До такої структури входить Консультативна група з управління надзвичайними ситуаціями, створена відповідно до Угоди між Канадою та Сполученими Штатами Америки про співробітництво у надзвичайних ситуаціях 2008 року для забезпечення централізованого нагляду за підтримкою спільного управління надзвичайних ситуацій.

80 Дивіться www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.

Одна з робочих груп, створених у рамках Консультативної групи, займається конкретно КІ, і її функція була визначена як забезпечення напряму та безперервності для підтримки Плану дій Канада-Сполучені Штати.

Відповідно до цієї мети План дій також передбачає надання механізмів і можливостей для секторальних і урядових координаційних рад Сполучених Штатів Америки та галузевих мереж Канади для спільної роботи над покращенням міжгалузевої транскордонної співпраці. Крім того, План дій створив віртуальну комірку аналізу ризиків критичної інфраструктури Канади та Сполучених Штатів для розробки та виробництва спільних аналітичних продуктів транскордонного застосування.

6.2.2.2 Обмін інформацією

У рамках цієї мети дві країни зобов'язалися працювати разом, щоб:

- Розробити сумісні механізми та протоколи для захисту та обміну конфіденційною критичною інформацією про інфраструктуру
- Визначити вимоги до інформації державного та приватного секторів для підтримки розробки цінних аналітичних продуктів
- Забезпечити ефективний обмін інформацією під час і після інциденту, що впливає на КІ

6.2.2.3 Управління ризиками

Відповідно до Плану дій, управління ризиками КІ зобов'язує дві країни працювати разом для оцінки ризиків і розробки планів для вирішення пріоритетних сфер. Підзаходи будуть визначені після ретельного аналізу пріоритетів кожної країни з урахуванням ризиків та визначення сфер спільного інтересу.

Вміст 23
Управління кордоном під час та після надзвичайної ситуації: Канада та США

Укладений Департаментом громадської безпеки та готовності до надзвичайних ситуацій Канади (відомий як «Громадська безпека Канади») і Департаментом внутрішньої безпеки США, рамки застосовуються до інцидентів, включаючи, але не обмежуючись терористичними нападами, які суттєво впливають на кордон між дві країни. Рамкова програма розроблена для доповнення існуючих ініціатив шляхом сприяння скоординованому, спільному та своєчасному прийняттю рішень щодо управління кордоном для пом'якшення впливу на людей та економіку.

Передбачені заходи включають:

- *Зв'язок: дві країни зобов'язуються спілкуватися одна з одною якомога швидше та підтримувати зв'язок між офіційними особами до відновлення роботи на кордоні. Вони також зобов'язуються обмінюватися інформацією про природу інциденту, повідомляти про ті товари та людей, які вважаються національним пріоритетом однієї або обох країн, і сприяти спільному обміну повідомленнями з секторами критичної інфраструктури, посадовими особами охорони здоров'я, торгівлею та широкою громадськістю..*

6.2.3 Ініціативи співпраці північних країн

За останні кілька років у країнах Північної Європи зростає кількість ініціатив, спрямованих на транскордонний вимір CIP. Серед них Північне співробітництво з управління надзвичайними ситуаціями є яскравим прикладом такого роду субрегіональних ініціатив. Так звану «посилену версію» цієї операційної платформи було узгоджено в 2009 році та об'єднало Данію, Фінляндію, Ісландію, Норвегію та Швецію. Ініціатива структурована навколо серії робочих груп, які щорічно звітують перед компетентними міністрами. У 2011 році була створена нова робоча група для розгляду вразливостей і перспектив спільної оперативної готовності в кіберсфері.[81]

[81] *Дивіться* www.msb.se/en/about-msb/international-co-operation/nordic-co-operations/.

Зокрема, на період 2019–2021 рр. міністри країн Північної Європи, відповідальні за цивільний захист і готовність, визначили низку пріоритетних напрямків співпраці між країнами-учасницями, у т.ч.:

- *Північне співробітництво щодо хімічних, біологічних, радіологічних, ядерних речовин і вибухових речовин високої потужності (іменованих «речовинами CBRNE»): метою є запобігання, виявлення та вирішення інцидентів, пов'язаних із речовинами CBRNE, шляхом виділення ресурсів для ліквідації серйозних аварій, забезпечити доступ до досвіду та співпрацювати з іншими секторами. Спільні навчання є невід'ємним компонентом робочої програми, бажано як частину навчань, передбачених Механізмом цивільного захисту ЄС.*
- *Північне співробітництво у сфері зв'язку в екстрених ситуаціях: у той час як Норвегія (через свою мережу екстреного зв'язку), Швеція (через національну систему цифрового зв'язку Rakel) і Фінляндія (через мережу громадської безпеки Virve) наразі взаємопов'язані, що забезпечує ефективний зв'язок і співпрацю через національні кордони, досліджується, як користувачі інших скандинавських наземних транкінгових радіосистем (TETRA)[82] – у Данії (Sine) та Ісландії – також можуть сприяти надійному та необмеженому реагуванню на надзвичайні ситуації та екстреним викликам.*

ВИВЧЕННЯ ПРОБЛЕМИ 44
Норвезько-шведський проект міжсистемного інтерфейсу

Норвезько-шведський проект міжсистемного інтерфейсу, відомий як «проект ISI», був схемою між Норвегією та Швецією, спрямованою на сприяння транскордонному командуванню та співпраці шляхом створення можливостей для зацікавлених сторін в обох країнах використовувати власне обладнання в рамках Nødnett (норвезька мережа громадської безпеки) і Rakel (шведська мережа екстреного зв'язку). Проект здійснювався з 2013 по 2016 рік і залучав норвезьких і шведських представників рятувальних служб, поліції, охорони здоров'я та швидкої допомоги, які працювали у трьох робочих групах. Паралельно з робочими групами проекту також була створена група розвитку технологій.

Проект здійснювався урядовими установами Норвегії та Швеції, відповідальними за розробку та експлуатацію систем екстреного зв'язку у відповідних країнах. Motorola Systems і Airbus були партнерами по співпраці, відповідальними за необхідні технологічні розробки. Одним із факторів успіху проекту стала його рання зосередженість на комунікаційних проблемах, які різні категорії користувачів відчувають у своїй повсякденній роботі в прикордонних районах двох країн. Результатом проекту стало:

- Пропозиція (проект) юридично обґрунтованого договору
- Методологія командування та співпраці
- Структура спілкування в чат-групах
- Загальна термінологія
- Правила використання технічного обладнання
- Навчання для користувачів і осіб, які приймають рішення
- Підсумкова основна вправа, де весь міжсистемний інтерфейс був перевірений у реальній ситуації

Джерело: www.msb.se/siteassets/dokument/publikationer/english-publications/a-quick-guide-to-the-norwegian-swedish-isi-project-a-cross- border-development-scheme.pdf.

---

[82] TETRA є відкритим стандартом сухопутного мобільного радіозв'язку для технології цифрового транкінгового радіозв'язку. Стандарт, розроблений експертами галузі громадської безпеки та двостороннього радіозв'язку спільно з Європейським інститутом телекомунікаційних стандартів, гарантує, що пристрої TETRA разом із мережевою інфраструктурою забезпечать безпечну, надійну та миттєву передачу голосу та даних у критичних місіях і операціях..

6.3 Транскордонна технічна допомога, допомога з розбудови потенціалу та фінансова допомога

Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки,

...

9. Наполегливо закликає держави, здатні це зробити, сприяти забезпеченню ефективного та цілеспрямованого розвитку потенціалу, навчанню та іншим необхідним ресурсам, технічній допомозі, передачі технологій і програмам, де це необхідно, щоб дозволити всім державам досягти мети захисту критичної інфраструктури від терористичні атаки

Додаток до Мадридських керівних принципів

У своїх подальших зусиллях щодо захисту критичної інфраструктури та «м'яких» цілей від

CIP – це не тільки ресурсозатратна робота на різних етапах і вимірах; це також вимагає мобілізації високого рівня досвіду в кількох сферах. Хоча CIP має бути пріоритетним питанням для всіх держав-членів, необхідні ресурси та міждисциплінарні навички доступні не в усіх із них. Як на галузевому, так і міжсекторальному рівні зростає усвідомлення потреби в цільовій технічній допомозі та розбудові потенціалу в цій сфері. У сфері цивільної авіації, наприклад, ICAO закликає держави з обмеженими ресурсами для боротьби з неминучою загрозою «розглянути можливість домовитися про юридичну та процедурну допомогу з сусідніми державами, які краще обладнані для збору та поширення інформації про загрози».[83]

[8] ICAO Aviation Security Manual (Doc 8973-

Вміст 24
Регіональні зусилля щодо захисту критичної інфраструктури: ініціатива OSCE та OAS

OSCE

Організація з безпеки та співробітництва в Європі (ОБСЄ) є найбільшою регіональною організацією у світі, до складу якої входять 57 держав. ОБСЄ дотримується комплексного підходу до безпеки, який охоплює політичні та військові, економічні та екологічні, а також людські аспекти. Таким чином, він розглядає широкий спектр проблем, пов'язаних з безпекою, включаючи контроль над озброєннями, заходи зі зміцнення довіри та безпеки, права людини, національні меншини, демократизацію, поліцейські стратегії, боротьбу з тероризмом, економічну та екологічну діяльність. Усі 57 держав-учасниць мають рівний статус, а рішення приймаються консенсусом на політично обов'язковій основі.

Відповідно до вказівок держав-учасниць, ОБСЄ має історію захисту критичної інфраструктури, починаючи з 2007 року з рішення Ради міністрів № 6/07[84] щодо захисту критичної енергетичної інфраструктури від терористичних атак. У тому ж році рішення Ради міністрів № 5/07[85] підкреслило роль державно-приватного партнерства в протидії тероризму, включаючи конкретне посилання на захист критичної інфраструктури. Країни-учасниці ОБСЄ розширили сферу діяльності організації щодо критичної інфраструктури до міжнародного транспорту та інших критичних секторів через Консолідовану рамкову програму ОБСЄ 2012 року для боротьби з тероризмом.[86] З 2007 року ОБСЄ підтримує своїх держав-учасниць шляхом розбудови потенціалу та технічних допомога, включно з підготовкою керівних матеріалів, таких як «Посібник із захисту критичної неядерної енергетичної інфраструктури від терористичних атак» 2013 року з упором на загрози, що виходять із кіберпростору[87] та – за межами сфери тероризму – Посібник із захисту електричних мереж від стихійних лих 2016 року.[88] У 2021 році ОБСЄ відкрила свій Віртуальний центр із захисту критично важливої енергетичної інфраструктури, який включає навчальні курси та інші матеріали для держав-учасниць.[89] У інших сферах, окрім тероризму, з 2013 року країни-учасниці ОБСЄ прийняли 16 кібер- та ІКТ-безпеки. заходи щодо створення (іменовані «СВМ»):[90] СВМ № 15 зосереджується саме на співпраці між державними органами, відповідальними за безпеку критичної інфраструктури, включаючи обмін передовим досвідом, обмін інформацією про загрози ІКТ та підвищення безпеки національних і транснаціональних ІКТ-включена КІ.

Як організація, заснована відповідно до розділу VIII *Статуту ООН, ОБСЄ також підтримує виконання ключових документів Організації Об'єднаних Націй, які стосуються критичної інфраструктури та захисту легких цілей, включаючи резолюції Ради Безпеки* 1540 (2004), 2396 (2017), 2341. (2017) *та Глобальна стратегія боротьби з тероризмом ООН.*

OAS

В рамках Організації американських держав (OAS), *Секретаріат багатовимірної безпеки наразі надає технічну підтримку державам-членам у процесі розробки моделі регіональної стратегії захисту КІ від усіх небезпек, включаючи стихійні лиха.*

Ініціатива реалізується через Міжамериканський комітет проти тероризму та Секретаріат інтегрального розвитку та за підтримки уряду Сполучених Штатів, зокрема Місії Сполучених Штатів в OAS, CISA *та Інженерного корпусу армії.*

Розробкою регіональної стратегії OAS *прагне*:

- Допомагати своїм державам-членам в управлінні, експлуатації, обслуговуванні та модернізації систем критичної інфраструктури проти всіх небезпек
- Створити регіональну спільноту експертів у цій галузі.

Джерело: *Представники* OSCE *та* OAS.

[84] *Дивіться* www.osce.org/mc/29482.

[85] *Дивіться* www.osce.org/mc/29569.

[86] Дивіться www.osce.org/pc/98008.

[87] Дивіться www.osce.org/files/f/documents/7/5/103954.pdf.

[88] Дивіться www.osce.org/files/f/documents/a/d/242651.pdf.

[89] Дивіться www.osce.org/secretariat/443674.

[90] Рішення Постійної ради ОБСЄ 1202: www.osce.org/pc/227281 схвалений Радою міністрів: www.osce.org/cio/288086.

[8] ICAO Aviation Security Manual (Doc 8973-

Держави-члени також можуть передбачити надання допомоги іншим, хто її потребує, на етапі планування для підвищення стійкості КІ. Це може мати форму передачі знань або ноу-хау щодо різних циклів CIP, від оцінки ризику до створення належної структури управління.

Відповідно до цього, Meridian Process висунув пропозицію, за якою країнам «з менш розвиненою політикою та діяльністю можуть бути запропоновані ресурси та знання, і вони можуть дізнатися від [країн-керівників або партнерів] про цінні організаційні чи процесні підходи та про пастки. уникати. Таким чином, їхня подорож CIIP може бути швидшою, ніж подорож самотужки... Пропозиція бути нацією-гідом, коли нація випереджає інші країни на шляху CIIP, також приносить користь. Країна-консультант може поставити питання CIIP, які країна-провідник ще не розглянула. Крім того, посилений CIIP у країні-друзі створює безпечніший вузол CII у кіберпросторі. У той же час країни-керівники повинні переконатися, що вся необхідна координація та дозвіл були здійснені з відповідними міністерствами та відомствами в їхніх країнах, перш ніж звертатися до потенційного партнера. Однак можна почати з неформальних дружніх обговорень, щоб встановити сумісність і взаємні інтереси, перш ніж кожна нація вирішить розвинути більш офіційні дружні стосунки».[91]

ВИВЧЕННЯ ПРОБЛЕМИ 45
Механізм цивільного захисту Європейського Союзу

Заснований у жовтні 2001 року Механізм цивільного захисту Європейського Союзу спрямований на зміцнення співпраці між державами-членами Європейського Союзу та шістьма країнами-учасницями щодо цивільного захисту з метою покращення запобігання, готовності та реагування на катастрофи.

Коли надзвичайна ситуація переважає можливості реагування окремої країни, вона може звернутися за допомогою через Механізм. За запитом Координаційний центр реагування на надзвичайні ситуації мобілізує допомогу чи експертів. Центр цілодобово стежить за подіями по всьому світу та забезпечує швидке розгортання екстреної підтримки через прямий зв'язок із національними органами цивільного захисту. Спеціалізовані групи та обладнання, такі як пошуково-рятувальні та медичні групи, можуть бути мобілізовані в короткий термін для розгортання в Європі та за її межами. Європейська Комісія відіграє ключову роль у координації реагування на стихійні лиха, беручи участь у щонайменше 75% транспортних та експлуатаційних витрат на розгортання.

