МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ, ІНЖЕНЕРІЇ ТА ТЕХНОЛОГІЙ
КАФЕДРА ЦИВІЛЬНОЇ ТА ПРОМИСЛОВОЇ БЕЗПЕКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Б.Д.ХАЛМУРАДОВ
«___» _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР
СПЕЦІАЛЬНІСТЬ 263 «ЦИВІЛЬНА БЕЗПЕКА»

Тема: «ДОСЛІДЖЕННЯ СИСТЕМ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Виконавець: студент групи 207 ЦБз СІГНАЄВСЬКИЙ Олександр Миколайович
(студент, група, прізвище, ім’я, по батькові)

Керівник: к.т.н., Зозуля Сергій Васильович
(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

Нормоконтролер _____ Федина В.П.
(підпис) (П.І.Б)

КИЇВ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет екологічної безпеки, інженерії та технологій
Кафедра цивільної та промислової безпеки
Спеціальність: 263 «Цивільна безпека
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____(Б.Д. Халмурадов)
«____» _____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
СІГНАЄВСЬКИЙ Олександр Миколайович

1. Тема роботи «ДОСЛІДЖЕННЯ СИСТЕМ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ» затверджена наказом ректора від «31» 08 2023р. № 1577/ст.

2. Термін виконання роботи з 02.10.2023 р. по 26.12.2023р.

3. Вихідні дані роботи:

- Аналіз та класифікація потенційних загроз для критичної інфраструктури.
- Визначення основних вразливостей та ризиків, пов'язаних з критичною інфраструктурою.
- Розробка методів захисту та підвищення стійкості критичної інфраструктури в умовах різноманітних загроз.
- Проведення практичних досліджень на прикладі конкретних об'єктів критичної інфраструктури з метою оцінки ефективності запропонованих методів захисту і стійкості.
- Формування висновків та рекомендацій для покращення систем безпеки і стійкості критичної інфраструктури.

4. Зміст пояснювальної записки: аналітичний огляд літературних джерел з тематики диплому. Організаційні заходи щодо забезпечення безпеки та стійкості об'єктів критичної інфраструктури. Визначення та класифікація різних типів загроз об'єктів критичної інфраструктури. Оцінка готовності на реагування підчас виникнення різних загроз та оцінка ефективності існуючих заходів захисту. Розробка рекомендації щодо попередженню та профілактиці пожежного захисту автомобільних заправних станцій.

5. Перелік обов’язкового ілюстративного матеріалу: таблиці, рисунки, діаграми, графіки.

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1	Провести загальну характеристику теми кваліфікаційної роботи		
2	Провести аналіз літературних джерел		
3	Написання тез до конференції		
4	Провести аналіз можливих джерел запалювання		
5	Написання 2 розділу роботи		
6	Написання 3 розділу роботи		
7	Підготовка до захисту дипломної роботи		

7. Дата видачі завдання: «02» 10 2023 р.

Керівник дипломної роботи: _____ Зозуля С.В.

Завдання прийняв до виконання: _____ Сігнаєвський О.М

РЕФЕРАТ

Кваліфікаційна робота складається із вступу, основної частини, що містить 3 розділи, висновку й списку літератури. Загальний обсяг роботи 87 сторінок. Робота містить 4 рисунок, 6 таблиць. Список бібліографічних посилань включає 34 джерел.

Ключові слова: БЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, СТІЙКІСТЬ

Мета і завдання виконання дипломної роботи Метою дослідження є ретроспективний аналіз та оцінка потенційних загроз, вразливостей, а також розробка методів та засобів забезпечення стійкості критичної інфраструктури.

Об'єкт дослідження є критична інфраструктура, яка включає в себе електростанції, транспортні вузли, мережі зв'язку, водні та каналізаційні системи, медичні установи та інші об'єкти, що відіграють стратегічну роль для суспільства та економіки.

Предмет дослідження – є системи безпеки та стійкості цих критичних інфраструктурних об'єктів. Дослідження спрямоване на вивчення потенційних загроз, визначення вразливостей та розробку методів та засобів для забезпечення їх стійкості в умовах несприятливих чинників.

Методи дослідження, застосовані в дипломній роботі: аналітичний аналіз небезпек, аналіз систем раннього виявлення аварійних ситуацій автомобільної заправної станції.

Наукова новизна забезпечення комплексного розуміння загроз об'єктам критичної інфраструктури та розробити ефективні стратегії їх захисту.

Практичне значення роботи. Запровадження розроблених систем дозволить підвищити загальний рівень безпеки на енергетичних об'єктах, знизити ризики для громадськості та оточуючого середовища.

Основні розділи роботи були обговоренні на одинадцятої міжнародній науково-технічної конференції 16 – 17 листопада 2023 року у м. Харків.

ЗМІСТ

ВСТУП

Актуальність теми «Дослідження систем безпеки та стійкості критичної інфраструктури» обумовлена зростаючими загрозами фізичної безпеки інфраструктурних об'єктів. Критична інфраструктура, такі як електростанції, транспортні вузли, мережі зв'язку, медичні установи тощо, є об'єктами, які становлять стратегічну важливість для суспільства та економіки. Зростаюча кількість кібератак, терористичні загрози, природні катастрофи та інші чинники роблять цю тему надзвичайно актуальною. Дослідження систем безпеки та стійкості критичної інфраструктури вимагає розвитку нових підходів та стратегій для захисту цих об'єктів в умовах постійно зростаючих загроз

Сьогодні, коли ризик пронизує все, що ми робимо, розрахунок ризиків є центральним елементом нашого життя. Що є менш поширеним і менш усталеним - але, можливо, більш важливим, ніж будь-коли в контексті фіскальних обмежень і обмежених ресурсів - так це те, як найкраще ідентифікувати і визначати пріоритети ризиків, з якими ми стикаємося, і, в свою чергу, робити розумні інвестиції, виходячи з цих пріоритетів. Оцінювання ризиків лежить в основі національної безпеки, яка, по суті, полягає в управлінні ризиками. З моменту покладення повноважень на Департамент спец. зв’язку експерти намагалися краще ідентифікувати і відрізняти більш високі ризики від більш низьких - процес, відомий як сегментація ризиків. Жодна сім'я, місто чи країна не може дозволити собі усунути всі ризики, навіть якщо б це було можливо. Оцінка ризиків дозволяє сегментувати ризики, а це, в свою чергу, допомагає нам зосередити наші обмежені ресурси на найбільш важливих питаннях безпеки. Питання полягає в тому, де і як ми повинні розгортати програми безпеки, щоб максимізувати нашу здатність стримувати і виявляти зловмисну діяльність.

Основною метою управління ризиками є підвищення безпеки технічної системи. Основою процесу управління ризиками є ідентифікація загроз,

оскільки ефективне управління без цих знань практично неможливе. Найбільш важливим є розпізнавання технічних загроз [37, 47]. Крім того, слід звертати увагу на людський фактор та фактор навколишнього середовища, організаційні структури та взаємозв'язки між ними [10, 38]. Тільки такий підхід гарантує уникнення так званого неідентифікованого ризику. Для так званого чистого ризику, пов'язаного з експлуатацією технічної системи, розроблені стандартні дії. Стандартні рішення щодо захисту та безпеки технічної системи повинні бути адекватними можливим загрозам [18, 33, 44]. Загалом під безпекою технічної системи розуміють здатність системи зберігати свої основні функціональні властивості від внутрішніх і зовнішніх загроз [64].

Оцінка ризику - це триступенева процедура, що складається з [22, 41, 43, 45, 46, 50]:

- ідентифікація небезпеки,
- оцінка ймовірності,
- аналіз наслідків.

Попередній аналіз показує, що пріоритетними питаннями, пов'язаними з системою оповіщення, повинні бути [26]:

- оцінка часу реагування для вжиття заходів,
- способи оповіщення різних груп населення (школи, лікарні тощо)
- розробка попереджувальних повідомлень відповідно до масштабу загрози, які дозволять реалізувати захисні процедури,
- сценарій поведінки населення в умовах оповіщення, зазначення альтернативних джерел для засобів масової інформації, що належать до об'єктів критичної інфраструктури (питна вода, електрична та теплова енергія, природний газ),
- навчання населення щодо знань про системи оповіщення та інформування, види загроз та їхні наслідки,
- функціонування аварійно-рятувальних служб швидкого реагування.

Аналіз показує, що система оповіщення є особливим видом інформаційної системи [27]. Використовуючи базову понятійну термінологію теорії систем щодо системи оповіщення, можна виділити три основні підсистеми: функціональну, структурну та корисність [23, 45].

Функціональна підсистема складається з наступних елементів:

- отримання попереджувальних сигналів: визначення інформаційних потреб, визначення зони спостереження з можливим поділом, розташування джерел інформації, вимірювання змін параметрів, що контролюються,

- аналіз попереджувальних сигналів: визначення показників вимірювання змін, характеристики допустимих діапазонів змін, визначення пріоритетності показників змін, інтерпретація та перевірка величини попереджувальних параметрів.

Структурна підсистема включає такі елементи, як: джерела інформації (внутрішні, зовнішні бази даних, історичні, поточні, перспективні) та оперативні групи (збір та аналіз даних, реагування на надзвичайні ситуації, центри управління в надзвичайних ситуаціях) [1, 8]. Комунальна підсистема складається з наступних елементів:

- отримання інформації: запис даних постійного моніторингу, інтерв'ю та анкетування,

- аналіз даних: методологія, техніка обробки даних, вибір показників,

- передача інформації: інформаційні технології, методи захисту даних, методи комп'ютерної підтримки прийняття рішень, правила вербальної комунікації.

Система раннього попередження дозволяє виявити загрози та запустити процедури протидії їм. Зменшення негативних наслідків можливе завдяки тому, що система попередження є частиною реагування в кризових ситуаціях. Системи оповіщення використовуються в управлінні ризиком, оскільки вони створюють можливості для його оцінки - виявляють надзвичайні загрози та сприяють оцінці негативних наслідків [9, 13, 63]. Крім того, система оповіщення визначає ефективність будь-яких рятувальних

операцій. Точна ідентифікація небезпеки та безперешкодна передача інформації дозволяють ефективно реагувати за допомогою попереджень та сигналів тривоги [6, 58].

При аналізі ризиків слід використовувати історичні знання про роботу системи, аналітичні методи та досвід операторів. У багатьох випадках частиною аналізу ризиків є аналіз людського фактору та аналіз надійності людини - диспетчера системи [5].

Критична інфраструктура (КІ) - це складна технологічна система, що працює безперервно і вимагає високого рівня безпеки. Проблемою для зловмисників є відстань між окремими підсистемами та їх елементами, що особливо ускладнює точний моніторинг системи. Така система є унікальною, її окремі елементи виконують різні функції, і в той же час вони взаємодіють, утворюючи єдине ціле. Їх правильна взаємодія визначає оптимальне функціонування з технічної, економічної та надійної точок зору [2, 7, 21, 22].

Критична інфраструктура міст повинна перебувати під постійним наглядом як з функціональних, так і з безпекових міркувань. Управління безпекою та ризиками в муніципальних системах, таких як у регіоні Балтійського моря, є основою для запобігання виникненню серйозних збоїв, які, як показує щоденний досвід, можуть призвести до економічних, екологічних і навіть людських втрат [3, 65, 69].

Ненадійність критичної інфраструктури може бути виміряна ймовірністю, частотою і тривалістю небажаних подій [2, 11, 12, 21]. Безпека критичної інфраструктури означає здатність виконувати свої функції, незважаючи на те, що відбуваються випадкові небажані події [22, 24]. У такому розумінні надійність означає здатність виконувати свої функції у сталих станах функціонування системи, а безпека визначається як можливість вижити в аварійних станах. Основним показником, що визначає рівень безпеки критичної інфраструктури, є ризик, пов'язаний з її функціонуванням [31].

Аналіз безпеки вимагає визначення робочих станів. З точки зору оператора системи можна виділити такі стани:

- всі процедури дотримані, оператор приймає правильні рішення згідно з рекомендаціями та показаннями підсистем захисту від небажаних подій, збоїв немає,

- всі процедури дотримані, при прийнятті рішення оператор враховує показання захисних підсистем, однак відбувається збій,

- порушення процедур, при прийнятті рішення оператор не враховує показання захисних підсистем, збій не відбувається,

- порушення процедур, при прийнятті рішення оператор не враховує показання захисних підсистем і відбувається збій.