Інструмент 26
Будівельні блоки кібербезпеки енергетичного сектора – USAID

https://resilient-energy.org/cybersecurity-resilience

Розроблений у рамках партнерства між Агентством США з міжнародного розвитку (USAID) і Національною лабораторією відновлюваної енергії, цей інструмент розроблений, щоб допомогти різним зацікавленим сторонам у країнах, які надає допомогу USAID, покращити безпеку електричної мережі

[91] Посібник із належної практики GFCE-Meridian із захисту критично важливої інформаційної інфраструктури для урядовців, GFCE-Meridian, 2016 р. Доступно за адресою www. meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

7. Секторальні міжнародні ініціативи

У цій главі наведено огляд ключових ініціатив, здійснених установами системи ООН у вибраній кількості секторів КІ. Ані перелік секторів, ані описані ініціативи не мають на меті бути вичерпними. Скоріше мета полягає в тому, щоб скерувати читачів до ресурсів та інструментів, які могли б допомогти їм у розробці надійних галузевих планів CIP у контексті більш широких національних стратегій.

7.1 Морський сектор

Будучи провідною міжнародною агенцією у цій сфері, Міжнародна морська організація (ІМО) займається питаннями захисту КІ, в тому числі від терористичних атак, у рамках своїх ініціатив щодо безпеки цивільної морської галузі. Це стосується як сектору судноплавства, так і порту. Що стосується останніх, зокрема, «хоча багато країн розглядають ... порти як критично важливу інфраструктуру, без чіткого національного та місцевого законодавства, політики та вказівок, які координують усі ці дії, заходи безпеки [є], у кращому випадку, розрізненими. Важливим для успіху режимів безпеки портів і портових засобів — як для протидії крадіжкам, так і для запобігання доступу терористів до суден — [є] добре скоординована превентивна стратегія, заснована на оцінці ризику».[92] Як заявив представник ІМО в Раді Безпеки. на нараді, щоб вирішити ці проблеми, «ІМО [розробила] ряд посібників, інструментів самооцінки та навчальних матеріалів для захисту портів, суден і морських установок. У міру розвитку загроз фокус ІМО на реагуванні на протидію тероризму був замінений наголосом на проактивних заходах... Те, що безпека на морі та забезпечення правопорядку на морі розглядалися як відомчі питання — для флоту, берегової охорони чи поліції — а не для багатьох - головною перешкодою було агентство, оскільки ці агентства часто конкурували за обмежені ресурси». Зокрема, Інтегрована програма технічного співробітництва ІМО у сфері глобальної безпеки на морі спирається на подвійні принципи технічної допомоги та нарощування потенціалу для підтримки країн у їхніх зусиллях щодо оцінки та усунення загроз їхнім морським кордонам і торговим потокам. Сюди входять нові загрози, такі як кібератаки. Збільшуючи

здатність країн дотримуватись договорів і стандартів, пов'язаних із безпекою на морі, ІМО підтримує підхід, заснований на міжвідомчому співробітництві. Наскільки це можливо, діяльність Програми здійснюється в тісній співпраці з регіональними організаціями та організаціями Організації Об'єднаних Націй, які поділяють з ІМО ту саму широку мету зміцнення глобальної морської безпеки. Це включає участь ІМО у спільних оцінках країни, які проводяться під егідою Контртерористичного комітету Ради Безпеки.[93]

Визнаючи необхідність більш цілісного підходу, Інтегрована програма технічного співробітництва ІМО також почала націлюватися на стратегічний рівень шляхом підтримки розробки національних стратегій морської безпеки, національних комітетів морської безпеки, національних реєстрів ризиків морської безпеки та інших подібних матеріалів. Стратегічний вимір у поєднанні з оперативною підтримкою має на меті забезпечити загальнодержавний підхід до безпеки на морі, уникаючи менталітету ізоляції та максимізуючи всі державні ресурси для боротьби з різними ризиками для безпеки на морі.

У цьому контексті ключовою структурою є Кодекс ISPS. Кодекс складається з двох розділів. Частина А є обов'язковою та містить детальні вимоги щодо безпеки на морі та в портах, яких повинні дотримуватися сторони Конвенції SOLAS, портові органи та судноплавні компанії.

---

[92] Заява представника ІМО «Рада Безпеки закликає держави-члени усунути загрози критичній інфраструктурі, одноголосно ухваливши резолюцію 2341 (2017)», Рада Безпеки, 7782-е засідання, 13 лютого 2017 р. Доступно за адресою: www.un.org/press/en/2017/sc12714.doc.htm.

[93] Див. ІМО, Інтегрована програма технічного співробітництва (ITCP). Доступний на www.imo.org/en/OurWork/TechnicalCooperation/Pages/ITCP.aspx.

Частина B надає серію необов'язкових вказівок щодо того, як виконати вимоги та зобов'язання, викладені в частині A. Цілі Кодексу ISPS такі:[94]

- Створити міжнародну структуру, яка сприятиме співпраці між державними установами, місцевими адміністраціями та судноплавством і портовою галуззю в оцінюванні та виявленні потенційних загроз безпеці для суден або портових засобів, що використовуються для міжнародної торгівлі, з метою впровадження превентивних заходів безпеки проти таких загроз.
- Визначити відповідні ролі та відповідальність усіх сторін, зацікавлених у забезпеченні морської безпеки в портах і на борту суден, на національному, регіональному та міжнародному рівнях.

  Забезпечити завчасне та ефективне зіставлення та обмін інформацією, пов'язаною з морською безпекою, на національному та регіональному рівнях і міжнародному рівнях.
- Надати методологію для оцінки безпеки суден і портів, яка полегшує розробку планів і процедур безпеки суден, компаній і портових засобів, які будуть використовуватися для реагування на різні рівні безпеки суден або портів.
- Забезпечити адекватні та пропорційні заходи безпеки на морі на борту суден і в портах.

Для управління потенційними загрозами безпеці Кодекс ISPS вимагає, щоб країни, портові органи та судноплавні компанії призначали відповідно офіцерів охорони портових засобів, офіцерів охорони суден та офіцерів безпеки компаній. Вони відповідають за розробку та реалізацію конкретних планів безпеки.

7.2 Сектор авіації

ICAO є спеціалізованою установою ООН, заснованою державами в 1944 році для управління та управління Конвенцією про міжнародну цивільну авіацію (Чиказька конвенція).[95]

ICAO співпрацює зі 193 сторонами Чиказької конвенції, а також з галузевими групами, щоб досягти консенсусу щодо міжнародних стандартів цивільної авіації та рекомендованих практик (іменованих в ICAO «SARPS») і політики на підтримку безпечного, ефективного, захищеного, економічно стійкий та екологічно відповідальний сектор цивільної авіації. Ці SARPS і політика використовуються державами-членами ICAO для забезпечення того, щоб їхні місцеві операції та правила цивільної авіації відповідали глобальним нормам, що, у свою чергу, дозволяє безпечно, безпечно та надійно виконувати понад 100 000 рейсів у глобальній авіаційній мережі в кожному регіоні світ.

На додаток до своєї основної роботи, пов'язаної з досягненням консенсусних міжнародних SARPS і політики між державами-членами та в галузі, а також серед багатьох інших пріоритетів і програм, ICAO також координує допомогу та розбудову потенціалу держав для підтримки численних цілей розвитку авіації; розробляє глобальні плани для координації багатостороннього стратегічного прогресу в галузі безпеки та аеронавігації; здійснює моніторинг і звітує про численні показники ефективності сектора повітряного транспорту; і перевіряє можливості держав щодо нагляду за цивільною авіацією у сферах безпеки та безпеки.

Що стосується стратегічної мети ICAO щодо авіаційної безпеки та сприяння, то вона в основному здійснюється за допомогою наступних заходів:

- Встановлення стандартів і рекомендованої практики для міжнародної цивільної авіації у сфері безпеки, сприяння, ідентифікації та управління кордонами.
- Постійний аудит і моніторинг ефективності авіаційної безпеки держав-членів з метою посилення їхніх спроможностей щодо відповідності вимогам авіаційної безпеки та нагляду.

---

[94] Див. IMO, Безпека на морі та піратство. Доступний на www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx.

[95] документ ICAO 7300/9; див. також United Nations, Treaty Series, том. 15, № 102.

- Надання допомоги у нарощуванні потенціалу та навчання з метою покращення можливостей держав у сфері авіаційної безпеки та спрощення.

Робота ICAO в цьому секторі закріплена в ряді договорів з авіаційної безпеки. Вони були прийняті протягом більш ніж п'ятдесяти років і зазвичай розглядаються як невід'ємна частина універсальної правової бази проти тероризму:

1963 Конвенція про злочини та, що вчиняються на борту повітряних суден
1970 Конвенція про боротьбу з незаконним захопленням повітряних суден
1971 Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації
1988 Протокол про боротьбу з незаконними актами насильства в аеропортах, що обслуговують міжнародну цивільну авіацію
1991 Конвенція про маркування пластичних вибухових речовин з метою їх виявлення
2009 Монреальська конвенція про відшкодування шкоди третім особам внаслідок актів незаконного втручання за участю повітряних суден
2010 Конвенція про боротьбу з незаконними актами, що стосуються міжнародної цивільної авіації
2010 Додатковий протокол до Конвенції про боротьбу з незаконним захопленням повітряних суден
2014 Протокол про внесення змін до Конвенції про правопорушення та деякі інші дії, вчинені на борту повітряних суден

Глобальний план авіаційної безпеки є основоположним довідковим документом для держав, промисловості, зацікавлених сторін та ICAO для спільної роботи над спільною метою підвищення авіаційної безпеки в усьому світі. Схвалений у 2017 році Радою ICAO План містить п'ять пріоритетних результатів:

- Підвищення обізнаності про ризики та реагування.
- Розвивиток культури безпеки та людських здібностей.
- Удосконалення технологічних ресурсів та сприяння інноваціям.
- Покращення нагляду і гарантії якості.
- Збільшення співпраці та підтримки.

Фундаментальним інструментом є Посібник з авіаційної безпеки (Doc 8973, Restricted),[96] який призначений для допомоги державам у впровадженні стандартів і рекомендованих практик, включених до додатку 17[97] – Авіаційна безпека – до Чиказької конвенції. Остання версія Посібника, тринадцяте видання, опубліковане наприкінці 2022 року, містить новий та оновлений посібник.

Особливий інтерес для CIP представляють найкращі практики, пов'язані з безпекою наземних територій аеропортів, перевіркою персоналу та транспортних засобів, кіберзагрозами для критично важливих авіаційних систем, створенням списку заборонених предметів на основі ризику, застосуванням альтернативних заходів безпеки для аеропортів із меншим ризиком. та звітування про інциденти з авіаційною безпекою.

Іншим відповідним інструментом є Заява про глобальні ризики авіаційної безпеки (Doc 10108, Restricted, яка наразі знаходиться у своєму третьому виданні). Цей живий документ надає державам інформацію високого рівня про глобальне середовище загроз і ризиків. Він містить аналіз глобальних загроз для цивільної авіації, інформацію про останні розробки в терористичній тактиці та технічний аналіз конкретних тенденцій авіаційної безпеки.

Визнаючи терміновість і важливість захисту KI, систем інформаційних і комунікаційних технологій і даних цивільної авіації від кіберзагроз, ICAO прагне розробити надійну структуру кібербезпеки. На своїй 40-й сесії Асамблея IKAO прийняла Резолюцію Асамблеї A40-10 щодо вирішення проблем кібербезпеки в цивільній авіації.

---

[96] Доступ до Посібника класифікується як обмежений. Його розповсюдження обмежується державними органами цивільної авіації та, за запитом, іншими суб'єктами, відповідальними за впровадження заходів авіаційної безпеки, такими як оператори аеропортів і повітряних суден, або інші суб'єкти, підтверджені відповідним державним органом. Посібник з авіаційної безпеки доступний в електронному вигляді для авторизованих користувачів за адресою https://drm.icao.int/ website.

[97] Додаток 17 – Безпека – включає, зокрема, Стандарти та рекомендовану практику безпеки міжнародної авіації та постійно переглядається та змінюється у світлі нових загроз і технологічних розробок, які впливають на ефективність заходів, призначених для запобігання актам незаконного втручання.

У резолюції кібербезпека розглядається через горизонтальний, наскрізний і функціональний підхід, підтверджуючи важливість і терміновість захисту систем KI та даних цивільної авіації від кіберзагроз і закликаючи держави впроваджувати Стратегію кібербезпеки ICAO.

Схвалена в 2013 році Асамблеєю ICAO на її 38-й сесії, Стратегія ICAO з ідентифікації мандрівників (TRIP) продовжує забезпечувати рамки для держав-членів у досягненні покращення авіаційної безпеки та сприяння, а також у виконанні їхніх зобов'язань згідно з резолюціями Ради Безпеки, що стосуються тероризму. Стратегія містить п'ять елементів, а саме: докази ідентичності; машинозчитувані проїзні документи; оформлення та контроль документів; системи та інструменти перевірки; і сумісні програми.

Рада Безпеки визнала лідерство та діяльність ICAO в політиці проїзної документації та оперативних питаннях, які зробили значний внесок у посилення авіаційної безпеки та сприяння, зокрема через прогресивні стандарти та специфікації проїзних документів, а також інструменти ідентифікації мандрівника для забезпечення кордонів.

Технічні специфікації, які забезпечують глобальну взаємодію проїзних документів, містяться в документі Doc 9303 «Машинозчитувані проїзні документи» (надалі «MRTDs»). Його восьме видання містить нову Частину 13, яка розробляє специфікації для видимих цифрових печаток (VDS), які будуть використовуватися для коду швидкої довідки (QR), що підтримує технології, що стоять за безконтактними процесами, що дозволяє особливо надійно перевірити автентичність результатів тестування та майбутніх сертифікатів про вакцинацію. Крім того, з метою забезпечення безперебійної подорожі для мандрівників із меншою кількістю контактів пасажирів в аеропорту, що призведе до здоровішого та безпечнішого досвіду подорожі, також було схвалено інструмент цифрових облікових даних для подорожей (DTC) та його специфікації, які дозволить розширити паспорт, сумісний з ICAO, на мобільний пристрій пасажира.

Крім того, ICAO встановлює стандарти та рекомендовану практику (SARPS) щодо створення основи для попередньої інформації про пасажирів (API) та запису імен пасажирів (PNR). Підтвердження особи є наріжним каменем зусиль, спрямованих на перешкоджання транскордонним переміщенням у рамках терористичної діяльності. З метою заохочення участі в каталозі відкритих ключів ICAO (PKD), поправка 26 до Додатку 9 – Спрощення – запровадила нову Рекомендовану практику (RP), RP 3.35.5, спрямовану на ті держави-члени ICAO, які використовують автоматизований прикордонний контроль. (ABC) системи. Цей RP заохочує

використання інформації, доступної через ICAO PKD, як засобу перевірки електронних паспортів шляхом порівняння розпізнавання обличчя з фотографією власника електронного паспорта.