Таким чином можна сформулювати основні положення роботи.

Мета і завдання виконання дипломної роботи Метою дослідження є ретроспективний аналіз та оцінка потенційних загроз, вразливостей, а також розробка методів та засобів забезпечення стійкості критичної інфраструктури.

Об’єкт дослідження є критична інфраструктура, яка включає в себе електростанції, транспортні вузли, мережі зв'язку, водні та каналізаційні системи, медичні установи та інші об'єкти, що відіграють стратегічну роль для суспільства та економіки.

Предмет дослідження – є системи безпеки та стійкості цих критичних інфраструктурних об'єктів. Дослідження спрямоване на вивчення потенційних загроз, визначення вразливостей та розробку методів та засобів для забезпечення їх стійкості в умовах несприятливих чинників.

Методи дослідження, застосовані в дипломній роботі: аналітичний аналіз небезпек, аналіз стійкості об’єктів критичної інфраструктури

Наукова новизна забезпечення комплексного розуміння загроз об'єктам критичної інфраструктури та розробити ефективні стратегії їх захисту.

Практичне значення роботи. Запровадження розроблених систем дозволить підвищити загальний рівень безпеки на автозаправних станціях, знизити ризики для громадськості та оточуючого середовища.

Основні розділи роботи були обговоренні на одинадцятої міжнародній науково-технічної конференції 16 – 17 листопада 2023 року у м. Харків.

РОЗДІЛ І
ОБҐРУНТУВАННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Бізнес-кейс — це процес прийняття рішень або обґрунтування для продовження проекту чи програми. Підприємство оцінює та зважує вигоди, витрати та ризики бажаного рішення проти альтернативних варіантів вирішення виявленої проблеми чи прогалини. Складність проблеми чи можливості може спричинити глибину процесу прийняття рішень. Хоча вартість усунення інциденту безпеки піддається кількісній оцінці, відновлення пошкодженої інфраструктури та репутації важко оцінити. Вартість відновлення після інциденту безпеки може бути дорожчою, ніж вартість запобігання таким подіям. Крім того, репутаційну шкоду може бути важко повністю виправити.

1.1 Створення та обґрунтування безпеки об'єктів критичної інфраструктури

Фахівці з безпеки можуть адаптувати своє бізнес-кейс, щоб представити конкретні інвестиції в безпеку або запропонувати ширшу ініціативу, таку як конвергентні або інтегровані функції кібербезпеки та фізичної безпеки. Незалежно від інвестицій у безпеку, компоненти процесу та бізнес-обґрунтування залишаються незмінними та повинні містити загальні елементи, наведені на рисунку 1.

Рис. 1.1 Елементи для створення бізнес-обґрунтування безпеки з першого погляду

Створення команди проекту безпеки

Вибір правильної команди є критично важливим першим кроком у створенні успішного бізнес-кейсу, і його слід адаптувати відповідно до обсягу проекту. Приклади членів команди проекту безпеки включають представників фізичної безпеки організації, інформаційних технологій (IT), управління надзвичайними ситуаціями, об’єктів, фінансів/бюджету, кадрових ресурсів, юридичних, програмного менеджменту, відповідальних за основні функції місії, і функції безперервності бізнесу області. Команда повинна розглянути можливість створення статуту, схваленого керівництвом, для визначення чітких ролей, обов’язків, очікувань щодо участі, графіку проекту та графіку спілкування команди.

Проведення оцінки ризиків

Перегляньте поточний стан безпеки вашої організації та проведіть оцінку ризиків, щоб зрозуміти організаційні ризики (загрози, вразливі місця та наслідки). Ретельно задокументуйте результати оцінки, щоб допомогти визначити обґрунтування бізнес-обґрунтування та визначити всі активи, які потребують захисту, і пов’язані з ними ризики для кожного. Хоча активи залежать від організації, приклади включають секретну та конфіденційну інформацію та пов’язані з ними простори/сервери, співробітників, безперервність операцій, зацікавлених сторін та приміщення. Для проектів безпеки, пов’язаних із федеральними об’єктами, організації можуть мати змогу посилатися на свою останню оцінку ризиків, яка є вимогою ISC.

Можуть виникнути можливості для забезпечення безпеки та сталості в тому самому проекті, що забезпечує більшу загальну віддачу від інвестицій. Команда проекту повинна зв’язатися з організаційним комітетом капітальних інвестицій або аналогічною організаційною структурою, яка відповідає за планування проекту та визначення пріоритетів у рамках процесу оцінки ризиків, щоб визначити, чи розглядаються подібні ініціативи чи інвестиції. Коли питання безпеки, безпеки та сталого розвитку вирішуються одночасно з розподілом витрат, як це може бути у випадку зі скляними конструкціями

(внутрішніми та зовнішніми), обидва проекти можуть заощадити гроші, але при цьому досягти своїх індивідуальних цілей і завдань.

Після завершення оцінки ризику команда проекту розробляє аналіз вигоди і витрат, використовуючи одну з кількох доступних методологій. Ефективне повідомлення про витрати та переваги варіантів безпеки включає аналіз і визначення того, які інвестиції в безпеку слід здійснити.

Опис проекту безпеки

Використовуючи результати оцінки ризиків, команда розробляє опис проекту або програми безпеки. Цей опис є загальнорівневим оглядом, що пояснює, як передбачуване рішення безпеки впорається з одним або декількома ризиками, визначеними в оцінці ризиків

Повідомлення про вплив на бізнес

Щоб розробити цей розділ, переконайтеся, що проектна документація визначає критично важливі активи, які потребують захисту, і кількісно визначає потенційні негативні наслідки нездатності належним чином захистити ці активи від виявлених загроз. По-перше, використайте результати оцінки ризиків, будь-які доступні підтверджуючі дані та пріоритетний список рекомендацій на основі найвищого ризику та впливу. Потім розрахуйте переваги рекомендованих інвестицій у безпеку та визначте, як це позитивно вплине на організацію.

Аналіз альтернативи.

Аналіз альтернативних інвестицій у безпеку та потенційних витрат, пов’язаних із уникненням інвестицій у безпеку, підтримає вашу бізнес-аргументацію безпеки. Оцінка інших методів безпеки федерального чи приватного секторів допоможе сформувати варіанти та стратегії пом’якшення. Команди проекту повинні розглянути два-три реальні варіанти, що відповідають визначеним потребам у безпеці, і включати варіанти з вищими та нижчими витратами, коротшими чи довшими часовими рамками та іншими можливими змінними, що впливають на витрати та вигоди

Передбачення потенційних факторів опору

Передбачення заперечень щодо інвестицій у безпеку допоможе підготувати необхідну інформацію та підхід, необхідний для їх вирішення. Без мотивуючих подій лідери можуть вагатися, чи варто інвестувати в превентивні та превентивні заходи безпеки. Хоча причини часто відрізняються залежно від розміру організації, типу, місця розташування та місії, кілька поширених заперечень включають вартість, незручність, недовіру до технологій безпеки та труднощі з кількісним визначенням рентабельності інвестицій. Щоб ефективно передати необхідність інвестування в безпеку та значні ризики, пов’язані з бездіяльністю, команда проекту повинна враховувати фактори опору, які впливають на зацікавленість вищого керівництва. Наявність відповідних відповідей і підтверджуючих даних сприятиме більш сприятливому результату.

Розроблення плану впровадження, графіку і критеріїв ефективності

План впровадження описує, як організація буде виконувати стратегію інвестицій у безпеку, і розбиває стратегію на кроки, які можна визначити; ставить завдання особовому складу; надає графік проекту; і визначає віхи та показники успіху. План має включати детальний опис необхідних ресурсів, а також план комунікації щодо того, як розгортання вплине на працівників і зацікавлених сторін.

Розроблення та надання рекомендацій

На цьому останньому етапі дослідження, аналіз і рекомендації перетворюються на презентабельний бізнес-кейс. Використовуючи бажаний формат презентації організації, ділове обґрунтування безпеки має починатися з «Початкового результату», щоб орієнтувати особу, яка приймає рішення, на ключову інформацію, щодо якої вони, як очікується, мають прийняти рішення та слідувати опису проекту безпеки; вплив на бізнес; аналіз альтернатив; витрати та вигоди; план і графік реалізації; і рекомендація. Презентація також повинна включати візуальні матеріали (дані, діаграми або графіки) і достатньо детальної інформації (про запас), щоб обмежити потребу в подальших запитах на інформацію.

Управління проектами

У той час як управління проектом має вирішальне значення для результатів модернізації системи безпеки, як-от застосування контрзаходів безпеки під час масштабної модернізації федерального об’єкта, детальні методи управління проектом виходять за рамки цього документа.

Розробка аналізу вигоди і витрат

У сьогоднішньому середовищі організації безпеки повинні конкурувати за ресурси та керувати ними. Це необхідне для кращої оцінки економічної ефективності посилення безпеки на державних об’єктах, «враховуючи те, що не повністю відомо, скільки суб’єктів господарювання витрачає на вдосконалення, і що фактори вартості відрізняються залежно від об’єкта. , стає ще більш важливою ключовою практикою, щоб організації як на рівні штаб-квартири, так і на рівні об’єктів мали інструменти, необхідні для прийняття обґрунтованих рішень щодо розподілу ресурсів». Розробка аналізу вигоди і витрат є корисною для надання допомоги організаціям, коли вони шукають фінансування для контрзаходів безпеки, розробляють основні програми безпеки, досягають необхідного рівня персоналу, навчання та розробляють річні бюджетні документи.

Рис. 1.2 Дев'яти етапна методологія управління та бюджетування

Опис потреб

Перш ніж рекомендувати дію, організації повинні продемонструвати необхідність запропонованої дії, створивши досить докладний опис того, що потрібно і чому. Мета полягає в тому, щоб пояснити проблему та дії, необхідні для вирішення проблеми. Джерела, які можуть стати каталізатором таких дій, включають, але не обмежуються:

• Виявлена вразливість на основі оцінки ризику

• Відповідність нормативним або виконавчим вимогам, таким як Президентська директива про національну безпеку-12 (HSPD-12), Політика щодо загального стандарту ідентифікації для державних службовців і підрядників

•Пристосування до змін організаційної місії

•Заміна або модернізація електронних систем безпеки протягом життєвого циклу

• Додатковий штат, необхідний для задоволення вимог місії

• Збій системи або інший виявлений недолік чи вразливість, що є наслідком небажаної події чи іншого інциденту, або в рамках щорічного тестування функціональності

• Отримані уроки або інша стратегія зменшення ризиків для протидії загрозам, що розвиваються

Розробка формулювання проблеми чи можливості, що чітко визначає проблему та необхідні можливості, може бути корисною під час опису потреби

Визначення базової лінії

Основна мета базової лінії полягає в тому, щоб надати особам, які приймають рішення, картину та наслідки бездіяльності, а також вторинне використання інформаційних показників ефективності. Базовий рівень представляє поточний стан і найкращу оцінку організації того, яким був би світ за відсутності певної дії. Щоб визначити базову лінію, організації може знадобитися розглянути широкий спектр факторів, включаючи найкращий

прогноз організації щодо того, як зміниться світ у майбутньому.[7] Наприклад, організації повинні розглянути еволюцію ризиків або майбутні зміни в місії. Однак цей крок не слід плутати з «базовим рівнем захисту», який використовується в процесі управління ризиками ISC.

Встановлення часового горизонту для аналізу

Організації повинні вибрати відповідний часовий горизонт для оцінки вигоди і витрат, що охоплюють можливі результати дії. Наприклад, оновлення VSS може мати вищу вартість першого року встановлення, ніж щорічні витрати на ремонт або обслуговування існуючої системи. Тим не менш, організації можуть отримати вигоду від зниження витрат на технічне обслуговування та підвищення надійності протягом усього терміну служби нової системи. Таким чином, аналіз повинен охоплювати багаторічний період, щоб розглянути витрати протягом життєвого циклу. Крім того, потрібно враховувати щорічне тестування, переваги від оновлення безпеки та витрати на обслуговування.

Вартість життєвого циклу можна визначити як загальну вартість уряду ініціативи чи програми протягом повного терміну її існування, включаючи витрати на дослідження та розробки, тестування, виробництво, обладнання, експлуатацію, технічне обслуговування, персонал, відповідність екологічним вимогам та утилізацію. [8] Комплексна оцінка витрат протягом життєвого циклу допомагає особам, які приймають рішення, оцінити довгострокову доступність ініціативи/програми. Оцінку слід проаналізувати та впорядкувати з огляду на виникнення, оскільки деякі витрати є одноразовими, тоді як інші витрати генеруються кожного разу, коли виробляється товар або виконується послуга.

Визначення низки альтернатив

Розглядаючи низку потенційно ефективних рішень або стратегій зменшення ризиків, організації зможуть усунути деякі альтернативи шляхом попереднього аналізу, залишаючи керовану кількість альтернатив для оцінки.

Кількість і вибір альтернатив, обраних для детального аналізу, є питанням судження.

Вибираючи альтернативи, слід зосередитися на сферах зі значним впливом, таких як порівняльний аналіз ризиків9 або основні чинники витрат. Додаток А містить фактори, міркування та приклад сценарію, який організації можуть використовувати при розробці альтернатив, включаючи рішення щодо ресурсів; підходи, орієнтовані на постачальника, або альтернативні варіанти фінансування; послуги, що базуються на об'єктивних цілях або результатах; мінімальні стандарти та вимоги залежно від розміру; контроль виконання; методи примусового виконання; строгість; дати реалізації; і вимоги, засновані на географічних та інших обмеженнях.

Визначення наслідків альтернатив

Після визначення можливих і потенційно ефективних альтернатив наступним кроком є визначення потенційних вигод і витрат. Може бути корисно визначити витрати таким чином:

• Вигоди та витрати, які можна монетизувати

• Вигоди та витрати, які можна виразити кількісно, але не монетизувати

• Вигоди та витрати, які не піддаються кількісній оцінці

Окрім прямих вигоди і витрат, визначте очікувані небажані побічні ефекти та додаткові переваги альтернатив. Наприклад, якщо метою є пом'якшення внутрішньої загрози, але альтернатива також може зменшити ймовірність успіху іншої злочинної діяльності, прямі вигоди та витрати слід додати відповідно. Також важливо відзначити, чому конкретну альтернативу було відхилено порівняно з бажаною альтернативою або запропонованим варіантом.

Нарешті, організації повинні звернути увагу на тих, хто несе витрати на базову лінію, пропоновані заходи та альтернативи, і тих, хто користується перевагами, часто не однакові. Це називається «ефектом розподілу» і описує вплив, який альтернатива створює на різні сторони. Якщо ефект розподілу існує, його слід включити в аналіз.

Монетизування вигоди та витрати

Організації повинні шукати найкращі обґрунтовано доступні дані для кількісної оцінки ймовірних переваг і витрат запропонованого варіанту та кожної альтернативи. Представлення вигоди і витрат у фізичних одиницях на додаток до грошових одиниць дає повну картину пропонованого економічного обґрунтування. Завершуючи аналіз, організації повинні включити такі елементи, як адміністративні витрати та заощадження або приріст/втрати продуктивності чи ефективності.

Кількісна оцінка переваг

Переваги, які піддаються кількісній оцінці, мають числове значення, наприклад долари, фізичну кількість матеріальних речей або відсоткову зміну. Переваги можуть випливати зі скорочення витрат або економії через зміни базової лінії. Перевагою альтернативи може бути зменшення ймовірності небажаної події або зменшення наслідків такої події.

Витрати

Детальний аналіз та визначення базової лінії є фундаментальними для визначення додаткових витрат і економії коштів для запропонованих дій та альтернатив. Посилаючись на оцінку базової лінії, виконану на Кроці 2 методології OMB, опишіть, що вже доступно, що зараз відбувається, а потім кількісно визначте базові елементи. Розглянемо витрати, які вже були понесені в базовій оцінці.:

• Витрати на експлуатацію та підтримку

• Витрати на персонал або допоміжну робочу силу

• Витрати на інформаційні технології

• Профілактичне обслуговування та ремонт

• Інші періодичні або випадкові витрати

• Витрати на контракти та закупівлі

Створення структури розподілу робіт [10] або іншої структури витрат встановлює вартість кожного елемента, забезпечує структуру та зменшує надмірність у оцінках витрат. Розгляньте витрати протягом життєвого циклу

за допомогою плану управління ресурсами, який охоплює всі етапи корисного використання продукту, від початкового етапу планування до розгортання для кінцевого користувача. Крім того, обов'язково задокументуйте основні правила та припущення. Шаблон аналізу витрат ISC Making a Business Case – Cost Analysis Template [11] був створений, щоб допомогти організаціям розрахувати витрати.

Знижка на майбутні витрати та вигоди (необов'язковий крок)

Дисконтування дозволяє порівняти переваги та витрати безпеки, які мали місце в минулому, з можливими подіями в майбутньому. Витратити гроші зараз є альтернативна вартість, але й переваги з'являться раніше, ніж пізно. Альтернативна вартість означає, що гроші, витрачені на запропонований варіант, можуть бути витрачені на щось інше, інвестовані або використані для зменшення боргу. У більшості випадків організаціям не потрібно дисконтувати витрати та вигоди.

Оцінка некількісних та не монетизованих вигоди та витрати

Деякі вигоди та витрати, як-от стримування інциденту безпеки, не піддаються прямому кількісному аналізу. Стримування — це принцип безпеки, якого часто прагнуть професіонали з безпеки шляхом «зміцнення цілі» або зменшення «привабливості цілі». Здатність запобігти виникненню інциденту безпеки або UE не піддається кількісному виміру через складність визначення кількості атак, які вдалося відвернути на основі запропонованих заходів безпеки. Переваги, які не підлягають кількісному вимірюванню, покладаються на якісний наратив, щоб додати цінність аналізу. Переваги та витрати, які важко оцінити кількісно та монетизувати, можна оцінити за допомогою аналізу беззбитковості чи порогового значення або розробки таблиці переваг, яка не піддається кількісному вимірюванню.

Аналіз беззбитковості

Якщо неможливо кількісно визначити або монетизувати ключові компоненти переваги заходів безпеки, організації можуть провести аналіз беззбитковості (або порогового значення), порівнюючи оцінені витрати на

впровадження заходів безпеки з розрахунковою грошовою вартістю уникнення успішної атаки. . Аналіз беззбитковості використовує оцінку прямих наслідків небажаної події, таких як травми; втрата життя; переривання роботи/послуги на місці; негайні витрати на відновлення; шкоди майну та інфраструктурі, а також навколишньому середовищу. Наприклад, прямі наслідки відверненого або стриманого інциденту з безпекою (або відвернені витрати) включають монетизовану вартість уникнутих смертельних випадків, несмертельних травм і госпіталізацій, пошкодження майна, а також витрати на порятунок і очищення. Поділ відвернених витрат на інцидент безпеки або наслідком небажаної події на річну вартість заходів безпеки призводить до кількості таких інцидентів, яких слід уникати на річній основі, щоб вигоди дорівнювали витратам. Непрямий наслідок – це ефект, не пов’язаний із подією, інцидентом чи подією, але спричинений прямим наслідком, наступними каскадними ефектами та/або пов’язаними рішеннями.

Розглядаючи аналіз переваг безпеки, важливо прив’язати ефективність запропонованих контрзаходів до інциденту безпеки або наслідком небажаної події. Таким чином, організації повинні розглядати сценарії, коли обґрунтовано очікується, що захід безпеки зменшить вірогідність сценарію. Наприклад, якщо захід спрямований на запобігання внутрішньої загрози, слід оцінити прямі наслідки інциденту безпеки внутрішньої загрози. Якщо заходи, які розглядаються, спрямовані на зниження ризику кіберзагрози, можливе кіберзлом і прямі наслідки порушення можуть бути використані в аналізі беззбитковості. CISA опублікувала звіти про витрати на кіберінциденти, які можуть служити орієнтиром для оцінки кібервитрат.[15]

Переваги, що не підлягає кількісному вимірюванню

Під час обґрунтування безпеки може бути корисно показати переваги, які не підлягають кількісному вимірюванню, з точки зору безпеки та переваги, не пов’язані з безпекою. Перелік переваг, які не підлягають кількісному вимірюванню, буде задокументовано в детальному поясненні в

рамках аналізу витрат протягом життєвого циклу з сильними якісними заявами. Організації можуть класифікувати переваги, які не підлягають кількісному вимірюванню (подібно до вимірних), для кожної альтернативи на основі їх відповідності меті та аналізу.

Охарактеризуйте невизначеність у вигодах, витратах і чистих вигодах

Будь-якому прогнозу майбутніх умов властива невизначеність. Аналітики повинні спробувати охарактеризувати джерела, природу та обмеження через невизначеність. Організації повинні розробити перелік потенційних припущень та/або сценаріїв для аналізу впливу невизначеності на базові та альтернативні варіанти. Наприклад:

• Як довго очікується, що обладнання безпеки прослужить за належного обслуговування?

• Який прогноз звіту про загрозу проектування щодо зазначеного наслідком небажаної події?

• Як довго організація, як очікується, залишатиметься на поточному місці?

• Чи передбачені зміни в місії організації?

1.2 Вибір економічно ефективних або альтернативних рішень

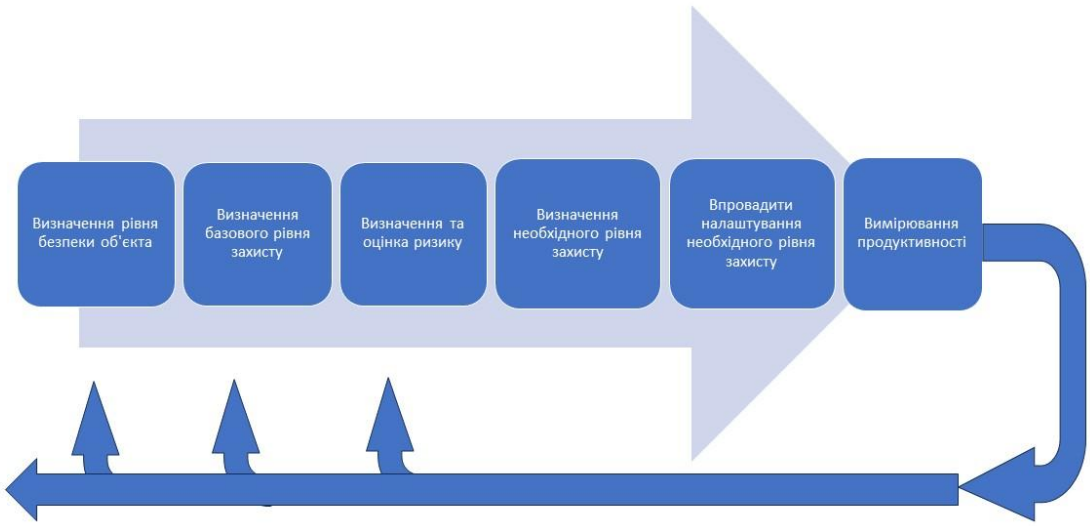
Адміністративно-бюджетне управління рекомендує організаціям порівнювати до чотирьох окремих варіантів. До них належать базовий рівень (статус-кво) з кращим варіантом, більш сувора та менш сувора альтернатива, а також переваги та вартість можливостей.[16] Процес вибору має відображати повний спектр переваг та витрат, включаючи технічне обслуговування, мікропрограмне забезпечення/ оновлення програмного забезпечення та заміна життєвого циклу.

Бувають випадки, коли організація не зробила б вибір шляхом порівняльного аналізу альтернатив. Прикладом є ситуація, коли комітет з безпеки об’єкта або представник орендаря для об’єктів з одним орендарем

(надалі «відповідальний орган») дотримуються ПУР і визначають досяжний рівень захисту. У таких випадках відповідальний орган працює з організацією безпеки, щоб визначити менш сувору альтернативу у формі найвищого досяжного рівня захисту через ітеративний процес перевірки контрзаходів, визначених у ПУР.