ICAO співпрацює з різними офісами, директоратами та спеціалізованими установами Організації Об'єднаних Націй (такими як Контртерористичне управління, Виконавчий директорат Контртерористичного комітету та Управління ООН з наркотиків і злочинності), а також іншими міжнародними організаціями (Інтерпол, IMO). та Всесвітня митна організація) для виконання зобов'язань, визначених у Глобальній стратегії боротьби з тероризмом ООН. Спільна діяльність безпосередньо пов'язана з авіаційною безпекою та спрощенням, ідентифікацією та управлінням прикордонним контролем, як описано в резолюціях Ради Безпеки 1373 (2001), 1624 (2005), 2178 (2014), 2309 (2016), 2341 (2017), 2395 (2017), 2396 (2017) і 2482 (2019). ICAO є членом Глобального договору про координацію боротьби з тероризмом і бере активну участь у роботі робочих груп з управління кордонами та правоохоронної діяльності, що стосуються боротьби з тероризмом, щодо нових загроз та CIP.

7.3 Сектор інформаційних технологій

Захист ICI від ризиків кібербезпеки є пріоритетною метою ITU. Буенос-Айресський план дій, прийнятий на Всесвітній конференції з розвитку електрозв'язку у 2017 році, включив до мети 2 «Сприяти розвитку інфраструктури та послуг, включаючи зміцнення довіри та безпеки у використанні телекомунікацій/IKT».[98]

[98] Заключний звіт конференції доступний за адресою www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

Робота ITU безпосередньо пов'язана з підвищенням стійкості КІІ проти кібератак. Його діяльність зосереджена навколо трьох основних блоків дій: встановлення стандартів; підвищення обізнаності; та нарощування потенціалу. Ключові поточні ініціативи, що стосуються кожного з цих блоків і висвітлені в наступних параграфах.

7.3.1 Стандартне налаштування

Робота зі стандартизації здійснюється рядом технічних дослідницьких груп, у яких представники членів ITU розробляють рекомендації (стандарти) у різних галузях міжнародного електрозв'язку. Дослідницька група 17, зокрема, займається розбудовою довіри та безпеки під час використання інформаційних і комунікаційних технологій для досягнення більш безпечної мережевої інфраструктури, послуг і програм. У рамках цієї дослідницької групи на сьогоднішній день прийнято понад 350 стандартів[99] (відомих як «Рекомендації та доповнення ITU-T»).

Сфери поточної роботи навчальної комісії 17 включають, серед іншого, кібербезпеку, управління безпекою, архітектури та інфраструктури безпеки, керування ідентифікацією, безпеку додатків та аспекти безпеки хмарних обчислень, Інтернет речей, інтелектуальна транспортна система, великі дані та розподілені технологія бухгалтерської книги. Основним посиланням на стандарти безпеки є рекомендація ITU-T X.509 щодо електронної автентифікації в мережах загального користування. ITU-T X.509 вважається визначним інструментом для розробки програм, пов'язаних з інфраструктурою відкритих ключів.

7.3.2 Підвищення обізнаності

Інноваційним інструментом, розробленим ITU, є Глобальний індекс кібербезпеки. Задуманий головним чином як інструмент підвищення обізнаності, Індекс прагне виміряти відданість країн кібербезпеці. Діяльність кожної країни оцінюється за п'ятьма напрямками: правові заходи, технічні заходи, організаційні заходи, розбудова потенціалу та співпраця.

Питання розроблено для оцінки зобов'язань у кожному компоненті. Згодом, шляхом консультацій із групою експертів, ці запитання зважуються, щоб отримати загальну оцінку за Індексом. Четверте видання Індексу вийшло у 2020 році.[100]

7.3.3 Розбудова потенціалу

ITU підтримує держави-члени у створенні національних груп реагування на комп'ютерні інциденти (відомих як «CIRT»). Вони складаються з національних координаційних центрів для координації своєчасної та ефективної відповіді на кібератаки. ITU зобов'язується допомагати своїм державам-членам протягом усього процесу створення цих команд, від оцінки їхньої готовності до допомоги на етапах планування та реалізації, на основі принципу постійної співпраці. Крім того, МСЕ організовує регулярні регіональні навчання (так звані «кібернавчання») для посилення співпраці між національними командами в одному регіоні.

На сьогоднішній день оцінки національних груп реагування на комп'ютерні інциденти завершено для більш ніж 80 країн, і такі групи створено або посилено в 17 країнах.

Інший аспект роботи ITU у сфері нарощування потенціалу зосереджений на допомозі країнам у розробці національних стратегій кібербезпеки. Ці зусилля були підштовхнуті публікацією у 2018 році «Посібника з розробки національної стратегії кібербезпеки».[101]

---

[99] Рекомендації ITU-T, розроблені 17-ю дослідницькою комісією ITU-T, є загальнодоступними за адресою www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17.

[100] Поточна версія Покажчика та попередні видання доступні за адресою www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[101] www.itu.int/hub/publication/d-str-cyb_guide-01-2018/.

7.4 Сектор звичайних озброєнь

У своїй резолюції 2370 (2017) Рада Безпеки визнає «цінність... заходів, спрямованих на досягнення ефективної фізичної безпеки та управління запасами стрілецької зброї та легкого озброєння, як важливий засіб сприяння припиненню постачання зброї терористам».[102]

Зокрема, у пункті 7 резолюції Рада підкреслює «важливість вжиття державами-членами відповідних заходів... для запобігання... грабежу або придбанню стрілецької зброї та легкої зброї з національних запасів терористами, і наголошує у зв'язку з цим на важливість надання допомоги державам у цих регіонах, щоб вони могли відстежувати та контролювати запаси стрілецької зброї та легкого озброєння, щоб запобігти їх придбанню терористами».

Стосовно захисту критичної інфраструктури, забезпечення фізичної безпеки та управління запасами звичайної зброї є критично важливим у подвійному сенсі. По-перше, це зменшує ризик використання такої зброї проти КІ, наприклад транспортних систем, урядових приміщень та будь-яких інших об'єктів, які окремі країни вважають критичними. По-друге, ці самі запаси можна розглядати як КІ самі по собі, оскільки вони відіграють важливу роль у підтримці оборонної політики країн.

Різноманітність міжнародних і регіональних документів є частиною міжнародно-правового режиму щодо звичайних озброєнь. Хоча ці інструменти забезпечують правову та оперативну основу для посилення державами-членами своїх внутрішніх правових режимів, вони не обов'язково утворюють однорідний набір інструментів. Наприклад, Протокол проти незаконного виробництва та торгівлі вогнепальною зброєю, її частинами та компонентами, а також боєприпасами до неї (Протокол про вогнепальну зброю)[103] розглядає це питання з точки зору кримінального правосуддя з метою забезпечення заходів для усунення транснаціонального характеру це явище та його зв'язки з організованою злочинністю. Інші документи, хоча й охоплюють подібні теми, розглядають це питання з точки зору роззброєння, торгівлі чи розвитку та більше зосереджуються на заходах щодо зменшення накопичення, розповсюдження, перенаправлення та неправомірного використання вогнепальної зброї. Як результат, державним органам важливо ознайомитися з неоднорідною міжнародно-правовою базою та забезпечити її повне впровадження.

Нижченаведений перелік є невичерпною компіляцією міжнародних (Організації Об'єднаних Націй та регіональних) договорів та інших керівних документів, які розглядають цю тему з різних точок зору..

Об'єднані Нації

Договори

- Protocol Протокол проти незаконного виробництва та обігу вогнепальної зброї, її частин і компонентів, а також боєприпасів до неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності (2001 р.)
- Договір про торгівлю зброєю (2013)

Інші інструменти

- Programme Програма дій щодо запобігання та викорінення незаконної торгівлі стрілецькою зброєю та легкими озброєннями в усіх її аспектах та боротьби з нею (2001 р.)
- Міжнародний документ, що дозволяє державам своєчасно та надійно ідендифікувати та відстежувати незаконну стрілецьку та легку зброю

---

[102] Ці заходи вже були передбачені в Програмі дій із запобігання та викорінення незаконної торгівлі стрілецькою зброєю та легкими озброєннями в усіх її аспектах і боротьби з нею. Згідно з цією програмою уряди погодилися вдосконалити національне законодавство про стрілецьку зброю, контроль імпорту та експорту та управління запасами, а також співпрацювати та допомагати (www.un.org/disarmament/convarms/salw/programme-of-action/).

[103] Протокол доповнює Конвенцію ООН проти транснаціональної організованої злочинності.

Африка

Договори

- Протокол про контроль над вогнепальною зброєю, боєприпасами та іншими супутніми матеріалами в регіоні Співтовариства розвитку півдня Африки (2001 р.)

  Найробійський протокол щодо попередження, контролю та скорочення стрілецької зброї та легкого озброєння в районі Великих озер і на Африканському Розі (2004)
- Конвенція Економічного співтовариства західноафриканських держав про стрілецьку і легку зброю, боєприпаси до них та інші пов'язані з ними матеріали (2006)
- Конвенція Центральної Африки про контроль над стрілецькою та легкою зброєю, боєприпасами до неї та всіма частинами та компонентами, які можуть використовуватися для їх виробництва, ремонту та складання (Кіншаська конвенція) (2010)

Інші інструменти

- Бамакська декларація щодо спільної позиції африканських країн щодо незаконного розповсюдження, обігу та торгівлі стрілецькою зброєю та легкими озброєннями (2000)
- Стратегія Африканського Союзу щодо контролю за незаконним розповсюдженням, обігом і торгівлею стрілецькою зброєю та легкими озброєннями (2011)
- План дій щодо реалізації Стратегії Африканського Союзу щодо контролю за незаконним розповсюдженням, обігом і торгівлею стрілецькою зброєю та легкими озброєннями

США

Договори

- План дій щодо реалізації Стратегії Африканського Союзу щодо контролю за незаконним розповсюдженням, обігом і торгівлею стрілецькою зброєю та легкими озброєннями (1997)

Інші інструменти

- Андський план із запобігання, боротьби та викорінення незаконної торгівлі стрілецькою та легкою зброєю в усіх її аспектах (2003)
- Типові правила контролю за міжнародним переміщенням вогнепальної зброї, її частин і компонентів, а також боєприпасів до неї (2000)
- Кодекс поведінки держав Центральної Америки щодо передачі зброї, боєприпасів, вибухових

речовин та інших супутніх матеріалів (2006)

Азіатсько-Тихоокеанський регіон

Інструменти

- Рамкова програма Nadi (Правова база спільного підходу до заходів контролю над зброєю)
- План дій ASEAN щодо боротьби з транснаціональною злочинністю (Асоціація держав Південно-Східної Азії) (1999)

Європа

Організація з безпеки та співробітництва в Європі

- План дій ОБСЄ щодо стрілецької зброї та легкого озброєння

- Довідник передових практик щодо звичайних боєприпасів, Довідник передових практик щодо звичайних боєприпасів (2008);
- Принципи ОБСЄ щодо контролю за брокерською діяльністю у сфері стрілецької та легкої зброї (2004);
- Стандартні елементи сертифікатів кінцевого користувача та процедури перевірки експорту стрілецької та легкої зброї (Форум співробітництва у сфері безпеки) (2004)
- Посібник із найкращих практик щодо стрілецької та легкої зброї (2003)
- Принципи ОБСЄ, що регулюють передачу звичайних озброєнь (1993)
- Документ ОБСЄ про стрілецьку та легку зброю (2000 р., перевиданий у 2012 р.)
- Рішення ОБСЄ №. 11/08 Представлення найкращих практик для запобігання дестабілізуючим передачам стрілецької зброї та легкого озброєння повітряним транспортом та у відповідній анкеті (2008)

Європейський Союз

- Спільна дія Ради від 12 липня 2002 року щодо внеску Європейського Союзу в боротьбу з дестабілізуючим накопиченням і розповсюдженням стрілецької зброї та легкої зброї
- Загальна позиція Ради 2003/468/CFSP від 23 червня 2003 року щодо контролю за посередництвом у сфері зброї
- Спільна позиція Ради 2008/944/CFSP від 8 грудня 2008 р., що визначає загальні правила контролю за експортом військових технологій та обладнання
- Регламент (ЄС) № 258/2012 Європейського Парламенту та Ради від 14 березня 2012 року про імплементацію статті 10 Протоколу ООН проти незаконного виробництва та торгівлі вогнепальною зброєю, її частинами та компонентами, а також боєприпасами до неї, який доповнює Конвенція Націй проти транснаціональної організованої злочинності та встановлення дозволу на експорт, імпорту та транзиту вогнепальної зброї, її частин і компонентів, а також боєприпасів
- Кодекс поведінки Європейського Союзу щодо експорту зброї (1998)
- Стратегія Європейського Союзу щодо боротьби з незаконним накопиченням і обігом стрілецької зброї та легкої зброї та боєприпасів до них (2005 р.).

7.5 Хімічний, біологічний, радіологічний та ядерний сектори

Можливість недержавних організацій, у тому числі терористичних груп та їхніх прихильників, отримати доступ до зброї та матеріалів масового знищення та використовувати їх, розглядається як серйозна загроза міжнародному миру та безпеці. У своїй резолюції щодо сьомого перегляду Глобальної контртерористичної стратегії ООН (резолюція 75/291) Генеральна Асамблея закликала всі держави-члени «запобігти придбанню терористами ядерних, хімічних і біологічних матеріалів і підтримати міжнародні зусилля». під егідою Організації Об'єднаних Націй, щоб запобігти придбанню терористами зброї масового знищення та засобів її доставки, і закликає всі держави-члени вживати та посилювати національні заходи, якщо це доцільно, щоб запобігти придбанню терористами зброї масового знищення та засобів її доставки. постачання та супутні матеріали, обладнання та технології, пов'язані з їх виготовленням» (п. 68). Рада Безпеки зробила подібні заяви, останнє з яких включено до резолюції 2325 (2016) від 15 грудня 2016 року, яка закликає всі держави-члени зміцнити свої національні режими боротьби з розповсюдженням зброї масового знищення у виконанні її основоположної резолюції 1540 (2004).

Управління по боротьбі з тероризмом

Відповідно до резолюції Ради Безпеки 2325 (2016), Глобальна контртерористична стратегія ООН закликає держави-члени, міжнародні організації та систему ООН:

- Боротьба з контрабандою хімічних, біологічних, радіологічних та ядерних матеріалів
- Переконайтеся, що досягнення біотехнології не використовуються в терористичних цілях
- Покращити прикордонний і митний контроль для запобігання та виявлення незаконного обігу зброї та матеріалів CBRN
- Поліпшити координацію планування реагування на терористичну атаку з використанням ХБРЯ зброї чи матеріалів CBRN

У відповідь на глобальну загрозу CBRN, Контртерористичне управління через Контртерористичний центр Організації Об'єднаних Націй розробило свою Програму із запобігання та реагування на тероризм, пов'язаний зі зброєю масового знищення/хімічно-біологічним, радіологічним та ядерним (WMD/CBRN) тероризмом. Програма спрямована на покращення розуміння державами-членами та міжнародними організаціями рівня цієї загрози. Він також підтримує їхні зусилля з запобігання, готовності та реагування на їхні запити. Зокрема, Програма надає підтримку у розбудові потенціалу, зосереджуючись на таких сферах, як прикордонний та експортний контроль, стратегічний контроль торгівлі, незаконний обіг, захист CBRN матеріалів та критичної інфраструктури, CBRN криміналістика, нові технології, реагування на інциденти та управління кризовими ситуаціями, зокрема інші заходи, глобальний портфель навчальних заходів.

Програма підтримує робочі групи Глобального договору про координацію боротьби з тероризмом, зокрема групи з нових загроз і захисту критичної інфраструктури, а також з управління кордонами та правоохоронної діяльності, пов'язаної з боротьбою з тероризмом.

Крім того, він призначений для зміцнення стратегічного партнерства з відповідними членами Глобального договору про координацію боротьби з тероризмом, пов'язаних із зброєю масового знищення та CBRN, і міжнародними ініціативами держав-членів, уможливлюючи розробку спільних, доповнюючих і взаємопідсилювальних проектів. Були встановлені тісні робочі відносини з Глобальною ініціативою по боротьбі з ядерним тероризмом та Глобальною групою семи під керівництвом Глобального партнерства проти розповсюдження зброї та матеріалів масового знищення.

Міжрегіональний дослідницький інститут злочинності та правосуддя ООН

Діяльність Міжрегіонального науково-дослідного інституту ООН з питань злочинності та правосуддя (UNICRI) у цій сфері ґрунтується на спостереженні, що існуючі національні стратегії визнають важливість розробки комплексного підходу, але, як правило, мають ізольовану позицію,

збережену структуруванням CBRN секторів. У світлі цього спостереження UNICRI підтримує розробку інтегрованого CBRN підходу, який включає всі міжнародні, регіональні та національні CBRN компоненти в загальну стратегію. Це передбачає застосування цілісного підходу, за допомогою якого всі зацікавлені сторони, діючи автономно, можуть встановлювати спільні цілі, визначати та керувати ресурсами для досягнення цих цілей, чітко розподіляти обов'язки та завдання, розробляти функціональні канали зв'язку, створювати культуру безпеки на основі загальних навчання та забезпечити, щоб отримані уроки були включені та засвоєні всією системою.

Відповідно до цього бачення UNICRI за технічної підтримки Міжнародного агентства з атомної енергії (МАГАТЕ), Організації із заборони хімічної зброї (OPCW), Групи імплементаційної підтримки Конвенції про заборону біологічної зброї, Всесвітньої організації охорони здоров'я (WHO), ІНТЕРПОЛ, Європол і Всесвітня митна організація запустили Програму зменшення CBRN ризиків і управління безпекою.[104] Основними цілями Програми є:

- Сприяти та підтримувати розвиток управління CBRN безпекою в країнах-учасницях шляхом заохочення комплексного CBRN підходу, встановлення чітких каналів зв'язку, покращення обміну інформацією та передачі передового міжнародного досвіду.

[104] See https://unicri.it/index.php/topics/cbrn.

- Оптимізувати обмін та використання накопиченого міжнародного та національного досвіду у сфері зменшення CBRN ризиків, включаючи застосування знань і уроків, отриманих у сфері ядерної безпеки, до сфери хімічної та біологічної безпеки.
- Розвивайте процес співпраці між членами мережі для визначення проблем і можливих рішень на основі інформації, доступної мережі. За допомогою цього підходу мета полягає в тому, щоб створити справжню відповідальність за політику та її реалізацію національними агентствами.

7.5.1 INTERPOL

У 2010 році на своїй вісімдесятій сесії Генеральна Асамблея Інтерполу прийняла історичне рішення[105] започаткувати всеохоплюючий потенціал із запобігання тероризму CBRN та реагування на підтримку 192 країн-членів Організації. У 2016 році Інтерпол посилив свою місію в галузі CBRN, зобов'язавшись допомагати країнам-членам у ідентифікації, відстеженні та виявленні зброї та матеріалів у своїй Глобальній контртерористичній стратегії – п'ятирічній гнучкій стратегічній структурі. перекриття незаконного обігу зброї та матеріалів, необхідних для терористичної діяльності. У Стратегії далі визначаються основні дії, які мають бути вжиті CBRN та Піддиректоратом з уразливих цілей з метою надання допомоги країнам-членам у запобіганні та реагуванні на глобальні загрози CBRN з боку недержавних організацій:

- Дія 4.3: Сприяти обміну розвідувальними даними між країнами-членами про предмети та способи дії, пов'язані з CBRN та IED
- Дія 4.4: Підвищення спроможності країн-членів запобігати та реагувати на CBRN та IED атаки шляхом створення програм контрзаходів.
- Дія 4.5: Розробка та координація транскордонних міжвідомчих операцій на основі розвідки для перехоплення незаконного обігу CBRN матеріалів та компонентів IED.
- Дія 4.7: Підтримувати та розвивати стратегічні партнерства з ХБРЯ в глобальному масштабі.

Впроваджуючи вищезазначені дії – і відповідно до Статуту NTERPOL 106 – Організація зосереджується виключно на боротьбі з загрозами CBRN, які становлять недержавні суб'єкти. Відповідно, Інтерпол утримується від розгляду питань, пов'язаних зі спонсорованим державою розповсюдженням зброї масового знищення, які ретельно розглядаються іншими міжнародно-правовими та інституційними механізмами. Тим не менш, спектр недержавних суб'єктів охоплює не лише терористичні групи, вовків-одинаків та інших злочинців як потенційних

кінцевих користувачів, а й широку картину незаконного обігу матеріалів CBRN та його різних компонентів. Постачальники, посередники, покупці та мережі контрабанди входять до компетенції INTERPOL.

Чітке згадування в резолюції Ради Безпеки 1540 (2004) недержавних суб'єктів зробило резолюцію природною точкою відліку для діяльності Інтерполу, пов'язаної з CBRN. Відтоді як Інтерпол вперше розвинув свій потенціал CBRN, він обмінювався офіційними листами з Комітетом 1540, в яких викладалися умови їхньої поточної співпраці та призначалися відповідні контактні особи. Нещодавно Інтерпол відігравав активну роль у рамках комплексного перегляду резолюції 2016 року. У більш широкому сенсі Інтерпол є призначеним «агентством-помічником» відповідно до ініціативи резолюції 1540 (2004), і більшість його діяльності в рамках CBRNE підтримує – прямо чи опосередковано – імплементацію резолюції.

---

[105] Постанова AC-2011-PEC-10 від 07.11.2011.

[106] Стаття 3 Статуту Інтерполу закріплює керівний принцип нейтралітету, прямо забороняючи Інтерполу займатися справами політичного, військового, релігійного чи расового характеру.

INTERPOL підтримує тісні робочі відносини з Управлінням ООН з питань роззброєння, особливо сприяючи діяльності з розбудови потенціалу реєстру експертів, які беруть участь у Механізмі Генерального секретаря з розслідування ймовірного використання хімічної та біологічної зброї..

У 2020 INTERPOL і Контртерористичний центр Організації Об'єднаних Націй Контртерористичного управління запустили спільну ініціативу з проведення глобального дослідження загроз щодо недержавних суб'єктів та їхніх матеріалів CBRNE. Завдяки розробці стратегічної оцінки загроз проти CBRNE, використовуючи інформацію національних правоохоронних органів, ця п'ятирічна ініціатива допоможе міжнародному співтовариству протистояти загрозі, яку створює доступ недержавних суб'єктів до матеріалів CBRNE. У зв'язку з тим, що правоохоронні органи в усьому світі ведуть діяльність із запобігання, готовності та реагування на тероризм ХБРЯ, оцінки загрози використовуватимуться для визначення пріоритетів майбутньої міжнародної підтримки та діяльності з розбудови спроможності, в тому числі через програму CBRNE Інтерполу та програму уразливих цілей..

INTERPOL створив піддиректорат з CBRNE та вразливих цілей, який підтримується аналітичним підрозділом, який проводить оцінку країни та регіону, збирає звіти та надає інформацію, яка пропонує напрямок цільової діяльності. Відділ із запобігання радіологічному та ядерному тероризму в складі Піддиректорату CBRNE та вразливих цілей зосереджується на розробці та виконанні проектів, спрямованих на підвищення обізнаності щодо наявності та вразливості радіологічних та ядерних матеріалів, і, у свою чергу, покращення спроможності та спроможності країн-членів для запобігання, виявлення, реагування та розслідування терористичних і злочинних актів із залученням цих матеріалів. Використовуючи міжвідомчий підхід, діяльність підрозділу сприяє налагодженню стосунків і обміну інформацією, а також заохочує розробку спільних планів реагування агентств. Ця мета досягається шляхом об'єднання представників поліції, митниці, органів охорони кордону, науки, академічних кіл, регуляторних органів, урядових міністерств та інших відповідних організацій.

В INTERPOL спеціалізовані групи зосереджені на запобіганні трьом видам тероризму:

- Радіологічний і ядерний тероризм
- Біотероризм
- Хімічний та вибуховий тероризм

Діяльність INTERPOL варіюється від аналізу даних, навчальних семінарів і настільних навчань до міжнародних конференцій і операцій на місцях. Методологія INTERPOL для протидії загрозам CBRNE

складається з трьох основних компонентів:

- Перший стовп включає в себе обмін інформацією та аналіз розвідданих. На додаток до проведення оцінки та аналізу загроз INTERPOL публікує регулярний аналітичний звіт: щомісячний дайджест INTERPOL CBRNE. Доповідь, надіслана країнам-членам та іншим передплатникам, узагальнює звіти з відкритих джерел про всі аспекти злочинності та тероризму з радіохвильовим, радіальним, радіальним і радіаційним радіонуклідами та надає аналітичну точку зору щодо окремих питань..
- Друга опора передбачає розвиток потенціалу та навчання. Організація допомагає своїм країнам-членам розвивати їхній потенціал, навички та знання з метою протидії загрозі CBRNE. Це працює для:
    - Підвищити рівень обізнаності правоохоронних органів щодо CBRNE
    - Проводити навчальні заняття з метою підвищення спроможності правоохоронних органів
    - Надати методи профілактики для використання країнами-членами
- Третій стовп полягає в наданні оперативної та слідчої підтримки. За запитом Інтерпол може надати оперативну підтримку своїм країнам-членам у формі групи реагування на інциденти. У разі терористичної атаки до складу цих груп можна залучити персонал, який має досвід у питаннях CBRNE. Крім того, Організація проводить низку ініціатив, проектів та операцій для підтримки міжнародної правоохоронної спільноти у боротьбі з торгівлею матеріалами CBRNE.

7.5.2 Хемічний сектор

OPCW розглядає питання захисту KI з точки зору просування ефективних методів управління безпекою процесів і хімічних об'єктів. У 2016 році Організація склала посібник із найкращих практик, який збирає та опрацьовує інформацію, отриману від 16 держав-членів.[107]

Зокрема, OPCW розглядає питання безпеки (які розуміються як заходи щодо «навмисних викидів» токсичних хімікатів) поруч із проблемами безпеки (а саме, заходи протидії «ненавмисним викидам»). Головні цілі Організації в цій сфері полягають у забезпеченні охоплення державами-членами наступних аспектів безпеки та безпеки:

- Запобігання: відноситься до розуміння та впровадження заходів для зменшення можливості виникнення хімічної аварії або інциденту з безпекою. Інцидент із хімічною безпекою може включати крадіжку хімічних матеріалів для подальшого нецільового використання або зловмисне викид хімікатів у навколишнє середовище.
- Виявлення: відноситься до систем і процесів, які підтримують раннє виявлення викидів або втрат хімікатів, а також підтвердження використання хімікатів після підозрюваного викиду (випадкового чи зловмисного). Системи виявлення повинні включати процеси повідомлення про ризик.
- Реагування: відноситься як до реагування на рівні об'єкта, так і до реагування на національному рівні на хімічну аварію чи інцидент із хімічною безпекою. Системи реагування включають залучення, оснащення та навчання служб реагування, таких як пожежники, небезпеки, надзвичайні ситуації та поліція.

Серед існуючих міжнародних інструментів та ініціатив OPCW виділила такі, що включають корисні елементи з питань хімічної безпеки та безпеки:

- Резолюція Ради Безпеки 1540 (2004), яка зобов'язує держави-члени, серед іншого, утримуватися від підтримки будь-якими засобами недержавних суб'єктів у розробці, придбанні, виробництві, володінні, транспортуванні, передачі або використанні ядерної, хімічної чи біологічної зброї та її системи доставки. Важливо те, що цей інструмент зосереджений на елементах превентивного виміру управління ризиками хімічної безпеки.
- Базельська конвенція про контроль за транскордонним перевезенням небезпечних відходів та їх видаленням, яка стосується міжнародного переміщення небезпечних матеріалів. Незважаючи на те, що Конвенція спрямована на запобігання викиду токсичних хімікатів у навколишнє середовище, впровадження заходів може підтримувати безпечне поводження з хімікатами та

зменшувати обсяг хімікатів під час транспортування та в системі утилізації відходів, підтримуючи найкращі практики хімічної безпеки та хімічної безпеки.

- Стокгольмська конвенція про стійкі органічні забруднювачі, спрямована на скорочення виробництва та використання стійких органічних забруднювачів. Норми та найкращі практики, прийняті для виконання цієї Конвенції, відіграють важливу роль у підвищенні хімічної безпеки та управління ризиками безпеки.
- Роттердамська конвенція про процедуру попередньої обґрунтованої згоди щодо певних небезпечних хімічних речовин і пестицидів у міжнародній торгівлі, яка регулює маркування та поводження з небезпечними хімічними речовинами, зокрема тими, що є предметом міжнародної торгівлі. Він містить стандарти та вказівки, корисні для підтримки практики безпеки ланцюга постачання.
- Директиви Севезо (I, II та III)[108], інструменти Європейського Союзу, які спрямовані на підвищення безпеки місць, що містять велику кількість небезпечних речовин.
- Глобальна гармонізована система класифікації та маркування хімікатів (GHS), стандарт, керований Організацією Об'єднаних Націй, створений для заміни безлічі схем класифікації та маркування небезпечних матеріалів, які раніше використовувались країнами по всьому світу. Незважаючи на те, що за своєю природою

[107] Дивіться www.opcw.org/sites/default/files/documents/ICA/ICB/OPCW_Report_on_Needs_and_Best_Practices_on_Chemical_Safety_and_Security_ManagementV3-2_1.2.pdf.

[108] Директива Ради 96/82/ЕС від 9 грудня 1996 року про контроль за небезпекою великих аварій, пов'язаних з небезпечними речовинами», а початкова Директива Севезо була «Директива 82/501/ЕС про контроль за ризиками великих аварій, пов'язаних з небезпечними речовинами».

він є добровільним, у деяких країнах він став обов'язковим на внутрішньому рівні.

- Responsible Care, глобальна ініціатива хімічної промисловості, яка, серед інших цілей, спрямована на підвищення безпеки продуктів і процесів і, як зазначено на її веб-сайті, «зобов'язує компанії, національні асоціації хімічної промисловості та їхніх партнерів надавати допомогу та консультації для сприяння відповідальне поводження з хімічними речовинами всіма тими, хто керує та використовує їх у всьому ланцюжку продукту».[109]
- Міжнародна організація зі стандартизації (ISO), яка встановила низку стандартів, що підтримують елементи хімічної безпеки та захисту, зокрема: 13000 щодо управління ризиками, 28000 щодо ланцюга поставок хімічних речовин, 14000 щодо екологічного менеджменту та 9000 щодо управління якістю.