Застосування в рамках процесу управління ризиками

ПУР визначає критерії та процеси, які особи, відповідальні за безпеку об’єкта, повинні використовувати для визначення рівня безпеки об’єкта та необхідного рівень захисту. Цей стандарт забезпечує інтегроване, єдине джерело засобів протидії фізичній безпеці та вказівки щодо налаштування протизаходів для всіх невійськових федеральних об’єктів. ПУР визначає досяжний рівень захисту, співмірний або максимально близький до рівня ризику, не перевищуючи рівень ризику. Щоб досягти цього, ПУР описує



шести етапний підхід, показаний на рисунку 1.3.

Рис. 1.3 Процес управління ризиками

Оцінка ризиків

ПУР вимагає проведення оцінки ризиків для федеральних об’єктів організацією безпеки об’єкта раз на п’ять років для об’єктів рівня безпеки [17] (FSL) I та II та раз на три роки для об’єктів FSL III, IV та V. Тому

доцільно залучати охоронні організації на ранньому етапі процесу планування та проектування проектів будівництва чи модернізації. На додаток до оцінки ризиків організації безпеки несуть відповідальність за рекомендації відповідних контрзаходів. Від відповідального органу вимагається або реалізувати рекомендації, або прийняти ризик як частину стратегії управління ризиками об'єкта.

У ПУР наголошується на оцінці економічної ефективності та вимірюванні продуктивності як частини суворого підходу до управління ризиками для ефективного розподілу ресурсів.[18] Коли вразливість виявлена та рекомендована стратегія зменшення ризику, відповідальний орган має прийняти рішення: продовжити виконання рекомендації, застосувати альтернативний (нижчий рівень) контрзахід або прийняти ризик. У таких випадках розробка бізнес-обґрунтування безпеки за допомогою BCA може бути цінним інструментом для отримання ресурсів, необхідних для впровадження відповідної стратегії зменшення ризиків. Розробка BCA відбуватиметься під час кроку 4: визначення необхідного або досяжного рівня безпеки. Якщо відповідальний орган влади вирішить прийняти ризик, аналіз і зусилля з обґрунтування безпеки можуть бути корисними під час наступного бюджетного циклу або інших можливостей фінансування в майбутньому.

Організації також можуть знайти BCA корисним у нетрадиційних способах підтримки контрзаходів, пов'язаних із політикою. Наприклад, видача працівникам карток підтвердження особи (PIV) потребує штату. Організаціям потрібно буде визначити, чи буде штат забезпечуватись поточними працівниками чи знадобляться додаткові працівники. Якщо організація обирає додатковий персонал, то розробка надійного бізнес-кейсу має допомогти організації отримати необхідні ресурси для реалізації своїх планів.

Вимірювання успіху

Вимірювання успіху має центральне значення для того, щоб організації безпеки могли продемонструвати лідерству позитивну рентабельність інвестицій. Вимірюючи успішність бізнес-обґрунтування безпеки, більшість організацій зосереджуються на якісних або кількісних показниках. Наприклад, вигоди, які піддаються кількісній оцінці, є фінансовими та можуть вимірювати уникнення витрат, скорочення витрат або економію коштів. І навпаки, кількісно невизначені атрибути можуть представляти внутрішні цінності, такі як мораль, задоволення або якість.

Показники ефективності

Щоб розробити вимірювання ефективності, спочатку визначте конкретні цілі або цілі, сформулювавши «як виглядає успіх». По-друге, визначте категорію вимірювання ефективності та, нарешті, окресліть, які конкретні дії чи заходи будуть вжиті.

Незалежно від того, який тип винагороди використовується для вимірювання успіху, організація повинна спочатку знати свою базову лінію для порівняння. Після встановлення базової лінії заходи запитуються знову у встановлений час (після встановлення/встановлення затвердженої опції безпеки), щоб перевірити, чи можна спостерігати будь-які зміни. У таблиці 6 наведено приклади деяких вимірювань ефективності, які використовуються для підтримки бізнес-кейсів.

РОЗДІЛ ІІ
ПРОЦЕС ОЦІНКИ РИЗИКІВ

У рамках системи управління ризиками COSO ERM2 оцінка ризиків слідує за ідентифікацією подій і передує реагуванню на ризики. Її мета - оцінити, наскільки великими є ризики, як індивідуальні, так і сукупні, щоб зосередити увагу керівництва на найважливіших загрозах і можливостях, а також закласти підґрунтя для реагування на ризики. Оцінка ризиків полягає у вимірюванні та визначенні пріоритетності ризиків таким чином, щоб управляти рівнями ризиків у межах визначених порогів толерантності, не допускаючи надмірного контролю і не втрачаючи бажаних можливостей. Подіями, які можуть ініціювати оцінку ризиків, є початкове створення програми ОУР, періодичне оновлення, початок нового проекту, злиття, поглинання або продаж, а також значна реструктуризація. Деякі ризики є динамічними і потребують постійного поточного моніторингу та оцінки, наприклад, певні ринкові та виробничі ризики. Інші ризики є більш статичними і потребують періодичної переоцінки, причому постійний моніторинг ініціює оповіщення про необхідність швидкої переоцінки у разі зміни обставин.

2.1 Ідентифікація ризиків.

Процес ідентифікації ризиків (або подій) передує оцінці ризиків і створює вичерпний перелік ризиків (а часто і можливостей), згрупованих за категоріями ризиків (фінансові, операційні, стратегічні, комплаєнс) та підкатегоріями (ринкові, кредитні, ліквідності тощо) для бізнес-підрозділів, корпоративних функцій та капітальних проектів. На цьому етапі створюється широка мережа для розуміння сукупності ризиків, що складають профіль ризиків підприємства. Хоча кожен зафіксований ризик може бути важливим для керівництва на рівні функцій і бізнес-підрозділів, список вимагає визначення пріоритетів, щоб зосередити увагу вищого керівництва і ради

директорів на ключових ризиках. Таке визначення пріоритетів досягається шляхом проведення оцінки ризиків. Розробка критеріїв оцінки.

Першим кроком у процесі оцінки ризиків є розробка загального набору критеріїв оцінки, які будуть застосовуватися в усіх бізнес-підрозділах, корпоративних функціях і великих капітальних проектах.

Ризики та можливості зазвичай оцінюються з точки зору впливу та ймовірності. Багато підприємств визнають корисність оцінки ризику за додатковими параметрами, такими як вразливість і швидкість настання.

Оцінка ризиків полягає у визначенні значущості кожного ризику та можливості за визначеними критеріями. Це може бути здійснено у два етапи, коли початковий скринінг ризиків виконується за допомогою якісних методів, а потім проводиться кількісний аналіз найбільш важливих ризиків. Оцініть взаємодію ризиків. Ризики не існують ізольовано. Підприємства усвідомили важливість управління взаємодією ризиків. Навіть незначні на перший погляд ризики самі по собі мають потенціал, взаємодіючи з іншими подіями та умовами, завдати великої шкоди або створити значні можливості. Тому підприємства тяжіють до інтегрованого або цілісного погляду на ризики, використовуючи такі методи, як матриці взаємодії ризиків, діаграми "краватка-метелик" та агреговані розподіли ймовірностей. Визначте пріоритетність ризиків.

Пріоритизація ризиків - це процес визначення пріоритетів в управлінні ризиками шляхом порівняння рівня ризику із заздалегідь визначеними цільовими рівнями ризику та пороговими значеннями толерантності. Ризик розглядається не лише з точки зору фінансового впливу та ймовірності, але й суб'єктивних критеріїв, таких як вплив на здоров'я та безпеку, репутацію, вразливість та швидкість настання.

Реагування на ризики. Результати процесу оцінки ризиків слугують основною інформацією для реагування на ризики, під час якого розглядаються варіанти реагування (прийняти, зменшити, поділити або уникнути), проводиться аналіз витрат і вигод, формулюється стратегія

реагування та розробляються плани реагування на ризики. Обговорення питань ідентифікації подій та реагування на ризики виходить за рамки цього документу. Для детального розгляду зверніться до COSO Enterprise Risk Management - Integrated Framework (2004).

Розробка критеріїв оцінки.

Традиційний аналіз ризиків визначає ризик як функцію ймовірності та впливу. Дійсно, це важливі показники. Однак малоймовірні події трапляються надто часто, а багато ймовірних подій не відбуваються. Гірше того, малоймовірні події часто відбуваються з дивовижною швидкістю.

Ймовірність та вплив самі по собі не дають повної картини. Щоб відповісти на питання, як швидко може виникнути ризик, як швидко ви можете відреагувати або відновитися, і скільки часу ви можете витримати простою, вам потрібно оцінити вразливість і швидкість настання події. Визначивши, наскільки ви вразливі до події, ви отримаєте уявлення про свої потреби. Оцінюючи, як швидко це може статися, ви розумієте необхідність гнучкості та швидкої адаптації.

Розробка шкал оцінювання Необхідна певна форма вимірювання ризиків. Без стандарту порівняння просто неможливо порівнювати та агрегувати ризики в організації. Більшість організацій визначають шкали для оцінки ризиків з точки зору впливу, ймовірності та інших вимірів. Ці шкали включають рівні оцінювання та визначення, які сприяють узгодженому тлумаченню та застосуванню різними групами. Чим більш описовими є шкали, тим більш послідовною буде їхня інтерпретація користувачами. Хитрість полягає в тому, щоб знайти правильний баланс між простотою та всеосяжністю.

Шкала повинна дозволяти значущу диференціацію для цілей ранжування та визначення пріоритетів. П'ятибальна шкала дає кращу дисперсію, ніж трибальна. Десятибальна шкала передбачає точність, яка зазвичай невиправдана в якісному аналізі, і експерти можуть витратити час,

намагаючись визначити різницю між оцінкою в шість або сім балів, коли різниця несуттєва і невиправдана.

Ілюстративні шкали надаються для впливу, ймовірності, вразливості та швидкості настання. Кожне підприємство відрізняється від інших, і шкали повинні бути адаптовані до галузі, розміру, складності та культури організації, про яку йде мова.

Вплив (або наслідок) - це ступінь, до якого подія ризику може вплинути на підприємство. Критерії оцінки впливу можуть включати фінансовий, репутаційний, регуляторний вплив, вплив на здоров'я, безпеку, охорону праці, навколишнє середовище, працівників, клієнтів та операційну діяльність. Підприємства зазвичай визначають вплив, використовуючи комбінацію цих видів впливу (як показано нижче), враховуючи, що певні ризики можуть мати фінансовий вплив на підприємство, в той час як інші ризики можуть мати більший вплив на репутацію або здоров'я та безпеку. Присвоюючи рейтинг впливу ризику, присвоюйте рейтинг найвищому очікуваному наслідку. Наприклад, якщо виконується будь-який з критеріїв для оцінки 5, то оцінка впливу дорівнює 5, навіть якщо інші критерії можуть бути нижчими за шкалою. Деякі організації визначають шкалу впливу як для можливостей, так і для ризиків.

Таблиця 2.1.1

Ілюстративна шкала впливу

Рейтинг	Дескриптор	Визначення
5	Екстремальний	- Фінансові втрати в розмірі X мільйонів або більше 3 - Довготривале негативне висвітлення в міжнародних ЗМІ; втрата частки ринку, що змінює правила гри - Значні судові переслідування та штрафи, судові процеси, включаючи колективні позови, ув'язнення керівництва

		- Значні травми або смертельні випадки серед працівників або третіх осіб, таких як клієнти чи постачальники - Звільнення кількох керівників вищого рангу
4	Високий	- Фінансові втрати від X мільйонів до X мільйонів - Довготривале негативне висвітлення в національних ЗМІ; значна втрата частки ринку - Звіт до регуляторного органу, що вимагає великого проекту для виправлення ситуації - Обмежений стаціонарний догляд, необхідний для працівників або третіх осіб, таких як клієнти або постачальники - Деякі топ-менеджери звільняються, висока плинність досвідчених кадрів, компанія не сприймається як кращий роботодавець.
3	Помірний	- Фінансові втрати від X мільйонів до X мільйонів - Короткострокове негативне висвітлення в національних ЗМІ - Звіт про порушення регулятору з вимогою негайного виправлення - Амбулаторне медичне лікування, необхідне працівникам або третім особам, таким як клієнти чи постачальники - Широкомасштабні проблеми з моральним духом персоналу та висока плинність кадрів.