Конкретно зосереджуючись на терористичній загрозі з боку недержавних суб'єктів, у 2017 році було проведено скликаний OPWC експертний семінар з міжнародної координації хімічної безпеки.110 На семінарі було проведено оглядове вправляння «з метою підведення підсумків існуючої міжнародної співпраці та координації з хімічної безпеки, виявити прогалини та обговорити майбутню діяльність, включаючи майбутні механізми координації». Ключовою рекомендацією було створення міжнародного координаційного механізму, «щоб дозволити ключовим міжнародним акторам, які підтримують розвиток глобального потенціалу хімічної безпеки... обговорювати пріоритети та методології, використовувати ресурси один одного, співпрацювати там, де це необхідно, для задоволення потреб окремих держав та підвищувати міжнародний профіль потреб хімічної безпеки та допомоги». Іншим ключовим результатом зустрічі стала рекомендація створити модель методології забезпечення хімічної безпеки.

Діяльність OPCW із розбудови потенціалу, що має безпосереднє відношення до KI в хімічному секторі, реалізується через Програму управління хімічною безпекою та безпекою.111 Завдяки обміну політикою та передовим досвідом із хіміками-практиками, політиками, національними органами влади та асоціаціями хімічної промисловості, Програма спрямована на сприяння та поширення культури управління хімічною безпекою та безпекою. Він забезпечує тренінги для спеціалістів з практичних аспектів хімічної безпеки та безпеки, а також форуми для обміну та обговорення передового досвіду серед зацікавлених сторін. З 2008 по 2018 рік у програмах з нарощування потенціалу з інтегрованого управління хімічними ризиками, які проводить Технічний секретаріат OPCW, взяли участь понад 2000 учасників з понад 130 держав-членів.

7.5.3 Ядерний сектор

Захист ядерних та інших радіоактивних матеріалів і пов'язаних з ними установок від терористичних атак та інших небезпек є пріоритетною метою МАГАТЕ. Його ініціативи в цій галузі реалізуються Відділом ядерної безпеки, який займається всіма питаннями, пов'язаними із запобіганням і виявленням, а також реагуванням на крадіжки, диверсії, несанкціонований доступ і незаконну передачу або інші зловмисні дії, пов'язані з ядерними та іншими радіоактивними матеріалами та пов'язаними з ними засоби. Правова база, що лежить в основі цих робочих сфер, включає мережу міжнародних документів, які включають, зокрема:

- Конвенція про фізичний захист ядерного матеріалу (з поправкою 2005 р.)
- Кодекс поведінки щодо безпеки радіоактивних джерел
- Резолюції Ради Безпеки ООН 1373 (2001), 1540 (2004) і 2325 (2016)
- Міжнародна конвенція про боротьбу з актами ядерного тероризму

Серія публікацій МАГАТЕ з ядерної безпеки доповнює вищезазначене, надаючи передові практики, технічні посібники, навчальні посібники та інші матеріали на користь держав-членів. Ці публікації включають посібник із

---

[109] Дивіться www.cefic.org/Responsible-Care.

[110] Експертний семінар з міжнародної координації хімічної безпеки, 7 грудня 2017 р. Доступно за адресою www.opcw.org/fileadmin/OPCW/Protection-Against-CW/OPCW_Chemical_Security_Workshop_-_Informal_Summary_-_October_2017_-_for_release.pdf.

[111] Дивіться www.opcw.org/resources/capacity-building/international-cooperation-programmes/chemical-safety-and-security.

впровадження під назвою «Створення інфраструктури ядерної безпеки для ядерно-енергетичної програми» (МАГАТЕ, 2013). Посібник містить технічне керівництво щодо розвитку інфраструктури ядерної безпеки, включаючи правову, нормативну та інституційну основу та національну стратегію ядерної безпеки. Його обґрунтування полягає в необхідності, як зазначено у передмові до посібника, «забезпечити, щоб ядерний та інший радіоактивний матеріал не потрапив до рук сторін, які можуть використовувати цей матеріал для злочинних чи терористичних актів, а також запобігати актам саботажу. проти об'єктів і пов'язаної з ними діяльності, в тому числі під час транспортування».

14 вересня 2021 року Рада керуючих схвалила План ядерної безпеки на період 2022–2025 років[112]. План описує запропоновану діяльність МАГАТЕ з ядерної безпеки, яка відповідає пріоритетам, висунутим державами-членами через рішення та резолюції директивних органів Агентства. План визначає, зокрема, набір пріоритетних сфер і підсфер для втручання через технічну допомогу та заходи з розбудови потенціалу, які включають:

- Продовжувати сприяти подальшому дотриманню Конвенції про фізичний захист ядерного матеріалу та поправок до неї з метою її універсалізації.
- Надавати допомогу, за запитом, у сферах запобігання, виявлення та реагування, а також пом'якшення внутрішньої загрози та культури ядерної безпеки.
- Посилити захист конфіденційної інформації та комп'ютерних систем, визнаючи загрози ядерній безпеці та від кібератак на ядерні об'єкти, а також пов'язану з ними діяльність, включаючи використання, зберігання та транспортування ядерних та інших радіоактивних матеріалів.
- Допомагати державам-членам, на їх запит, у розробці національних законодавчих і регулятивних рамок; заохочувати та полегшувати технічний обмін знаннями, досвідом та передовою практикою щодо використання та безпеки радіоактивних джерел протягом усього їх життєвого циклу.
- Зміцнювати культуру ядерної безпеки та надавати можливості для навчання та навчання з ядерної безпеки.

[112] Дивіться www.iaea.org/sites/default/files/gc/gc65-24.pdf.

Додаток I
Вибрані ресурси щодо CIP за країнами[1]

Аргентина

Резолюція No.1523 (2019)	Нормативний акт	Постанова, прийнята Урядовим секретаріатом з питань модернізації за участі Комітету з кібербезпеки в рамках Національної стратегії кібербезпеки, визначає поняття критичної інфраструктури та критичної інформаційної інфраструктури. Він також затверджує глосарій термінів кібербезпеки, в якому такі поняття, як доступ, загроза, кібератака, файли cookie і витік даних, серед іншого. У преамбулі резолюції пояснюється, що Комітет з кібербезпеки провів детальний аналіз визначень, прийнятих різними країнами та міжнародними організаціями, таким чином прагнучи використати міжнародний досвід і знання в цьому питанні. Постанова зобов'язує Національного директора з кібербезпеки періодично переглядати та оновлювати глосарій	www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Австралія

Стратегія стійкості КІ: план(2015)	Стратегічний і політичний документ	Стратегія спрямована на підтримку безперервної роботи КІ в умовах усіх небезпек. Основними результатами, яких прагне досягти Стратегія, є: • Міцне та ефективне партнерство бізнесу та влади • Покращене управління ризиками операційного середовище • Ефективне розуміння та управління стратегічними питаннями • Зріле розуміння та застосування організаційної стійкості У документі окреслено основні заходи, які будуть здійснюватися на національному рівні для досягнення цих результатів.	www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF
Національні рекомендації щодо захисту КІ від тероризму (2015)	Стратегічний і політичний документ	Керівні принципи доповнюють Стратегію стійкості КІ, забезпечуючи основу для національного підходу до CIP проти конкретної загрози, яку становлять терористичні акти.	www.police.vic.gov.au/sites/default/files/2019-03/NationalGuidelinesForProtectingCriticalInfrastructureFromTerrorismNovember2015.pdf
Закон про безпеку КІ (2018)	Нормативний акт	Метою цього Закону є створення основи для управління ризиками, пов'язаними з критичною інфраструктурою, включно з: Підвищення прозорості власності та операційного контролю КІ в Австралії, щоб краще розуміти ці ризики • Сприяння співпраці та співпраці між усіма рівнями влади, регуляторними органами, власниками та операторами • Забезпечення режиму для Співдружності для реагування на серйозні інциденти кібербезпеки 2 грудня 2021 року до Закону про безпеку критичної інфраструктури 2018 року було внесено зміни, які розширили охоплення з 4 секторів до 11 секторів і 22 класів активів.	www.legislation.gov.au/Details/C2021C00570
Стратегія відповідності та забезпечення дотримання Центру кібербезпеки та інфраструктурної безпеки (2022)	Стратегічний і політичний документ	Мета цієї стратегії полягає в тому, щоб окреслити, як Центр кібербезпеки та безпеки інфраструктури забезпечуватиме дотримання вимог суб'єктів, які він регулює, забезпечуючи дотримання ними нормативних зобов'язань згідно з відповідним законодавством. Забезпечуючи найкращу практику, орієнтоване на галузь, активне та залучене регуляторне партнерство, яке співпрацює з промисловістю для покращення безпеки та процвітання Австралії, Центр використовує підхід до всіх небезпек у кожному з 11 критичних секторів інфраструктури, які він регулює, спираючись на через сильну увагу до кібербезпеки. Стратегія відповідності та забезпечення виконання пояснює ключові принципи, які лежать в основі підходу Центру до регулювання, відповідності та правозастосування, і її слід читати разом із публікацією Центру «Захищаємо Австралію разом» і Стратегією стійкості критичної інфраструктури.	www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-compliance-enforcement-strategy-april-2022.pdf

[1] Інформація, наведена в цьому додатку, не є вичерпним переліком існуючих державних ресурсів щодо CIP. Інформація була включена на основі актуальності, веб-доступності, географічного представлення та відповідей, наданих урядами у відповідь на вербальну ноту, надіслану державам-членам Управлінням з боротьби з тероризмом 2 березня 2022 року з проханням «поділитися своїми передовими практиками». про захист критичної інфраструктури (англійською або іншою доступною мовою)».

Бельгія

Закон про безпеку та захист КІ (2011 р. зі змінами 2018 р.)	Нормативний акт	Акт : • Частково транспортує Директиву ЄС 2008/114/ про визначення європейської КІ • Встановлює критерії та процедури ідентифікації та позначення КІ • Визначає внутрішні та зовнішні заходи безпеки для CIP • Визначає обсяг та умови обміну інформацією між операторами КІ та компетентними державними установами • Встановлює громадський контроль і санкції за порушення закону	www.nbb.be/doc/cp/fr/2018/20180925_loi_du_1juillet2011.pdf

Канада

Концепція управління надзвичайними ситуаціями для Канади (2011)	Стратегічний і політичний документ	Встановлює загальний підхід для різних федеральних, провінційних і територіальних ініціатив з управління надзвичайними ситуаціями. Рамкова програма спрямована на забезпечення консолідації федеральної, провінційної та територіальної співпраці та забезпечення більш узгоджених, взаємодоповнюючих дій між різними урядовими ініціативами на федеральному, провінційному та територіальному рівнях. Він підкреслює ключові компоненти управління надзвичайними ситуаціями. Він також вводить нові терміни та переглядає існуючі визначення таких термінів, як «усі небезпеки» та «стійкість», щоб відобразити сучасні розробки у сфері управління надзвичайними ситуаціями.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frm-wrk/mrgnc-mngmnt-frmwrk-eng.pdf
Стратегія кібербезпеки (2018)	Стратегічний і політичний документ	Прагне зміцнити кіберсистеми та сектори КІ, спираючись на три стовпи: захист державних систем; Партнерство для захисту життєво важливих кіберсистем за межами федерального уряду; Допомога канадцям у безпеці в Інтернеті.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
Національна стратегія розвитку КІ (2009)	Стратегічний і політичний документ	Базуючись на принципах Системи управління надзвичайними ситуаціями, Стратегія пропонує, щоб федеральні, провінційні та територіальні уряди та десять секторів КІ співпрацювали для посилення стійкості КІ в Канаді. Співпраця базується на розвитку партнерства на основі наявних повноважень і обов'язків. Для сприяння цим партнерствам Стратегія окреслює механізми покращеного обміну інформацією та захисту інформації та визначає важливість підходу до управління ризиками.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
План дій для КІ (2021-2023)	Стратегічний і політичний документ	План дій підтримує просування Національної стратегії 2009 року, підтверджуючи зобов'язання уряду Канади тісно співпрацювати з партнерами сектору КІ, провінціями та територіями для більш безпечної та стійкої Канади. План дій базується на прогресі, досягнутому в рамках попередніх планів дій, визначає нові види діяльності, засновані на мінливому середовищі загроз, і підтримуватиме спільний підхід для підвищення безпеки та стійкості КІ країни.	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx

Китай

Правила безпеки та захисту КІІ (2021)	Нормативний	Положення визначає політику країни щодо захисту ІСІ. Зокрема, Загальні положення покладають на Департамент громадської безпеки Державної ради відповідальність за керівництво та нагляд за роботою із захисту безпеки КІ. Різні розділи встановлюють правила ідентифікації КІ, відповідальності та обов'язків операторів КІ, а також юричну відповідальність операторів за недотримання правил.	https://digichina. tive-sept-1-2021/

Франція

Указ № 2007-585 від 23 квітня 2007 року про деякі нормативні положення частини першої Оборонного кодексу	Нормативний акт	Вносить зміни до Кодексу оборони шляхом введення набору статей, які встановлюють інституційну основу для захисту життєво важливої діяльності («activités d'importance vitale») (див. статті R. 1332-1-1332-42).	www.legifrance.gouv.fr/affichTexte.do;jsessionid=B3D2B-93BA4D5B3162AC56B-149F71F4EC.tplgfr30s_3?cid-Texte=JORFTEX-T000000615627&date-Texte=20070424

Міжвідомча інструкція з безпеки життєво важливої діяльності (№ 6600/SGDSN/PSE /PS, 7 January 2014)	Нормативний акт	Інструкція, прийнята Генеральним секретаріатом оборони та національної безпеки, містить широкі положення щодо впровадження інституційної архітектури Франції щодо захисту КІ.	http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf
Національна стратегія цифрової безпеки (2015)	Стратегічний і політичний документ	Встановлює стратегічні цілі та інституційний підхід для забезпечення стійкості Франції проти кіберзагроз, включаючи загрози КІІ.	www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
План Vigipirate (2015)	Стратегічний і політичний документ	План Vigipirate передбачає 300 заходів, які охоплюють 13 основних сфер діяльності, таких як транспорт, охорона здоров'я та мережі. На підставі оцінки терористичної загрози, зробленої розвідувальними службами, Генеральний секретаріат з питань оборони та національної безпеки видає вказівки, що визначають заходи, які мають вживати суб'єкти, відповідальні за пильність, запобігання та захист від терористичних загроз. Оператори КІ повинні перевести заходи плану у власні плани безпеки.	www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf

Німеччина

Національна стратегія захисту критичної інфраструктури (2009)	Стратегічний і політичний документ	Узагальнює цілі та завдання Федеральної адміністрації та її політичний і стратегічний підхід. Стратегія також є відправною точкою для консолідації результатів, отриманих на сьогоднішній день, і для їх подальшого розвитку з огляду на нові виклики.	www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=-publicationFile&v=1
Стратегія кібербезпеки для Німеччини (2011)	Стратегічний і політичний документ	Забезпечує основу для кібербезпеки протягом наступних п'яти років. Політична основа для уряду, спільно з промисловістю та суспільством, щоб забезпечити безпечне та автономне використання нових технологій шляхом належного оснащення органів безпеки, ефективного захисту критичної інфраструктури та бізнесу та підвищення безпеки цифрової сфери для населення	www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html

Японія

Основний закон про кібербезпеку (2014 р. - поправки внесені в 2018 р.)	Нормативний акт	Закон спрямований на забезпечення кібербезпеки, одночасно гарантуючи вільний потік інформації. Через посилення загроз кібербезпеці в 2018 році до закону було внесено зміни з метою підготовки Японії до проведення Олімпійських і Паралімпійських ігор у Токіо 2020 року. Зокрема, була створена Рада з кібербезпеки, щоб дати можливість різним державним і приватним організаціям взаємно співпрацювати в обміні інформацією про кібербезпеку та обговоренні необхідних контрзаходів. До складу ради входять представники національних і місцевих адміністративних органів, інфраструктурних і кіберсуб'єктів, освітніх і науково-дослідних установ, експерти.	www.lexology.com/library/detail.aspx?g=5a1b0e44-9f84-432e-9bed-88523b2eb-b6a
Стратегія кібербезпеки (2021)	Стратегічний і політичний документ	Стратегію кібербезпеки розроблено на основі Основного закону про кібербезпеку. CIP розглядається в рамках однієї з ключових цілей Стратегії: «Створення цифрового суспільства, в якому люди можуть жити з почуттям безпеки». У підрозділі «Покращення захисту критичної інфраструктури на основі співпраці між державним і приватним секторами» Стратегія посилається на Політику кібербезпеки для захисту критичної інфраструктури 2017 року як документ, на основі якого національний уряд докладає зусиль для захисту КІ.	www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf
Політика кібербезпеки для захисту КІ (2017)	Стратегічний і політичний документ	Політика є центральним документом із захисту КІ в країні. Він відображає три пріоритети: • Сприяння провідній діяльності операторів КІ (класифікація операторів КІ у світлі взаємозалежності) • Покращення механізмів обміну інформацією під час підготовки до Олімпійських та Паралімпійських ігор • Сприяння готовності до інцидентів на основі управління ризиками	www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf

Нова Зеландія

Проект інфраструктурної стратегії (2021)	Стратегічний і політичний документ	Проект стратегії, підготовлений Комісією з інфраструктури, описує інфраструктурні проблеми, з якими стикається Нова Зеландія. До них належать довгострокові виклики, у тому числі виклики, пов'язані з безпекою, а також можливості, які відкриває зміна технологій. Він визначає кілька цілей і рекомендацій. Під заголовком «Посилення стійкості до потрясінь і стресів» визначено необхідність узгодженого підходу до КІ, зокрема: • Потрібно визначити та ідентифікувати КІ країни • Найкращий підхід до управління загрозами кібербезпеці • Потрібно включити безпеку постачання основних інфраструктурних матеріалів у плвнування ризиками	www.tewaihanga.govt.nz/assets/Uploads/211012-Draft-New-Zealand-Infrastructure-Strategy.pdf
Закон про цивільну оборону та управління в надзвичайних ситуаціях (2002)	Нормативний акт	Закон забезпечує законодавчу основу для забезпечення стійкості національної інфраструктури: • Встановлення вимог та обов'язків постачальників послуг життєво необхідної інфраструктури, таких як вода та електроенергія, у центральному уряді, місцевому уряді та приватному секторі. • Визначення комунальних служб рятувальної служби як постачальників послуг КІ та встановлення вимог щодо скоординованої готовності та безперервності цих служб рятувальної служби у випадку надзвичайної ситуації, а також вимог щодо розкриття інформації. • Вимагання підготовки Національної стратегії стійкості до стихійних лих і Національного плану управління надзвичайними ситуаціями, які каскадно доповнюють скоординовані місцеві плани. Контроль за дотриманням Закону здійснює Національне агентство з управління надзвичайними ситуаціями.	www.legislation.govt.nz/act/public/2002/0033/51.0/DLM149789.html
Довідник із системи національної безпеки (2016)	Стратегічний і політичний документ	У Посібнику викладено механізми країни як щодо управління національною безпекою, так і у відповідь на потенційну, зароджуючу чи фактичну кризу національної безпеки. Він складається з чотирьох розділів: частина 1: Система національної безпеки; частина 2: Структури управління національною безпекою; частина 3: Реакція на потенційну, виникаючу або фактичну подію; частина 4: Супровідні додатки.	https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf
Стратегія кібербезпеки (2019)	Стратегічний і політичний документ	Стратегія визначає п'ять напрямів першочергових дій. У ньому конкретно згадується CI в пріоритетній сфері «Чуйна та стійка Нова Зеландія». Стратегія супроводжується річною робочою програмою, яка окреслює ряд кроків для просування в кожній пріоритетній сфері. Відповідальний міністр публікує щорічний звіт про прогрес у кожній сфері.	https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019

Польща

Національна програма захисту критичної інфраструктури (2020)	Стратегічний і політичний документ	Програма визначає: • Національні пріоритети, цілі, вимоги та стандарти для забезпечення ефективного функціонування КІ • Компетентні державні органи, відповідальні за системи CIP • Критерії, що використовуються для розрізнення об'єктів, установок, пристроїв і послуг	www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej
Стратегія національної безпеки (2020)	Стратегічний і політичний документ	У Стратегії міститься чітке посилання на CIP у її складовій частині, яка стосується «Стійкості держави та консолідованої громадянської оборони». Розділ 2.8 передбачає реалізацію «моделі захисту критичної інфраструктури, забезпечення її безперервної роботи та безперебійного надання послуг». Стратегія також містить керівні принципи щодо CIP у конкретних секторах, таких як охорона здоров'я, економічна та енергетична безпека.	www.bbn.gov.pl/ftp/ dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Португалія

Стратегія боротьби з тероризмом (2015)	Стратегічний і політичний документ	Національна стратегія базується на п'яти стовпах: виявлення, запобігання, захист, переслідування та реагування. У розділі «Захист» мета включає «посилення безпеки пріоритетних цілей». Стратегія вимагає розробки плану дій для захисту та підвищення стійкості КІ, як національних, так і європейських.	Прем'єр-міністр Португалії (веб-посилання на запит)

Національна стратегія кібербезпеки (2019-2023)	Стратегічний і політичний документ	Стратегія ґрунтується на трьох стратегічних цілях, які перетворюються на шість осей втручання. Зокрема, вісь 3 стосується «Захисту кіберпростору та інфраструктури».	Прем'єр-міністр Португалії (веб-посилання на запит)

Republic of Moldova

Постанова Уряду № 701 про затвердження Положення про захист об'єктів критичної інфраструктури від тероризму (2018)	Нормативний акт	Положення встановлює процес планування, організації та реалізації заходів антитерористичного захисту об'єктів КІ шляхом раціонального використання наявних людських, фінансових і матеріальних ресурсів та врахування специфічних уразливих місць КІ. Постанову прийнято в рамках Закону № 120 про запобігання тероризму та боротьбу з ним (див. приклад)	Information received from Permanent Mission of the Republic of Moldova to the United Nations

Russian Federation

Акт про безпеку критичної інформаційної інфраструктури (2017)	Нормативний акт	Викладає основні принципи, визначення та порядок забезпечення безпеки ІСІ Російської Федерації. У ньому викладені елементи та принципи Державної системи виявлення, попередження та пом'якшення наслідків кібератак на інформаційні ресурси Російської Федерації, яка включає, серед інших елементів, національний координаційний центр з комп'ютерних інцидентів (див. https:/ /cert.gov.ru/index.html). Федеральний закон також визначає критерії визначення певних інформаційних активів як критичної інфраструктури (такої як соціальна, економічна, оборонна, політична та екологічна), а також ролі та обов'язки державних органів, основні вимоги до безпеки та захисту активів ІСІ, права та зобов'язання операторів і власників ІСІ, а також наслідки невиконання цих вимог та зобов'язань. Нарешті, Закон створює національний реєстр ІСІ та визначає принципи регулярного державного нагляду та оцінки загроз.	http://kremlin.ru/acts/bank/42128

Сенегал

Національна стратегія кібербезпеки (2017)	Стратегічний і політичний документ	Стратегія включає наступні елементи: • Оцінка стратегічного контексту кібербезпеки в Сенегалі, включаючи поточні та майбутні загрози • Урядове бачення кібербезпеки та стратегічні цілі, яких необхідно досягти • Інституційна основа для його реалізації Стратегічна ціль 2 стосується саме посилення захисту інфраструктури ІСІ та інформаційних систем держави.	www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

Singapore

Закон про захист інфраструктури (2018)	Нормативний акт	Закон про захист інфраструктури є частиною антитерористичної системи країни. Закон має на меті посилити безпеку будівель і посилити захист чутливих місць, забезпечивши це: • Основні розробки розроблено з урахуванням безпеки, зокрема шляхом включення заходів безпеки наперед у проект будівлі. • Місця скупчення людей захищаються від терористичних загроз шляхом видання спеціальних заходів безпеки (розпоряджень та наказів). • Конфіденційні місця та їх оточення захищені розширеними повноваженнями (наприклад, заборона несанкціонованого фотографування). Закон супроводжується інструкцією, яка встановлює його законодавчі вимоги для власників та осіб, відповідальних за спеціальні розробки та спеціальну інфраструктуру, призначену відповідно до Закону.	https://sso.agc.gov.sg/Acts-Supp/41-2017/Published/20171031?DocDate=20171031&WholeDoc=1
Закон про кібербезпеку (2018)	Законодавчий інструмент	Закон офіційно закріплює політику країни в цій галузі та формулює захист ІСІ в конкретних концепціях кібербезпеки та заходах захисту (додаткову інформацію див. у прикладі)	www.csa.gov.sg/legislation/cybersecurity-act

Стратегія кібербезпеки (2021)	Стратегічний/ політичний документ	Стратегія складається з трьох стратегічних стовпів. У рамках компонента 1 («Створення стійкої інфраструктури») передбачається, що Агентство кібербезпеки Сінгапуру тісно співпрацюватиме з власниками ІСІ та галузевими лідерами для посилення кібербезпеки операційних технологічних систем, таких як системи промислового контролю, де кібератаки можуть спричинити фізичні та економічні втрати.	www.csa.gov.sg/ News/Publications/ singapore-cybersecuri-ty-strategy-2021

Південна Африка

Закон про захист критичної інфраструктури (2019)	Нормативний акт	Закон передбачає: • Ідентифікацію та оголошення інфраструктури як КІ • Фактори, які слід враховувати для забезпечення прозорої ідентифікації та декларування КІ • Заходи захисту та стійкості КІ • Створення Ради КІ та її функції; • Функції Національного уповноваженого органу відповідно до Закону • Призначення та функції інспекторів • Повноваження та обов'язки осіб, які контролюють КІ • Забов'язання щодо звітності	www.gov.za/sites/default/files/gcis_document/201911/42866 28-11act8of2019criticalinfraprotectact.pdf

Іспанія

Закон № 8/2011 про встановлення заходів щодо захисту КІ (2011)	Нормативний інструмент	Закон координує дії всіх компетентних державних органів і сприяє співпраці та залученню власників і операторів КІ. Він транспонує в національне законодавство заходи, включені в Директиву ЄС 2008/114 / ЕС, зокрема ідентифікацію та класифікацію європейських КІ.	www.boe.es/buscar/act.php?id=BOE-A-2011-7630
Королівський указ 704/2011 про затвердження Правил захисту критичної інфраструктури (2011)	Нормативний акт	Указ реалізує рамкові положення, викладені в Законі № 8/2011.	www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf
Стратегія Національної безпеки (2021)	Нормативний акт	Загрози КІ повністю включені в документ як загрози національній безпеці.	www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Швеція

Закон про охорону безпеки (2019)	Нормативний акт	Закон спрямований на кращий захист інформації та заходів, важливих для безпеки Швеції, від кібератак (включно з тими, які призначені для викрадення конфіденційних даних і тих, які спрямовані на зрив критичних операцій).	https://rkrattsbaser.gov.se/sfst?bet=2018:585

Швейцарія

Національна стратегія CIP 2018-2022 (2017)	Стратегічний і політичний документ	Стратегія, прийнята Федеральним відомством цивільного захисту, оновлює початкову стратегію (видану в 2012 році), встановлюючи вищі цілі. Переглянута стратегія спрямована на те, щоб перевести виконану роботу в інституціоналізований процес, закріпити це в законодавстві та доповнити його на ситуаційній основі.	www.babs.admin.ch/fr/aufgabenbabs/ski.html
Національна стратегія захисту від кіберризиків (2018-2022) (2018)	Стратегічний і політичний документ	Спираючись на попередню стратегію на період 2012-2017 років, переглянута стратегія на 2018-2022 роки розглядає операторів КІ як основну цільову групу для своїх заходів. Нова стратегія визначає десять сфер дій, спрямованих на вирішення різних проблем аспекти кіберризиків. Загалом у цих сферах діяльності сформульовано 29 заходів, які базуються на ряді головних принципів, таких як «децентралізоване впровадження», «допоміжна роль держави» та «підхід, що ґрунтується на ризиках».	www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html

Сполучене Королівство Великої Британії та Північної Ірландії

Стратегія національного захисту (2015)	Стратегічний і політичний документ	Стратегія національної безпеки є головним документом, який окреслює основи та цілі бачення країни щодо захисту КІ.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
План безпеки та стійкості сектора на 2018 рік (2019)	Стратегічний і політичний документ	Кабінет міністрів щороку замовляє плани секторальної безпеки та стійкості для провідних державних відомств для 13 найважливіших секторів країни. У планах описано: • Підходи провідних державних відомств до безпеки та стійкості критичного сектора • Their assessments of significant risks to their sectors • Їхній підхід до безпеки та стійкості у Великобританії • Діяльність, яку вони планують здійснити для пом'якшення та реагування на ці ризики Повні плани безпеки та стійкості сектору є секретними документами, оскільки містять конфіденційну інформацію про безпеку. Однак щороку уряд публікує несекретні підсумки, щоб надати представникам громадськості інформацію про заходи, які здійснюються в кожному секторі для підвищення безпеки та стійкості. Індивідуальні плани класифікуються, але Кабінет міністрів узагальнює кожну версію в один загальний секторний план стійкості для КІ.	www.gov.uk/government/collections/sector-resilience-plans
Національний реєстр ризиків надзвичайних ситуацій (2017)	Стратегічний і політичний документ	Надає огляд ключових ризиків, які потенційно можуть спричинити значні збої у Сполученому Королівстві протягом наступних п'яти років. Документ ілюструє типи надзвичайних ситуацій, які можуть виникнути, що робить уряд і партнери, щоб пом'якшити їх, і як представники громадськості та малий бізнес можуть захистити себе. Ряд розділів безпосередньо присвячені захисту КІ від терористичних актів.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

Україна

Закон про КІ (2021)	Нормативний акт	акон визначає правові та організаційні основи створення та функціонування національної системи CIP та її законодавчої складової у сфері внутрішньої безпеки.	https://cis-legislation.com/document.fwx?rgn=136781