2	Незначний	- Фінансові втрати від X мільйонів до X мільйонів - Пошкодження місцевої репутації - Повідомлення про інцидент регулятору, без подальших дій - Відсутність або незначні травми працівників або третіх осіб, таких як клієнти чи постачальники - Загальні проблеми з моральним духом персоналу та збільшення плинності кадрів
1	Випадково	- Фінансові втрати до X мільйонів - Увага місцевих ЗМІ була швидко виправлена - Не підлягає звітності перед регулятором - Не постраждали працівники або треті особи, такі як клієнти або постачальники - Поодинокі випадки незадоволення з боку персоналу

Вірогідність - це можливість того, що певна подія відбудеться. Ймовірність може бути виражена якісними термінами (часта, ймовірна, можлива, малоймовірна, рідкісна), відсотковою ймовірністю або частотою. При використанні числових значень, таких як відсоток або частота, необхідно вказати відповідний період часу, наприклад, річну частоту або більш відносну ймовірність протягом терміну експлуатації проекту або активу. Іноді підприємства описують ймовірність у більш особистих і якісних термінах, таких як "подія, яка, як очікується, відбудеться кілька разів протягом кар'єри" або "подія, яка, як очікується, не відбудеться протягом кар'єри".

Таблиця 2.1.2

Ілюстративна шкала правдоподібності

Рейтинг	Щорічна періодичність		Ймовірність	
	Дескрип-тор	Визначення	Дескр-иптор	Визначення
5	Часті	До одного разу на 2 роки або частіше	Майже впевне ний.	90% або більша ймовірність виникнення протягом терміну експлуатації активу або проекту
4	Ймовірно	Один раз на 2 роки до одного разу на 25 років	Ймовір но	65% до 90% ймовірності виникнення протягом терміну експлуатації активу або проекту
3	Можливо	Один раз на 25 років до одного разу на 50 років	Можли во	Від 35% до 65% ймовірності виникнення протягом терміну експлуатації активу або проекту
2	Мало-ймовірно	Один раз на 50 років до одного разу на 100 років	Мало-ймовір но	Від 10% до 35% ймовірності виникнення протягом терміну експлуатації активу

				або проекту
1	Рідкісний	Раз на 100 років або менше	Рідкісний	<10% ймовірність виникнення протягом терміну експлуатації активу або проекту

Вразливість - це вразливість організації до ризикової події з точки зору критеріїв, пов'язаних з готовністю, маневреністю та адаптивністю організації. Вразливість пов'язана з впливом та ймовірністю. Чим більш вразливою є організація до ризику, тим більшим буде вплив, якщо подія відбудеться. Якщо заходи реагування на ризики, включно з контролем, не впроваджені та не функціонують належним чином, ймовірність настання події зростає. Оцінка вразливості дозволяє організаціям визначити, наскільки добре вони управляють ризиками. Критерії оцінки вразливості можуть включати здатність передбачати події, наприклад, планування сценаріїв, реальні варіанти4 , здатність запобігати подіям, наприклад, реагування на ризики, здатність швидко реагувати та адаптуватися в міру розгортання подій, а також здатність протистояти подіям, наприклад, буфер капіталу та фінансова стійкість. Також можуть бути враховані інші фактори, такі як швидкість змін у галузі або організації. Не існує універсальної шкали оцінювання. Кожна організація повинна визначити шкалу відповідно до своїх потреб.

Таблиця 2.1.3

Ілюстративна шкала вразливості

Рейтинг	Дескриптор	Визначення
5	Дуже високий	- Не здійснюється планування сценаріїв - Відсутність можливостей на рівні підприємства/процесу для управління ризиками - Реакції не впроваджуються - Відсутність планів управління на випадок непередбачуваних

		ситуацій або кризових ситуацій
4	Високий	- Здійснено сценарне планування для ключових стратегічних ризиків - Низький рівень спроможності на рівні підприємства/процесу щодо управління ризиками - Реагування здійснюється частково або не досягає цілей контролю - Наявні деякі плани управління на випадок непередбачених обставин або кризових ситуацій
3	Середній	- Проведено стрес-тестування та аналіз чутливості сценаріїв - Середні можливості для управління ризиками на рівні підприємства/процесу - Реагування впроваджено та досягнуто цілей у більшості випадків - Більшість планів управління в надзвичайних ситуаціях та кризових ситуаціях впроваджено, обмежена кількість репетицій
2	Низький	- Визначені стратегічні варіанти - Середні та високі можливості на рівні підприємства/процесу щодо управління ризиками - Реагування впроваджено та досягнуто цілей, за винятком екстремальних умов - Плани управління на випадок надзвичайних ситуацій та кризових ситуацій впроваджено, проведено кілька репетицій.
1	Дуже низький	• Розгортання реальних варіантів для максимізації стратегічної гнучкості • Можливості високого рівня підприємства/процесу для вирішення ризиків

		• Наявність резервних механізмів реагування, які регулярно перевіряються на критичні ризики • Наявні плани на випадок надзвичайних ситуацій і врегулювання кризових ситуацій, які регулярно відпрацьовуються

Швидкість початку.

Швидкість настання означає час, потрібний для прояву ризикової події, або, іншими словами, час, який минув між настанням події та моментом, коли компанія вперше відчула її наслідки. Знати швидкість початку корисно під час розробки планів реагування на ризик.

Внутрішній і залишковий ризик

Оцінюючи ризики, важливо визначити, чи буде респондентам запропоновано оцінити невід'ємний ризик, залишковий ризик або обидва. В «Управлінні ризиками підприємства – Інтегрована структура» (2004) COSO визначає невід'ємний ризик як ризик для суб'єкта господарювання за відсутності будь-яких дій, які керівництво може вжити для зміни ймовірності або впливу ризику. Залишковий ризик - це ризик, який залишається після відповіді керівництва на ризик. Застосувати цю концепцію складніше, ніж може здатися на перший погляд. Деякі суб'єкти тлумачать невід'ємний ризик як рівень ризику, припускаючи, що поточні заходи реагування не вдасться, а залишковий ризик – це рівень ризику, припускаючи, що існуючі заходи реагування працюють згідно з проектом. Інші суб'єкти господарювання трактують невід'ємний ризик як поточний рівень ризику, припускаючи, що існуючі заходи реагування діють згідно з проектом, а залишковий – це розрахунковий ризик після введення заходів реагування, які розглядаються. Перший підхід більше зосереджений на ефективності контролю поточного середовища, а другий підхід – на оцінці варіантів реагування на ризик. Немає однієї правильної відповіді, і будь-який підхід може бути корисним залежно від мети оцінки та характеру ризиків, що розглядаються.

2.2 Оцінка ризиків

Оцінка ризику часто виконується як двоетапний процес. Початковий скринінг ризиків і можливостей виконується з використанням якісних методів, а потім більш кількісна обробка найважливіших ризиків і можливостей, які піддаються кількісній оцінці (не всі ризики піддаються кількісному виміру). Якісна оцінка складається з оцінки кожного ризику та можливості відповідно до описових шкал, як описано в попередньому розділі. Кількісний аналіз потребує числових значень як впливу, так і ймовірності з використанням даних із різних джерел.

Якість аналізу залежить від точності та повноти числових значень і валідності використаних моделей. Припущення та невизначеність моделі слід чітко повідомити та оцінити за допомогою таких методів, як аналіз чутливості.

Як якісні, так і кількісні методики мають переваги та недоліки. Більшість підприємств починають з якісних оцінок і з часом розвивають кількісні можливості відповідно до потреб прийняття рішень.

Для якісного оцінювання найбільш часто використовуваними методами оцінювання є інтерв'ю, міжфункціональні семінари, опитування, порівняльний аналіз та аналіз сценаріїв. Кількісні методи варіюються від бенчмаркінгу та аналізу сценаріїв до генерування перспективних точкових оцінок (детерміновані моделі), а потім до генерування прогнозних розподілів (ймовірнісні моделі). Деякі з найпотужніших імовірнісних моделей з точки зору всього підприємства включають моделі причинно-наслідкового ризику, які використовуються для оцінки валового прибутку, грошових потоків або доходів за певний часовий горизонт із заданими рівнями довіри.

Аналіз існуючих даних

Перегляд внутрішніх і зовнішніх даних може допомогти людям оцінити ймовірність і вплив ризику або можливості. Джерела даних про

виникнення ризику включають внутрішні та зовнішні аудиторські звіти, публічні документи, страхові претензії та дані внутрішніх подій про збитки, включаючи випадки, опубліковані страховими компаніями, галузевими консорціумами та дослідницькими організаціями. Хоча покладання на наявні дані забезпечує об’єктивність, важливо оцінити релевантність даних у поточних і прогнозованих умовах. Коригування можуть бути виправдані за допомогою експертної оцінки. У цих випадках обґрунтування коригувань має бути чітко задокументовано та повідомлено.

Інтерв'ю та крос-функціональні семінари

Оцінювання можна проводити за допомогою індивідуальних інтерв’ю або фасилітованих зустрічей. Міжфункціональні семінари є кращими, ніж інтерв’ю чи опитування з метою оцінювання, оскільки вони сприяють розгляду ризикових взаємодій і руйнують відокремлене мислення. Семінари покращують розуміння ризику, об’єднуючи різні точки зору. Наприклад, при розгляді такого ризику, як порушення інформаційної безпеки, учасники семінару з інформаційних технологій, юриспруденції та комплаєнсу, зв’язків з громадськістю, обслуговування клієнтів, стратегічного планування та управління операціями можуть надати різну інформацію щодо причин, наслідків, ймовірності та взаємодії ризиків . Співбесіди можуть бути більш доцільними для вищого керівництва, членів правління та вищих лінійних керівників через обмеження часу. Семінари можуть не працювати добре в культурах, які пригнічують вільний обмін інформацією або розбіжними думками.

Опитування

Опитування корисні для великих, складних і територіально розподілених підприємств або там, де культура пригнічує відкрите спілкування. Результати опитування можна завантажити в аналітичні інструменти, що дає змогу переглядати ризики та можливості за рівнями (члени правління, керівники, менеджери), за бізнес-підрозділами, за географією чи категорією ризику.

Опитування також мають недоліки. Частота відповідей може бути низькою. Якщо опитування анонімне, може бути важко виявити прогалини в інформації. Якість відповідей може бути низькою, якщо респонденти поверхово приділяють запитання опитування, поспішаючи завершити, або якщо вони щось неправильно розуміють і не мають можливості поставити уточнюючі запитання. Але, мабуть, найбільше респонденти не отримують користі від міжфункціональних обговорень, які підвищують обізнаність людей про ризики та розуміння ними, надають контекст і інформацію для підтвердження оцінок ризиків і аналізують взаємодію ризиків між ізоляцією. З цих причин опитування не слід розглядати як заміну семінарам та іншим методам поглибленого аналізу ключових ризиків.

Бенчмаркінг – це спільний процес між групою організацій. Порівняльний аналіз зосереджується на конкретних подіях або процесах, порівнює показники та результати за допомогою загальних показників і визначає можливості покращення. Дані про події, процеси та заходи створюються для порівняння ефективності. Деякі компанії використовують порівняльний аналіз, щоб оцінити ймовірність і вплив потенційних подій у галузі. Дані порівняльного аналізу доступні в дослідницьких організаціях, галузевих консорціумах, страхових компаніях і рейтингових агентствах, державних установах, а також регуляторних і наглядових органах. Наприклад, компанія, що надає нафтопромислові послуги, може порівняти свій ризик безпеки, використовуючи такі показники, як травми з втратою робочого часу, використовуючи дані для подібних компаній.

2.3 Сценарний аналіз ризику

Сценарний аналіз давно визнаний корисним у стратегічному плануванні. Він також корисний для оцінки ризиків та їхньої прив'язки до стратегічних цілей. Він передбачає визначення одного або декількох сценаріїв ризику, деталізацію ключових припущень (умов або рушійних сил),

які визначають серйозність впливу, та оцінку впливу на ключову мету. У наведеному нижче прикладі керівництво хотіло зрозуміти, як це може негативно вплинути на прибуток. Було визначено шість сценаріїв, що впливають на прибуток, визначено причинно-наслідкові фактори (такі як зміни цін, обсягів або стан економіки), відкалібровано детальні припущення та оцінено вплив на прибуток. Сценарії можуть бути розроблені спільно власниками ризиків і персоналом ОУР, а також побудовані і затверджені фахівцями з різних функцій і керівництва.