США

Національний план захисту КІ (2013)	Стратегічний і політичний документ	Описує, як учасники спільноти CI від уряду та приватного сектору працюють разом, щоб керувати ризиками та досягати результатів безпеки та стійкості. План 2013 року відповідає вимогам Президентської політичної директиви № 21 щодо безпеки та стійкості КІ, підписаної в лютому 2013 року. Він був розроблений у результаті спільного процесу за участю зацікавлених сторін із усіх 16 секторів КІ, усіх 50 штатів, усіх рівнів управління та промисловості.	www.cisa.gov/national-infrastructure-protection-plan
Президентська політична директива 21: Безпека та стійкість критичної інфраструктури (2013)	Нормативний акт	Директива доручає виконавчій владі: • Розвивайте здатність ситуаційної обізнаності, яка розглядає як фізичні, так і кібернетичні аспекти функціонування інфраструктури майже в реальному часі • Зрозумійте каскадні наслідки збоїв інфраструктури • Оцініть і вдосконаліть державно-приватне партнерство • Оновити Національний план захисту інфраструктури • Розробіть комплексні плани досліджень і розвитку	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Виконавчий наказ 13636: Покращення кібербезпеки критичної інфраструктури (2013)	Нормативний акт	Наказ доручає виконавчій владі: • Розробити технологічно нейтральну добровільну структуру кібербезпеки • Сприяти та стимулювати впровадження практик кібербезпеки • Збільшити обсяг і покращити своєчасність і якість обміу інформацією про кіберзагрози • Включати надійний захист конфіденційності та громадських свобод у кожну ініціативу для забезпечення критичної інфраструктури • Досліджувати використання існуючого регулювання для сприяння кібербезпеці	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Додаток II
Резолюція Ради Безпеки 2341 (2017)

Рада Безпеки,

Згадуючи свої резолюції 1373 (2001), 1963 (2010), 2129 (2013) and 2322 (2016),

Підтверджуючи свою головну відповідальність за підтримання міжнародного миру та безпеки відповідно до Статуту Організації Об'єднаних Націй,

Знову підтверджуючи свою повагу до суверенітету, територіальної цілісності та політичної незалежності всіх держав відповідно до Статуту Організації Об'єднаних Націй,

Знову підтверджуючи, що тероризм у всіх формах і проявах становить одну з найсерйозніших загроз міжнародному миру та безпеці, і що будь-які акти тероризму є злочинними та невиправданими, незалежно від їх мотивів, коли б, де б і ким би вони не були вчинені, і залишаючись налаштованими продовжувати сприяти підвищення ефективності загальних зусиль у боротьбі з цим лихом на глобальному рівні,

Підтверджуючи, що тероризм становить загрозу міжнародному миру та безпеці і що протидія цій загрозі вимагає колективних зусиль на національному, регіональному та міжнародному рівнях на основі поваги до міжнародного права, включаючи міжнародне право прав людини та міжнародне гуманітарне право, і Статут ООН,

Підтверджуючи, що тероризм не повинен асоціюватися з будь-якою релігією, національністю, цивілізацією чи етнічною групою,

Підкреслюючи, що активна участь і співпраця всіх держав і міжнародних, регіональних і субрегіональних організацій необхідні для перешкоджання, погіршення, ізоляції та зведення з ладу терористичної загрози, і наголошуючи на важливості реалізації Глобальної протидії ООН Стратегія боротьби з тероризмом (GCTS), що міститься в резолюції 60/288 Генеральної Асамблеї від 8 вересня 2006 року, та її подальші перегляди,

Знову наголошуючи на необхідності вживати заходів для запобігання тероризму та боротьби з ним, зокрема, шляхом відмови терористам у доступі до засобів для здійснення їхніх атак, як

зазначено в Другому компоненті GCTS ООН, включаючи необхідність посилення зусиль для покращення безпеки та захисту особливо вразливі цілі, такі як інфраструктура та громадські місця, а також стійкість до терористичних атак, зокрема у сфері цивільного захисту, визнаючи, що держави можуть вимагати допомоги з цією метою,

Визнаючи, що кожна держава визначає, що є її критичною інфраструктурою, і як ефективно захистити її від терористичних атак,

Визнаючи зростаючу важливість забезпечення надійності та стійкості критичної інфраструктури та її захисту від терористичних атак для національної безпеки, громадської безпеки та економіки відповідних держав, а також добробуту та добробуту їх населення,

Визнаючи, що готовність до терористичних атак включає запобігання, захист, пом'якшення наслідків, реагування та відновлення з наголосом на сприянні безпеці та стійкості критичної інфраструктури, у тому числі шляхом державно-приватного партнерства, якщо це доречно,

Визнаючи, що зусилля щодо захисту передбачають численні потоки зусиль, наприклад планування; інформування та попередження населення; оперативна координація; розвідка та обмін інформацією; заборона і зрив; скринінг, пошук і виявлення;контроль доступу та перевірка особи; кібербезпека; заходи фізичного захисту; управління ризиками для програм захисту; управління ризиками для програм захисту та діяльності; цілісність і безпека ланцюга постачання

Визнаючи життєво важливу роль, яку відіграють інформовані та обережні спільноти у підвищенні обізнаності та розумінні середовища терористичної загрози, зокрема у виявленні підозрілих дій та звітуванні про підозрілу діяльність правоохоронним органам, а також важливість розширення обізнаності громадськості, залучення та державно-приватного партнерства за необхідності, особливо щодо потенційних терористичних загроз і вразливостей через регулярний національний і місцевий діалог, навчання та інформаційну роботу,

Відзначаючи зростаючу транскордонну взаємозалежність критичної інфраструктури між країнами, такої як та, яка використовується, зокрема, для виробництва, передачі та розподілу енергії, повітряного, наземного та морського транспорту, банківських та фінансових послуг, водопостачання, розподілу продуктів харчування та охорони здоров'я,

Визнаючи, що в результаті зростаючої взаємозалежності між секторами критичної інфраструктури деякі критичні інфраструктури потенційно сприйнятливі до зростаючої кількості та більш широкого спектру загроз і вразливостей, які викликають нові проблеми безпеки,

Висловлюючи занепокоєння тим, що терористичні атаки на критично важливу інфраструктуру можуть суттєво порушити функціонування уряду та приватного сектору та спричинити додаткові наслідки за межами сектору інфраструктури,

Підкреслюючи, що ефективний захист критичної інфраструктури вимагає галузевих і міжгалузевих підходів до управління ризиками та включає, серед іншого, виявлення терористичних загроз і підготовку до них, щоб зменшити вразливість критичної інфраструктури, запобігання та припинення змов терористів проти критичної інфраструктури, де це можливо, мінімізацію впливу і час відновлення у разі шкоди в результаті терористичної атаки, визначення причини шкоди або джерела атаки, збереження доказів атаки та притягнення винних у атаці до відповідальності,

Визнаючи у зв'язку з цим, що ефективність захисту критичної інфраструктури значно підвищується, коли вона базується на підході, який враховує всі загрози та небезпеки, зокрема терористичні атаки, а також у поєднанні з регулярними та змістовними консультаціями та співпрацею з операторами критичної інфраструктури та правоохоронними органами та органами безпеки посадовими особами, відповідальними за охорону критичної інфраструктури, та, у разі необхідності, з іншими зацікавленими сторонами, включаючи власників приватного сектору,

Визнаючи, що захист критичної інфраструктури вимагає внутрішнього та транскордонного співробітництва з державними органами, іноземними партнерами та власниками та операторами

такої інфраструктури в приватному секторі, а також обміну своїми знаннями та досвідом у розробці політики, передового досвіду та отриманих уроків,

Нагадуючи, що резолюція 1373 (2001) закликала держави-члени знайти шляхи інтенсифікації та прискорення обміну оперативною інформацією, особливо щодо дій або переміщень терористичних осіб або мереж; підроблені або фальсифіковані проїзні документи; торгівля зброєю, вибухівкою або чутливими матеріалами; використання комунікаційних технологій терористичними групами; та загрозу, яку становить володіння терористичними групами зброєю масового знищення, і співпрацювати, зокрема через двосторонні та багатосторонні домовленості та угоди, для запобігання та придушення терористичних нападів,

Відзначаючи роботу відповідних міжнародних, регіональних і субрегіональних організацій, організацій, форумів і нарад щодо посилення захисту, безпеки та стійкості критичної інфраструктури,

Вітаючи продовження співпраці у боротьбі з тероризмом між Контртерористичним комітетом (CTC) і Міжнародною організацією кримінальної поліції (INTERPOL), Управлінням ООН з наркотиків і злочинності, зокрема щодо технічної допомоги та нарощування потенціалу, а також усіма іншими об'єднаними Органи націй та рішуче заохочуючи їхню подальшу взаємодію з Цільовою групою Організації Об'єднаних Націй з реалізації заходів щодо боротьби з тероризмом (CTITF) для забезпечення загальної координації та узгодженості зусиль системи ООН у боротьбі з тероризмом,

1. *Заохочує* всі держави докладати узгоджених і скоординованих зусиль, у тому числі шляхом міжнародного співробітництва, для підвищення обізнаності, розширення знань і розуміння проблем, пов'язаних з терористичними нападами, з метою покращення готовності до таких нападів на критичну інфраструктуру;

2. *Заохочує* всі держави докладати узгоджених і скоординованих зусиль, у тому числі шляхом міжнародного співробітництва, для підвищення обізнаності, розширення знань і розуміння проблем, пов'язаних з терористичними нападами, з метою покращення готовності до таких нападів на критичну інфраструктуру;

3. *Нагадує* про своє рішення в резолюції 1373 (2001) про те, що всі держави визнають терористичні акти серйозними кримінальними злочинами у внутрішньому законодавстві та правилах, і закликає всі держави-члени забезпечити встановлення кримінальної відповідальності за терористичні атаки, спрямовані на знищення або виведення з ладу KI, а також планування, навчання, фінансування та матеріально-технічна підтримка таких атак;

4. *Закликає* держави-члени вивчити способи обміну відповідною інформацією та активно співпрацювати у запобіганні, захисті, пом'якшенні наслідків, забезпеченні готовності, розслідуванні, реагуванні на терористичні атаки або відновленні після них, запланованих або скоєних проти критичної інфраструктури;

5. *Далі закликає* держави встановити або зміцнити національне, регіональне та міжнародне партнерство з зацікавленими сторонами, як державними, так і приватними, у відповідних випадках для обміну інформацією та досвідом з метою запобігання, захисту, пом'якшення, розслідування, реагування та відновлення після збиток від терористичних атак на об'єкти критичної інфраструктури, в тому числі шляхом спільного навчання, а також використання або встановлення відповідних мереж зв'язку чи оповіщення про надзвичайні ситуації;

6. *Настійно закликає* всі держави забезпечити тісну співпрацю та ефективно співпрацювати з питань захисту критичної інфраструктури від терористичних атак;

7. *Заохочує* Організацію Об'єднаних Націй, а також ті держави-члени та відповідні регіональні та міжнародні організації, які розробили відповідні стратегії щодо захисту критичної інфраструктури, працювати з усіма державами та відповідними міжнародними, регіональними та субрегіональними організаціями та установами для визначити та поділитися передовою практикою та заходами для управління ризиком терористичних атак на критичну інфраструктуру;

8. *Підтверджує, що ініціативи регіонального та двостороннього економічного співробітництва та розвитку відіграють життєво важливу роль у досягненні стабільності та процвітання, і у зв'язку з цим закликає всі держави посилити співпрацю для захисту критичної інфраструктури, включаючи проекти регіонального зв'язку та відповідні транскордонні зв'язки. інфраструктури, від терористичних нападів, у відповідних випадках, через двосторонні та багатосторонні засоби обміну інформацією, оцінки ризиків та спільної правоохоронної діяльності;*

9. *Наполегливо закликає держави, здатні це зробити, сприяти забезпеченню ефективного та цілеспрямованого розвитку потенціалу, навчанню та іншим необхідним ресурсам, технічній допомозі, передачі технологій і програмам, де це необхідно, щоб дозволити всім державам досягти мети захисту критично важливих інфраструктура проти терористичних атак;*

10. *Доручає CTC за підтримки Виконавчого директорату Контртерористичного комітету продовжувати, якщо це доцільно, у межах своїх повноважень вивчати зусилля держав-членів із захисту критичної інфраструктури від терористичних атак, що стосується виконання резолюції 1373 (2001) з метою виявлення передового досвіду, прогалин і слабких місць у цій сфері;*

11. *Заохочує у зв'язку з цим CTC, за підтримки CTED, а також CTITF продовжувати співпрацю для сприяння технічній допомозі та розбудові потенціалу та підвищення обізнаності у сфері захисту критичної інфраструктури від терористичних атак у зокрема шляхом зміцнення діалогу з державами та відповідними міжнародними, регіональними та субрегіональними організаціями та тісної співпраці, в тому числі шляхом обміну інформацією, з відповідними двосторонніми та багатосторонніми постачальниками технічної допомоги;*

12. *Заохочує* Робочу групу CTITF із захисту критично важливої інфраструктури, включаючи вразливі об'єкти, безпеки Інтернету та туризму, продовжувати сприяти, а також у співпраці з іншими спеціалізованими установами Організації Об'єднаних Націй надавати допомогу у розбудові потенціалу для посилення впровадження заходів на запит від держав-членів;

13. *Просить* CTC протягом дванадцяти місяців повідомити Раді про виконання цієї резолюції;

14. *Вирішує* займатися цим питанням.

Додаток III
Додаток до мадридських керівних принципів(витяг)

V. Захист KI, вразливих або м'яких цілей і туристичних об'єктів[2]

49. У своїй резолюції 2341 (2017) Рада Безпеки закликала держави розглянути можливість розробки або подальшого вдосконалення своїх стратегій для зменшення ризиків для критичної інфраструктури від терористичних нападів, у тому числі шляхом, серед іншого, оцінки та підвищення обізнаності про відповідні ризики; вжиття заходів готовності, включаючи впровадження ефективної відповіді на такі атаки та сприяння кращій сумісності в сфері безпеки та управління наслідками; сприяння ефективній взаємодії між усіма зацікавленими сторонами.

50. У своїй резолюції 2396 (2017) Рада Безпеки наголосила на необхідності для держав розробляти, переглядати або змінювати національні оцінки ризиків і загроз для врахування м'яких цілей, щоб розробити відповідні плани реагування на випадок непередбачених ситуацій і надзвичайні ситуації. терористичні атаки. Він також закликав держави встановити або зміцнити національне, регіональне та міжнародне партнерство з державними та приватними зацікавленими сторонами щодо обміну інформацією та досвідом з метою запобігання, захисту, пом'якшення наслідків, розслідування, реагування та відновлення збитків від терористичних атак проти м'яких цілей.

51. Критична інфраструктура та небезпечні цілі є особливо вразливими та привабливими як об'єкти тероризму. Вразливі місця можуть бути збільшені через взаємозв'язок, взаємозв'язок і взаємозалежність критичної інфраструктури. Привабливість легких цілей для терористів випливає не лише з їх відкритого формату та обмеженої безпеки для полегшення доступу, але й з потенціалу спричинити жертви серед цивільного населення, хаосу, публічності та економічного впливу.

52.Держави-члени несуть основну відповідальність за захист KI та легких цілей. Кожна

держава визначає критичну інфраструктуру та м'які цілі відповідно до свого національного контексту. Проте зростає потреба у збільшенні співпраці між державами та приватними компаніями, які володіють, експлуатують та керують критично важливою інфраструктурою та м'якими цілями, щоб задовольнити потреби безпеки, зменшити вразливість та обмінюватися інформацією про загрози, вразливі місця та заходи з з метою зменшення ризику нападу. Спільні тренінги, комунікаційні мережі, обмін інформацією (наприклад, про методології, найкращі практики та навчання) і механізми раннього попередження повинні бути використані та вдосконалені.