Причинно-наслідкові моделі Валова маржа під ризиком (GMaR), Грошовий потік під ризиком (CFaR) та Прибуток під ризиком (EaR) - це показники, побудовані на основі причинно-наслідкових моделей, де конкретні фактори ризику зумовлюють майбутню невизначеність ключових компонентів грошових потоків або прибутків. Кожен фактор ризику може бути детально змодельований і включений в загальну модель. Використання причинно-наслідкової моделі ризику може дати уявлення про те, як історичні взаємозв'язки можуть розірватися і суттєво відхилитися від очікувань.

Озброївшись знаннями про те, як кожен фактор ризику може змінитися в майбутньому і вплинути на грошові потоки або прибутки, ризик можна краще вимірювати і управляти ним. Саме додаткове розуміння факторів ризику, що спричиняють невизначеність, робить причинно-наслідкові моделі кроком вперед порівняно з простою екстраполяцією минулих взаємозв'язків у рамках проформа-підходу.

Насправді, як проформа-моделі, побудовані на історичних співвідношеннях, так і причинно-наслідкові моделі ризику можуть бути корисними і повинні розглядатися як взаємодоповнюючі погляди на невизначене майбутнє. Незалежно від типу моделі, слід чітко визначити рівень довіри до оцінок рівнів ризику та припущень, зроблених під час аналізу.

Вхідні дані моделі можуть бути отримані з минулих записів, відповідного досвіду, відповідної опублікованої літератури, маркетингових

досліджень, консультацій з громадськістю, експериментів і прототипів, а також економічних, інженерних та інших моделей. Якщо історичні дані недоступні, не релевантні або неповні, може бути використано експертне опитування. Опитування експертів найчастіше використовується для оцінки обґрунтованої ймовірності, особливо для малоймовірних подій з високим рівнем впливу. Експерти є цінним джерелом інформації та знань. Але експерти також привносять упередження. На щастя, існує великий масив знань про евристику та упередження, а також способи їх подолання.

Оцінка взаємодії ризиків

ОУР дає змогу отримати інтегрований і цілісний погляд на ризики. Ключовим моментом тут є те, що ціле не дорівнює сумі частин. Щоб зрозуміти ризик портфеля, потрібно розуміти ризики окремих елементів плюс їхню взаємодію, зумовлену наявністю природних хеджів і ризиків, що взаємно підсилюють один одного. Розуміння взаємодії ризиків і подальше управління ними вимагає подолання ізоляції.

Простий спосіб розглянути взаємодію ризиків - згрупувати пов'язані ризики в широку зону ризику (наприклад, згрупувати ризики, пов'язані з джерелами постачання, каналами дистрибуції, концентрацією постачальників тощо, в ризик ланцюга постачання), а потім призначити відповідальних за цю зону ризику і нагляд за нею.

Три чіткі способи відображення взаємодії ризиків, що зростають за рівнем складності та багатства інформації, - це карти взаємодії ризиків, кореляційні матриці та діаграми-метелики. Карта взаємодії ризиків Карта взаємодії ризиків - це найпростіша форма графічного представлення, в якій один і той самий перелік ризиків формує осі x та y. Взаємодія ризиків позначається символом X або іншим якісним показником

За наявності історичних даних взаємодію ризиків можна виразити кількісно за допомогою кореляційної матриці. Це особливо корисний метод для застосування в категорії ризику, такій як ринковий ризик. Труднощі у визначенні кореляцій для ризиків включають можливість того, що минулі

причинно-наслідкові зв’язки не вказуватимуть на майбутні зв’язки, відсутність історичних даних, різницю в часових рамках (коротко-, середньо- та довгострокових), а також велику кількість необхідних ризиків. для оцінки в масштабах підприємства.

Розробка повної картини — дерева несправностей,

Дерева подій і діаграми краваток-метеликів

Діаграми, які розбивають складну подію ризику на її складові частини, показуючи ланцюги подій, які можуть призвести до події або стати її результатом, можуть бути незамінними для ідентифікації та оцінки реагування на ризик і ключових індикаторів ризику. Діаграми можуть бути якісними або служити основою для кількісних моделей. Три діаграми, які часто використовуються, це дерева несправностей, дерева подій і метелики. Дерева несправностей використовуються для аналізу подій або комбінацій подій, які можуть призвести до небезпеки або події. Дерева подій використовуються для моделювання послідовностей подій, що виникають внаслідок одного ризику. Метеликова діаграма поєднує дерево несправностей і дерево подій і отримала свою назву через свою форму. Імовірнісні моделі, побудовані на діаграмах-метеликах, є універсальними для кількісної оцінки властивих і залишкових рівнів ризику та виконання аналізу «що-якщо», сценарію та аналізу чутливості.

Пріоритезуйте ризики

Після того, як ризики оцінено та їх взаємодію задокументовано, настав час розглянути ризики як повний портфель, щоб зробити наступний крок – визначити пріоритети для реагування на ризики та звітувати різним зацікавленим сторонам. Термін «профіль ризику» представляє весь портфель ризиків, з якими стикається підприємство. Деякі організації представляють цей портфель як ієрархію, деякі як сукупність ризиків, нанесених на теплову карту. Підприємства з більш зрілими програмами ERM і кількісними можливостями можуть агрегувати індивідуальні розподіли ризиків у кумулятивний розподіл ймовірності збитків і називати це профілем ризику.

Подібно до оцінки ризиків, ранжування та пріоритезація часто виконується в два етапи. По-перше, ризики класифікуються відповідно до одного, двох або більше критеріїв, таких як рейтинг впливу, помножений на рейтинг вірогідності, або вплив, помножений на вразливість. По-друге, ранжований порядок ризиків переглядається в світлі додаткових міркувань, таких як лише вплив, швидкість настання або величина розриву між поточним і бажаним рівнем ризику (поріг толерантності до ризику). Якщо початкове ранжування здійснюється шляхом множення фінансових втрат на ймовірність, тоді остаточне визначення пріоритетів має враховувати якісні фактори.

Ієрархії та згортання та деталізація

Найпростіший спосіб агрегувати ризики - це впорядкувати їх відповідно до ієрархії. Це часто робиться в системах управління ризиками, де ризики можна впорядкувати за організаційними підрозділами, типами ризиків, географією чи стратегічними цілями. Кращі системи дозволяють користувачам згортати та детально аналізувати та звітувати. Це надає повний перелік оцінених ризиків, але не допомагає визначити пріоритети.

Карти ризиків

Ще один простий спосіб перегляду портфоліо – це створити карту ризиків, яку часто називають тепловою картою. Зазвичай це двовимірні представлення впливу, нанесені на графік проти ймовірності. Вони також можуть відображати інші відносини, такі як вплив проти вразливості. Для ще більшої інформації розмір точок даних може відображати третю змінну, таку як швидкість початку або ступінь невизначеності в оцінках.

Найпоширенішим способом визначення пріоритетності ризиків є визначення рівня ризику для кожної області графіка, як-от дуже високий, високий, середній або низький, де чим вищий сукупний рейтинг впливу та ймовірності, тим вищий загальний рівень ризику. Межі між рівнями залежать від суб’єкта господарювання залежно від схильності до ризику. Наприклад, суб’єкт із більшою схильністю до ризику матиме межі між рівнями ризику,

зміщеними у верхній правий кут, а суб'єкт із більшим ухиленням від ризику матиме межі між рівнями ризику, зміщеними у нижній лівий кут. Крім того, деякі суб'єкти встановлюють асиметричні межі, приділяючи дещо більшу увагу впливу, ніж вірогідності. Наприклад, ризик, який має рейтинг впливу помірний і рейтинг вірогідності частого, має призначений рівень ризику високий, тоді як ризик, який має рейтинг впливу екстремальний і рейтинг вірогідності можливого, має призначений рівень ризику дуже високий.

Після нанесення на теплову карту ризики ранжуються від найвищого до найнижчого з точки зору рівня ризику. Потім ці рейтинги можуть бути скориговані на основі інших міркувань, таких як уразливість, швидкість настання або детальне знання природи впливу. Наприклад, у групі ризиків із позначенням «дуже високий» ризики, які мають надзвичайний вплив на здоров'я та безпеку або репутацію, можуть мати пріоритет над ризиками, які мають надзвичайний фінансовий вплив, але менший вплив на здоров'я та безпеку чи репутацію.

Використовуючи числові оцінки в якісному середовищі, важливо пам'ятати, що цифри є мітками і не підходять для математичних маніпуляцій, хоча деякі суб'єкти множать рейтинги, наприклад, для впливу та ймовірності, щоб розробити попередній рейтинг.

Якщо суб'єкти господарювання визначили масштаби впливу як для можливостей, так і для ризиків, вони можуть нанести ризики на карту, як показано на прикладі 6. Це дає змогу безпосередньо порівняти можливості та ризики з найвищим рейтингом для розгляду та визначення пріоритетів.

Розглянемо такий приклад: компанія визначила 60 ризиків, щоб включити їх у свій всесвіт ризиків. Потім він визначив відповідних оцінювачів. Він використовував комбінацію інтерв'ю, семінарів та опитування для виконання початкової якісної оцінки критеріїв впливу, ймовірності, вразливості та швидкості настання. Взаємодії ризику були оцінені для найвищих ризиків, і оцінки були уточнені. Ризики були нанесені на теплову карту для виконання початкового визначення пріоритетів.

Дванадцять ризиків, нанесених на «дуже високий» рівень ризику, позначений червоним кольором на тепловій карті нижче. Ці ризики були визначені як «ключові» ризики, що означає, що про них повідомлятимуть і контролюватимуть виконавче керівництво та рада директорів.

Іншим корисним графіком для встановлення пріоритетів є діаграма MARCI (для пом'якшення, забезпечення, перерозподілу та сукупного впливу), зображена на прикладі 8. Діаграма MARCI відображає ризики за двома осями впливу та вразливості та вказує на швидкість настання кожного ризику розмір точок даних. Це особливо корисно, коли основною метою визначення пріоритетів є реагування на ризики: ризики, які відображаються найдальше у верхньому правому квадранті, представляють найвищий вплив і вразливість і найбільше виграють від додаткової ефективності управління в управлінні ризиками.

Продовжуючи наш приклад, 12 ризиків із оцінкою «Дуже високий» були нанесені на діаграму MARCI для подальшого уточнення пріоритезації та виконання попередньої оцінки типу відповідної реакції на ризик. З цього погляду компанія може побачити, як її програма хеджування зменшує її вразливість до підвищення цін на мідь (ризик 3), і оцінити своє попереднє рішення не хеджувати коливання курсу (ризик 12). Керівництво також бачить, що порушення ланцюга постачання (ризик 1) може статися без попередження та серйозного впливу. Цей та інші ризики в його квадранті вимагають заходів для зменшення вразливості. Команда виконавчого керівництва та члени правління приділятимуть особливу увагу діям керівництва щодо реагування на ці ризики. 12 основних ризиків були позначені тегами для подальшої кількісної оцінки та ймовірнісного моделювання.

Агрегування в кількісному середовищі

У ситуаціях, коли ключові ризики були кількісно визначені за допомогою загального показника, такого як фінансові збитки або показник ризику, можна агрегувати окремі розподіли ймовірностей в єдиний розподіл,

що відображає кореляції та ефекти портфеля. Заходи, які набувають популярності для цієї мети, це валовий прибуток під ризиком, грошовий потік під ризиком і прибутки під ризиком.

Основними застосуваннями для єдиного показника ризику, що представляє агреговане уявлення про ризик (протягом певного періоду часу при визначеному рівні довіри), є розподіл капіталу, оцінка платоспроможності та вимірювання використання ризику та потенціалу щодо схильності до ризику. Моделі агрегування ризиків надзвичайно варіюються від одного підприємства до іншого, навіть у сфері фінансових послуг.

Втілення на практиці

Щоб бути ефективним і стійким, процес оцінки ризиків має бути простим, практичним і зрозумілим. Успіх залежить від відданості керівництва та ресурсів. Процес мають виконувати люди з відповідними навичками, які підтримуються технологіями, які правильно підходять для поставленого завдання.

Функція ERM на корпоративному рівні необхідна для визначення загальних стандартів, координації оцінок між бізнес-підрозділами та полегшення аналізу взаємодії ризиків. Центральна функція ERM має бути укомплектована людьми, які володіють необхідними навичками фасилітації, управління проектами та аналітичними навичками, а також знаннями передової практики управління ризиками. Функція ERM має бути доповнена людьми, які займають посади, найближчі до ризиків. Власники ризику в кінцевому підсумку несуть відповідальність за оцінені рівні ризику та визначення та впровадження планів реагування на ризики, щоб привести ризики в допустимі межі. Цей гібридний підхід «зверху донизу» та «знизу вгору» поєднує найкраще з обох світів, досягаючи узгодженості та всебічного охоплення, одночасно впроваджуючи підзвітність та використовуючи досвід людей в організації, які найближче до ризиків.

Людей не вистачає. Щоб бути ефективними, вони повинні підтримуватися правильною технологією. Багато організацій починають свій

шлях ERM у простому середовищі електронних таблиць. Це може бути практичним на ранніх стадіях розробки, оскільки і власники ризиків, і вище керівництво з'ясовують свої вимоги до аналітики та звітності. Наступні роки можуть бути досить складними без автоматизації, особливо якщо організація є великою, складною та територіально розподіленою.

На щастя, велика кількість постачальників програмного забезпечення увійшла в простір ERM, і кожен рік приносить нові інновації та вдосконалені пропозиції. Системи існують у низці цінових точок з аналітичними можливостями, що збільшуються разом із ціною. Більшість систем швидко окупляться завдяки економії витрат на робочу силу.

Нарешті, оцінка ризику не може існувати у вакуумі, інакше вона стає марною заняттям. COSO Enterprise Risk Management – Integrated Framework наголошує на необхідності оцінки та контролю за ризиками з цілісної точки зору. Процес має бути в рамках більшої структури, яка використовує зібрану інформацію для прийняття рішень щодо реагування на ризики та моніторингу, а також повертає інформацію в процес стратегічного планування. Функція ERM повинна мати повноваження для моніторингу та нагляду за впровадженням реагування на ризики. Якщо учасники не бачать, що їхні внески та наполеглива праця під час оцінки ризиків призводять до конкретних дій, які справляють реальні зміни, вони стануть цинічними та відійдуть від процесу в наступні роки.

РОЗДІЛ ІІІ
ВИЗНАЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Загальна характеристика стійкості

Дослідження розпочалося із завдання оцінити, як сектори визначають стійкість, а потім визначити, чи встановлені цілі стійкості в секторах, і якщо так, то яким чином. З нашої попередньої роботи ми дізналися, що сектори критичної інфраструктури визначають стійкість по-різному і застосовують різні принципи та практики, які відповідають конкретному визначенню. Загальне визначення стійкості інфраструктури, що міститься у звіті Ради за 2022 рік "Стійкість критичної інфраструктури", стало гарною відправною точкою для вироблення спільної мови про стійкість. Однак, кожен сектор використовує свою термінологію, яка вкорінена в їхній історії, культурі, діяльності та бізнес-середовищі. Будь-які зусилля, спрямовані на підвищення стійкості секторів критичної інфраструктури, повинні спочатку визнати різницю в термінології та підходах до управління ризиками, які використовуються в цих секторах.

Переважною концепцією управління ризиками в електроенергетиці є надійність. Електрична мережа - це тісно пов'язана система генеруючих станцій, високовольтних ліній електропередач, підстанцій, розподільчих систем та інших об'єктів. Оскільки електроенергію не можна зберігати, вона повинна вироблятися в міру необхідності, а пропозиція повинна бути збалансована з попитом. Крім того, електроенергія йде "шляхом найменшого опору" і, як правило, не може бути спрямована в певному напрямку. Це означає, що операції з виробництва та передачі електроенергії в Україні відстежуватися і контролюватися в режимі реального часу, 24 години на добу, щоб забезпечити безперебійний і достатній потік електроенергії. Це вимагає співпраці та координації дій сотень учасників електроенергетичної галузі.

Коротко кажучи, надійність - це здатність задовольняти потреби в електроенергії кінцевих споживачів, навіть коли певні події зменшують кількість доступної електроенергії. Першочерговим завданням електроенергетичного сектору є надійність об'єднаної енергосистеми - основної системи генерації та передачі електроенергії в електромережі. Хоча окремі комунальні підприємства дуже занепокоєні забезпеченням електропостачання своїх споживачів через розподільчі системи, сектор в цілому покладається на цілісність об'єднаної енергосистеми і прагне її підтримувати.

НКРЕ визначає надійність об'єднаної енергетичної системи з точки зору двох основних та функціональних аспектів: Адекватність - здатність об'єднаної енергетичної системи забезпечувати сукупний попит на електричну енергію та енергетичні потреби споживачів у будь-який час з урахуванням планових та обґрунтовано очікуваних позапланових відключень елементів системи. Безпека - здатність об'єднаної енергосистеми протистояти раптовим збоям, таким як коротке замикання або непередбачувана втрата елементів системи внаслідок непередбачуваних обставин.

Управління ризиками в електроенергетичному секторі стосується (1) ймовірності того, що певна подія знизить надійність об'єднаної енергосистеми та її міждержавних з'єднань, і (2) наслідків, якщо це станеться. Усі керівники електроенергетичного сектору, з якими ми спілкувалися, називали надійність як головну мету сектору і давали схожі пояснення основних понять і принципів.

Вони також поділилися спільним розумінням стандартів НКРЕ щодо планування та експлуатації електромережі, які використовуються для досягнення високого рівня надійності. Однак, коли їх попросили дати визначення стійкості в електроенергетичному секторі, їхні погляди розійшлися. У той час як надійність зазвичай розглядається як "підтримання світла увімкненим", дехто вважав, що стійкість - це здатність швидко відновлюватися, коли світло вимикається. Інші, з якими ми спілкувалися,

розглядали стійкість як набагато ширше поняття, що охоплює всі аспекти надійності. Дехто говорив про стійкість як про здатність переживати події та відновлювати роботу об'єктів після них. Стійкість також описували як елемент загального дизайну електричної системи: здатність великої взаємопов'язаної мережі поглинати удари. Один з керівників протиставив стійкість (здатність витримувати удари і відновлюватися) надмірності (наявність принаймні одного резервного варіанту на випадок виходу з ладу компонента). Більшість керівників, з якими ми спілкувалися, зазначили, що якщо надійність відносно легко визначити і виміряти, то стійкість - складніше.

Не маючи універсального визначення стійкості, електроенергетичний сектор не розробив загальногалузевих цілей стійкості, що базуються на кінцевих результатах. Натомість власники та оператори розглядають надійність як головну мету для сектору і розробили низку стандартів, керівних принципів та нормативних документів для її досягнення. Однак це не означає, що електроенергетичні компанії не намагаються старанно впроваджувати практики забезпечення стійкості. Конкретні визначення стійкості є менш важливими, ніж фундаментальні концепції стійкості. Завдяки нашим інтерв'ю та дослідженням ми виявили вражаючий набір практик управління ризиками, які широко використовуються у всьому секторі. Щоб упорядкувати та описати ці практики, ми спиралися на концепцію стійкості, розроблену експертом з питань стійкості Стівеном Флінном (Stephen Flynn). Концепція ґрунтується на чотирьох характеристиках: Надійність - здатність продовжувати працювати або залишатися стійкими перед обличчям катастрофи. У деяких випадках це означає, що конструкції або системи повинні бути достатньо міцними, щоб витримати передбачуваний удар. В інших випадках надійність вимагає розробки запасних або резервних систем, які можуть бути задіяні, якщо щось важливе вийде з ладу або перестане працювати.

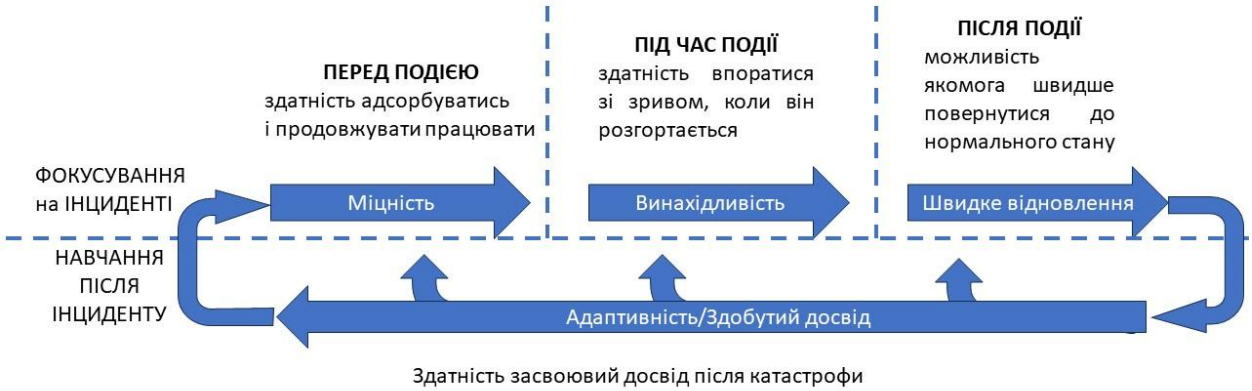
Надійність також передбачає інвестиції та підтримку елементів критичної інфраструктури, щоб вони могли витримати події з низькою ймовірністю, але з високими наслідками.

Винахідливість - здатність вміло керувати катастрофою в процесі її розгортання. Вона включає в себе визначення варіантів, визначення пріоритетів, що слід зробити як для контролю над збитками, так і для початку їх пом'якшення, а також донесення рішень до людей, які будуть їх реалізовувати. Винахідливість залежить насамперед від людей, а не від технологій.

Швидке відновлення - здатність якнайшвидше повернутися до нормального життя після катастрофи. Ретельно розроблені плани на випадок надзвичайних ситуацій, компетентні аварійні операції та засоби доставки потрібних людей і ресурсів у потрібні місця мають вирішальне значення.

Адаптивність - засіб засвоєння нових уроків, які можна винести з катастрофи. Вона передбачає перегляд планів, модифікацію процедур і впровадження нових інструментів і технологій, необхідних для підвищення надійності, винахідливості та можливостей відновлення до наступної кризи.

Ми організували ці особливості в послідовність подій, показану на Рисунку 3.1. Надійність включає заходи, які вживаються до події; винахідливість включає заходи, які вживаються під час розгортання кризи; швидке відновлення включає заходи, які вживаються одразу після події, щоб повернути ситуацію до нормального стану; а адаптивність включає заходи, які вживаються після інциденту, та отримані уроки, які засвоюються в рамках всієї системи.



Здатність засвоювий досвід після катастрофи

Рис. 3.1 Послідовність подій

Іншим виміром стійкості є час. Електроенергетична система складається з величезної кількості дорогих, довгострокових капітальних активів, які мають відносно повільний оборот. У короткостроковій перспективі інфраструктура та активи системи є фіксованими, і комунальні підприємства покладаються на практики, які залучають людей, плани, процеси та процедури для підвищення стійкості. Більшість практик часто можуть бути реалізовані в короткі терміни і, як правило, коштують дешевше, ніж капітальні поліпшення. Однак у довгостроковій перспективі комунальні підприємства можуть впроваджувати нові технології та змінювати дизайн електричної системи, щоб підвищити її стійкість. Ці заходи, як правило, є більш дорогими і потребують більше часу на реалізацію, але можуть забезпечити більш тривалу стійкість, оскільки безпека "вбудована" в інфраструктуру. Виходячи з цих відмінностей, Дослідницька група розділила кожну з чотирьох категорій стійкості на ті, що стосуються людей і процесів, і ті, що стосуються інфраструктури та активів. Ми називаємо всю цю організацію конструкцією стійкості.