53. Для того, щоб максимізувати потенціал для захисту м'яких цілей, державно-приватні партнерства повинні розвиватися або зміцнюватися на всіх рівнях управління, включаючи державний, місцевий і провінційний. Держави-члени повинні заохочувати та підтримувати такі партнерства з компаніями, які можуть сприяти всім аспектам готовності, а саме захист від терористичних атак, пом'якшення наслідків, реагування на них та відновлення після них, а також розслідування таких інцидентів..

---

[2] Дивіться www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf.

54. Зусилля щодо захисту передбачають численні потоки зусиль, наприклад планування; інформування та попередження населення; оперативна координація; розвідка та обмін інформацією; заборона і зрив; скринінг, пошук і виявлення; контроль доступу та перевірка особи; кібербезпека; заходи фізичного захисту; управління ризиками для програм захисту та діяльності; цілісність і безпека ланцюга постачання.

Керівний принцип 50[3]

У своїх зусиллях щодо розробки та впровадження заходів для захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевими органами влади, повинні:

Визначення, оцінка та підвищення обізнаності щодо відповідних ризиків і загроз терористичних атак на критичну інфраструктуру та легкі цілі;

(a) Визначати, що являє собою критичну інфраструктуру та слабкі цілі в національному контексті, на основі поточного аналізу терористичних можливостей, намірів і минулих атак, а також регулярно проводити оцінку ризиків, щоб йти в ногу з мінливим характером загрози та супротивника, в тому числі шляхом використання існуючих інструментів і вказівок, розроблених міжнародними та регіональними організаціями;[4]

(b) Розробляти,впроваджувати та застосовувати на практиці стратегії та плани дій для зменшення ризиків терористичних атак на критичну інфраструктуру та м'які цілі, які об'єднують та використовують можливості відповідних державних і приватних зацікавлених сторін;

(c) Вживати заходів готовності, в тому числі для забезпечення ефективного захисту та відповіді на такі атаки, що ґрунтується на комплексній оцінці ризику;

(d) Сприяти кращій сумісності в сфері безпеки та управління кризами;

(e) Сприяти кращій сумісності в сфері безпеки та управління кризами;

(f) Встановлення або зміцнення механізмів обміну інформацією, знаннями (такими як інструменти та вказівки) та досвідом між державними та приватними зацікавленими сторонами для розслідування та реагування на терористичні напади на такі цілі.[5]

Керівний принцип 51[6]

У своїх подальших зусиллях щодо захисту критичної інфраструктури та легких цілей від терористичних атак держави-члени, діючи у співпраці з місцевою владою, повинні також розглянути:

---

[3] Питання захисту критичної інфраструктури, вразливих або слабких цілей і туристичних об'єктів конкретно не розглядаються в Мадридських керівних принципах. Рекомендації, надані в керівних принципах 50 і 51, спрямовані на підтримку виконання резолюції 2341 (2017) щодо захисту критичної інфраструктури, доповненої резолюцією 2396 (2017) та її положеннями щодо захисту легких цілей. Вони також базуються на вказівках, наданих у таких документах: Виконавча дирекція, Технічний посібник; і Виконавчий директорат і Управління по боротьбі з тероризмом, Захист критичної інфраструктури від терористичних атак: Компендіум передових практик (2018 р.).

[4] У своєму Керівництві з авіаційної безпеки ICAO надає вказівки щодо застосування стандартів і рекомендованих практик, описаних у додатку 17 до Конвенції про міжнародну цивільну авіацію. Опубліковане в 2017 році десяте видання Посібника містить новий і оновлений посібник. Особливий інтерес щодо захисту критичної інфраструктури становлять матеріали, що стосуються безпеки наземних зон аеропортів, перевірок персоналу та транспортних засобів та кіберзагроз для критично важливих авіаційних систем. Див. ICAO, Керівництво з авіаційної безпеки, 10-е видання, документ 8973; та ICAO, Додаток 17 до Конвенції про міжнародну цивільну авіацію: Безпека – захист міжнародної цивільної авіації від актів незаконного втручання, 10-е видання, Міжнародні стандарти та рекомендована практика (квітень 2017 р.).).

[5] Резолюція 2396 (2017), пункти. 27 і 28.

[6] Питання захисту критичної інфраструктури, вразливих або слабких цілей і туристичних об'єктів конкретно не розглядаються в Мадридських керівних принципах. Рекомендації, надані в керівних принципах 50 і 51, спрямовані на підтримку виконання резолюції 2341 (2017) щодо захисту критичної інфраструктури, доповненої резолюцією 2396 (2017) та її положеннями щодо захисту легких цілей. Вони також базуються на вказівках, наданих у таких документах: Виконавча дирекція, Технічний посібник; і Виконавчий директорат і Управління по боротьбі з тероризмом, захист критичної інфраструктури від терористичних атак. Див. також пункти резолюції 2396 (2017). 27 і 28.

(a) Оновлення планування на випадок надзвичайних ситуацій, наприклад, інструкцій, навчань і тренінгів для правоохоронних органів, інших відповідних міністерств і галузевих учасників, щоб йти в ногу з реальними загрозами, вдосконалювати стратегії та гарантувати, що зацікавлені сторони адаптуються до мінливих загроз;

(b) Впровадження національних рамок і механізмів для підтримки прийняття рішень на основі ризиків, обміну інформацією та державно-приватного партнерства як для уряду, так і для промисловості, в тому числі з метою спільної роботи для визначення пріоритетів і спільної розробки відповідних продукти та інструменти, такі як загальні вказівки щодо спостереження або спеціальні захисні заходи, запропоновані для різних типів об'єктів (наприклад, стадіонів, готелів, торгових центрів або шкіл);

(c) Встановлення процесів для обміну оцінками ризиків між урядом, промисловістю та приватним сектором для сприяння та підвищення обізнаності про ситуацію та зміцнення безпеки та стійкості до м'яких цілей;

(d) Встановлення процесів для обміну інформацією з промисловістю та партнерами з приватного сектору шляхом, наприклад, видачі дозволів безпеки та підвищення обізнаності;

(e) Сприяння державно-приватному партнерству шляхом розробки механізмів співпраці, підтримки власників бізнесу та операторів і менеджерів інфраструктури та обміну планами, політикою та процедурами, якщо це доцільно;

(f) Допомога в забезпеченні ефективного та цілеспрямованого розвитку потенціалу, навчанні та інших необхідних ресурсах, а також технічній допомозі, якщо така доставка необхідна, щоб дозволити всім державам розвинути відповідний потенціал для реалізації планів на випадок непередбачених обставин і реагування на напади на м'які цілі.

Додаток IV

Глобальна стратегія з тероризмом ООН (витяги)

Глобальна контртерористична стратегія ООН (резолюція 60/288, додаток)

II– Заходи щодо запобігання тероризму та боротьби з ним

Ми постановляємо вжити наступних заходів для запобігання тероризму та боротьби з ним, зокрема, шляхом відмови терористам у доступі до засобів для здійснення їхніх атак, до їхніх цілей та бажаного впливу їхніх атак:

...

18. Активізувати всі зусилля для покращення безпеки та захисту особливо вразливих об'єктів, таких як інфраструктура та громадські місця... визнаючи, що держави можуть потребувати допомоги з цією метою.

III. Заходи щодо розбудови спроможності держав запобігати тероризму та боротися з ним і зміцнювати роль системи ООН у цьому відношенні

Ми визнаємо, що розбудова потенціалу в усіх державах є ключовим елементом глобальних зусиль по боротьбі з тероризмом, і постановляємо вжити наступних заходів для розвитку спроможності держав запобігати тероризму та боротися з ним, а також покращити координацію та узгодженість у системі Організації Об'єднаних Націй у просуванні міжнародної співробітництво у боротьбі з тероризмом:

...

13. Заохочувати ООН співпрацювати з державами-членами та відповідними міжнародними, регіональними та субрегіональними організаціями для визначення та обміну передовим досвідом запобігання терористичним нападам на особливо вразливі цілі. Ми запрошуємо Міжнародну організацію кримінальної поліції співпрацювати з Генеральним секретарем, щоб він міг подати відповідні пропозиції. Ми також визнаємо важливість розвитку державно-приватного партнерства в цій сфері.

Глобальна контртерористична стратегія ООН: сьомий огляд (резолюція 75/291 Генеральної Асамблеї)

Генеральна Асамблея,

...

Висловлюючи занепокоєння терористичними нападами на вразливі цілі, включаючи критичну інфраструктуру та громадські місця («м'які» цілі), визнаючи, що кожна держава-член визначає, що є її критичною інфраструктурою чи громадськими місцями, оцінює рівень їхньої вразливості та визначає засоби їх ефективного захисту від терористичні атаки,

Висловлюючи особливе занепокоєння тим, що терористичні атаки на критично важливу

інфраструктуру можуть суттєво порушити функціонування уряду та приватного сектору та спричинити додатковий вплив за межі сектору інфраструктури, і тому підкреслюючи зростаючу важливість захисту критичної інфраструктури від терористичних атак та сприяння взаєморозумінню активна готовність до таких атак, у тому числі через державно-приватне партнерство, якщо це доречно,

...

69. *Рішуче засуджує* всі терористичні акти проти критичної інфраструктури, включаючи критичні енергетичні об'єкти, та проти інших уразливих цілей, і закликає всі держави-члени вжити всіх необхідних заходів для запобігання таким нападам, а також їхнім можливим радіологічним, радіоактивним та екологічним наслідкам, а також протидіяти такі терористичні акти, включаючи переслідування винних;

...

71. *Закликає* держави-члени посилити зусилля для покращення безпеки та захисту особливо вразливих об'єктів, включаючи релігійні об'єкти, навчальні заклади, туристичні об'єкти, міські центри, культурні та спортивні заходи, транспортні вузли, мітинги, ходи та колони, а також посилити їхню стійкість до терористичних атак, зокрема у сфері цивільного захисту, і заохочує держави-члени розглянути можливість розробки або подальшого вдосконалення своїх стратегій для зменшення ризиків для критичної інфраструктури від терористичних атак, які повинні включати, серед іншого, оцінку та підвищення обізнаності щодо відповідні ризики, вжиття заходів готовності, включаючи ефективну відповідь на такі атаки, а також сприяння кращій сумісності в безпеці та управлінні наслідками та сприяння ефективній взаємодії всіх зацікавлених сторін;

...

73. *Закликає держави-члени* посилити зусилля для покращення безпеки та захисту особливо вразливих об'єктів, включаючи релігійні об'єкти, навчальні заклади, туристичні об'єкти, міські центри, культурні та спортивні заходи, транспортні вузли, мітинги, ходи та колони, а також посилити їхню стійкість до терористичних атак, зокрема у сфері цивільного захисту, і заохочує держав-членів мати можливість розробки або подальшого вдосконалення своїх стратегій для зменшення ризиків для критичної інфраструктури від терористичних атак, які повинні включати, серед іншого, оцінку та підвищення обізнаності щодо відповідних ризиків , вжиття заходів готовності, що включає ефективну

відповідь на такі атаки, а також сприяння кращої сумісності в безпеці та управлінських наслідках та сприяння ефективній взаємодії всіх відвідуваних сторінок;

74. *Заохочує* Антитерористичне управління та організації Глобального договору про координацію боротьби з тероризмом тісно співпрацювати з державами-членами та відповідними міжнародними, регіональними та субрегіональними організаціями для визначення та обміну найкращими практиками запобігання терористичним нападам на особливо вразливі цілі, включаючи критичну інфраструктуру громадських місцях («м'які» цілі), а також визнає важливість розвитку державно-приватного партнерства в цій сфері;

Додаток V

Глобальний договір про координацію боротьби з тероризмом ООН

Глобальний договір про координацію боротьби з тероризмом Організації Об'єднаних Націй є найбільшим механізмом координації трьох основ діяльності Організації Об'єднаних Націй: мир і безпека, сталий розвиток, права людини та гуманітарні питання. Він спрямований на посилення спільного підходу до дій Організації Об'єднаних Націй для підтримки держав-членів, на їх прохання, у збалансованому впровадженні Глобальної контртерористичної стратегії ООН та інших відповідних резолюцій і мандатів Організації Об'єднаних Націй. Угоду про боротьбу з тероризмом було розроблено як частину реформи Генеральним секретарем архітектури боротьби з тероризмом Організації Об'єднаних Націй після створення, який виконує функції секретаріату Угоди про боротьбу з тероризмом.

Станом на квітень 2022 року Договор про боротьбу з тероризмом об'єднує 45 організацій як членів або спостерігачів, у тому числі 41 орган ООН, а також Інтерпол, Всесвітню митну організацію, Міжпарламентський союз і Групу розробки фінансових заходів. Нижче наведено членів і спостерігачів Контртерористичного договору:

Учасники:

1267 Моніторингова група

комітету 1540 Експертна група

комітету

Організація Договору про всеосяжну заборону ядерних випробувань (CTBTO)

Департамент охорони та безпеки Виконавчої дирекції

Контртерористичного комітету

Департамент миротворчих операцій

Департамент політичних справ і питань миротворчості

Департамент глобальних комунікацій

Виконавчий офіс Генерального секретаря, відділ верховенства права

International Civil

Авіаційна організація (ICAO) Міжнародна організація кримінальної

поліції

(INTERPOL) Міжнародна організація праці (ILO)

Міжнародна морська організація (IMO)

Управління по боротьбі з тероризмом

Офіс спеціального радника по Африці Управління з питань

роззброєння

Управління інформаційно-комунікаційних технологій Управління правових питань

Управління Верховного комісара ООН з прав людини (OHCHR)

Офіс Уповноваженого Генерального секретаря у справах молоді

Офіс із запобігання геноциду та відповідальності за захист

Офіс Спеціального представника Генеральногосекретаря з питань дітей і збройних

конфліктів

Офіс спеціального представника Генерального секретаря з питань сексуального насильства під

час конфлікту

Офіс спеціального представника Генерального секретаря з питань насильства над дітьми Організація

із заборони хімічної зброї (OPCW)

Спеціальний доповідач з питань просування та захисту прав людини та основних свобод під час

боротьби з тероризмом Альянс цивілізацій ООН

Програма розвитку ООН (UNDP)

Організація Об'єднаних Націй з питань освіти, науки і культури (UNESCO)

Організація ООН з питань гендерної рівності та розширення прав і можливостей жінок

(UN-Women) Міжрегіональний дослідницький інститут злочинності та правосуддя

ООН (UNICRI)

Інститут ООН з дослідження проблем роззброєння

(UNIDIR) Навчальний і дослідницький інститут ООН

(UNITAR)

Управління ООН з наркотиків і злочинності

Коледж персоналу системи ООН Всесвітня митна організація (WCO) Всесвітня організація охорони

здоров'я (WHO)

Спостерігачі:

Департамент економічних і соціальних питань

Міжнародна організація з міграції (IOM)

Міжпарламентський союз (IPU)

Управління з координації гуманітарних питань

Управління Верховного комісара ООН у справах біженців (UNHCR)

Дитячий фонд ООН (UNICEF)

22-25521

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

INTERPOL