Нарешті, не всі загрози вирішуються однаково. Ненавмисні дії, такі як шторми, повені, землетруси та вихід з ладу обладнання, є частиною повсякденної роботи, до яких комунальні підприємства можуть підготуватися за допомогою планів, навчань та безпосереднього досвіду. Навмисні дії, такі як крадіжки і цілеспрямовані фізичні напади, важче спланувати і вони вимагають інших практик і стратегій. Кібератаки, які можуть бути випадковими або зловмисними, являють собою новішу форму підриву, що вимагає особливого набору практик забезпечення стійкості. За допомогою інтерв'ю та досліджень Ми виявили понад 100 прикладів практик забезпечення стійкості в електроенергетичному секторі.

3.2 Концептуальні засади визначення цілей стійкості.

Розробка загальноприйнятого набору цілей, орієнтованих на кінцевий результат, для кожного сектору є складним завданням. Кожна підгалузь, сегмент галузі, власник та оператор мають особливі потреби в бізнесі, безпеці та операційній діяльності. Занадто специфічні галузеві цілі можуть не підходити для всіх підприємств, тоді як загальні галузеві цілі можуть бути занадто широкими, щоб керувати розробкою стратегій стійкості для окремих підприємств. У багатьох секторах також немає єдиної організації або органу, який би мав повноваження або повноваження скликати наради для розробки відповідних цілей для всього сектору. Незважаючи на ці виклики, Дослідницька група змогла розробити загальну структуру і процес для визначення цілей стійкості сектору на основі дослідження електроенергетичного сектору. Ця структура може слугувати моделлю для прийняття іншими секторами CIKR. Структура складається з трьох взаємопов'язаних елементів, розробка цілей, галузеве застосування та підвищення стійкості.

Розробка цілей Першим кроком є встановлення базової лінії поточних практик забезпечення стійкості. У нашому тематичному дослідженні електроенергетичного сектору ми задокументували сотні конкретних практик планування, безпеки, ведення бізнесу та операційної діяльності, які сприяють підвищенню стійкості окремих компаній та сектору в цілому. Ми проаналізували практики, спрямовані на подолання різноманітних потенційних фізичних та кібер-ризиків, спричинених природними погодними явищами, аваріями, старінням обладнання, зловмисними діями та перебоями в ланцюгах поставок. Ми проаналізували весь спектр практик - від процедур і практик, характерних для конкретних компаній, до загальногалузевого планування та архітектури інфраструктурних об'єктів. У сукупності ці практики визначають поточну ситуацію зі стійкістю в секторі. Другий крок полягає в тому, щоб описати та впорядкувати ці практики відповідно до типу

спроможності до стійкості, яку вони забезпечують, використовуючи конструкт стійкості, описаний у Розділі 2.

Чотири основні принципи організації включають надійність (здатність до поглинання), винахідливість (антикризове управління в режимі реального часу), швидке відновлення та адаптивність (засвоєння отриманих уроків). У нашому тематичному дослідженні ми також розмежували практики, пов'язані з людьми та процесами, і практики, пов'язані зі структурою інфраструктури та активів, для кожної з чотирьох категорій. Додаткові відмінності були зроблені для практик, пов'язаних з ненавмисними діями, навмисними діями та кіберподіями.

Третій крок полягає у визначенні низки перспективних цілей стійкості сектору, які випливають з цих практик. Метою цього кроку є не встановлення остаточних цілей стійкості сектору, а скоріше пропозиція потенційних цілей стійкості, які узгоджуються з поточними практиками сектору. Для електроенергетичного сектору базові практики стійкості, організовані в рамках концепції стійкості NIAC, дозволили сформувати низку цілей високого рівня, які добре узгоджуються з тим, як сектор планує та управляє надійністю електромережі. Це такі цілі:

1) Витримувати удар від будь-якої небезпеки без втрати критично важливих функцій.

2) Запобігати каскадному поширенню перебоїв живлення на взаємопов'язані системи.

3) Мінімізувати тривалість і масштаби відключень електроенергії за допомогою стратегій швидкого відновлення.

4) Зменшити майбутні ризики шляхом врахування уроків минулих перебоїв, симуляцій та навчань, а також належних процесів оцінки ризиків.

Застосування в секторі Для перевірки надійності перспективних цілей стійкості сектору, четвертим кроком є оцінка стійкості сектору з використанням сценарію з високим рівнем впливу, який передбачає ризики, що виходять далеко за межі типових або історичних ризиків, з якими

стикається сектор, і далеко за межі сценаріїв, до яких він належним чином підготувався для виконання бізнес-вимог та вимог регуляторних органів.

Ефективно використана в процесі.

Комплексної перевірки ядерного сектору та відтворена для тематичного дослідження електроенергетичного сектору, ця оцінка може бути виконана за допомогою декількох різних методів, включаючи настільні вправи, моделювання та імітацію, інженерні дослідження та інші способи. Для тематичного дослідження електроенергетичного сектору ми провели цілеспрямовані одноденні практичні навчання в системі газо- та електропостачання Балтімора, які включали зловмисні катастрофічні атаки на декілька підстанцій. Сценарій був спеціально розроблений для того, щоб вивести з ладу стратегічно важливі об'єкти енергосистеми. Ми доповнили цей сценарій результатами інших модельних вправ та досліджень в електроенергетичному секторі, включаючи три сценарії з дослідження НКРЕ "Ризики низькочастотних подій з високим ступенем впливу" та два сценарії з дослідження "Безпечна мережа '09". Оцінка покликана виявити прогалини та недоліки у практиці забезпечення стійкості в секторі. Прогалини та недоліки вказують на обставини, за яких сектор не в змозі досягти перспективних цілей стійкості сектору. Зосередивши увагу на секторі за межами поточних очікуваних ризиків, ми змогли отримати уявлення про типи підвищення стійкості, які дозволять сектору краще реагувати не лише на сценарії з високим рівнем впливу, але й на низку менш значущих сценаріїв. У різних сценаріях з високим рівнем впливу, використаних у тематичному дослідженні для електроенергетичного сектору, було виявлено низку прогалин, включаючи механізми скоординованих державно-приватних дій, вразливість підстанцій, відсутність у комунальних підприємств досвіду реагування на цілеспрямовані фізичні атаки та невизначеність ролі уряду під час масштабної кібератаки.

Покращення стійкості. Справжня цінність розробки перспективних цілей стійкості сектору, тестування їх в екстремальних сценаріях і виявлення

прогалин полягає в тому, що цей процес виявляє можливості для підвищення стійкості. Незмінно, прогалини та недоліки піднімають фундаментальні питання про відповідні ролі та обов'язки приватного сектору та уряду в оплаті та впровадженні рішень у сфері безпеки. Під час наших інтерв'ю майже всі керівники змогли визначити можливості для підвищення стійкості сектору, але зазначили, що більшість з них або занадто дорогі, або потрібні більше для цілей національної безпеки, ніж для бізнес-цілей. Діалог на високому рівні між керівниками галузі або між галуззю та урядом вважається одним з найкращих підходів для розробки рішень та визначення ролей. У тематичному дослідженні для електроенергетичного сектору ми скликали круглий стіл керівників компаній, щоб оцінити прогалини та недоліки, виявлені в сценаріях з високим рівнем впливу. Керівники розробили кілька рішень для усунення конкретних прогалин і недоліків, які були інтегровані в наші рекомендації.

Важливим внеском у цей процес є аналіз інфраструктурних факторів, які відображають умови та обставини, що впливають на спроможність сектору знаходити ресурси та впроваджувати рішення. Наприклад, спроможність ядерного сектору, який налічує 104 станції, що експлуатуються 32 компаніями, впроваджувати рішення з безпеки значно відрізняється від спроможності сектору комерційних об'єктів, який налічує тисячі власників і операторів таких різноманітних об'єктів, як офісні будівлі, казино, торгові центри і спортивні стадіони. Під час інтерв'ю та щотижневих конференцій було виявлено та обговорено кілька ключових інфраструктурних факторів. Зразок набору інфраструктурних факторів, який може слугувати початковим шаблоном для інших секторів критичної інфраструктури. Останнім кроком у рамках концепції є розробка або модифікація цілей стійкості сектору, які визначаються на основі діалогу між державним і приватним секторами.

Перспективні цілі можуть бути змінені, щоб відобразити конкретні ризики та обставини. Таким чином, як уряд, так і промисловість можуть уточнити державні та приватні обов'язки щодо подолання інфраструктурних

ризиків, для яких існує мало прецедентів, і підвищити загальну стійкість національної інфраструктури.

Стійкість в електроенергетичному секторі. Понад 3 000 традиційних електроенергетичних компаній та сім регіональних операторів електропередач контролюють величезну, тісно інтегровану систему електростанцій, ліній електропередач, розподільчих об'єктів та мереж зв'язку, які працюють і взаємодіють одночасно та в режимі реального часу, забезпечуючи електроенергією побутових, комерційних та промислових споживачів. Європейська електромережа, яку зазвичай називають найбільшим і найскладнішим механізмом у світі, охоплює країни європейського союзу, Велико Британію та невелику частину Угорщіни, працює з надійністю 99,9 відсотка, що вимагає передових технологій моніторингу та управління, а також кваліфікованих операторів, які працюють злагоджено в режимі 24/7/365. Взаємозв'язок між системами та тісна співпраця між комунальними підприємствами, виробниками електроенергії та операторами електропередач дозволяють мережі витримувати збої в роботі обладнання та інші непередбачувані події, зберігаючи при цьому світло увімкненим. Управління ризиками є невід'ємною частиною експлуатації електромережі. Підтримання надійності електроенергетичної системи є головним завданням сектору та основою його стратегії управління ризиками.

Сектор розглядає ризик як ймовірність того, що операційна подія знизить надійність електромережі до такої міри, що наслідки будуть неприйнятними. Оскільки неможливо або недоцільно запобігати всім руйнівним подіям, сектор планує та експлуатує електроенергетичну систему таким чином, щоб у разі виникнення подій їхній вплив був керованим, а наслідки - прийнятними. Електроенергетичний сектор розуміє, що споживачі очікують безперебійного електропостачання, а комунальні підприємства роблять все можливе, щоб задовольнити ці очікування. Коли виникають перебої, пріоритетами сектору є: 1) підтримка цілісності об'єднаної енергосистеми в режимі реального часу (щоб уникнути каскадного

відключення) та 2) захист обладнання для генерації та передачі електроенергії від катастрофічних пошкоджень (які можуть поставити під загрозу надійність протягом тижнів або місяців).

Надійність вбудована в кожен рівень об'єднаної енергосистеми, в основу генерації та передачі електроенергії. Резервування вбудовано в систему шляхом з'єднання декількох ліній електропередач, які дозволяють електроенергії рухатися від місця її виробництва до місця споживання, навіть коли деякі лінії виведені з ладу. Вимикачі та інші технології використовуються для ізоляції несправностей (коротких замикань) в окремих частинах системи, коли вони виникають, щоб підтримувати загальну цілісність об'єднаної мережі. Численні оператори системи передачі, які пройшли навчання та сертифіковані відповідно до суворих стандартів НКРЕ, чергують у кожному центрі управління мережею в режимі 24/7/365.

Державні системи оцінювання надають операторам системи передачі картину стану енергосистеми в режимі реального часу, що дозволяє їм виявляти та ізолювати проблеми і виправляти їх до того, як вони стануть каскадними. Один генеральний директор розповів нам, що деякі системи оцінки стану та енергоменеджменту мають понад 700 непередбачуваних ситуацій для моделювання наслідків, якщо певний компонент виходить з ладу або має бути виведений з експлуатації. У разі виникнення непередбачуваних ситуацій системи оцінки стану можуть працювати безперервно, і хоча енергосистема є високоавтоматизованою, оператори мають підготовку, можливості та повноваження для того, щоб обійти автоматичне реагування і вручну переналаштувати систему, щоб зменшити або іншим чином розподілити навантаження на споживачів, щоб забезпечити безперервну надійну роботу енергосистеми або мінімізувати її вплив. Управління ризиками, надійність і відновлення настільки вкорінені в роботу електромережі, що опитані нами керівники не часто думають про свою практику як про стійкість. Енергокомпанії мають великий досвід реагування на надзвичайні ситуації та відновлення і розробили моделі управління

ризиками, які допомагають прогнозувати вплив погодних умов, непередбачуваних відмов обладнання та стихійних лих, що дає їм змогу ефективніше готуватися до них. Комунальні підприємства отримують нові уроки з кожної події і впроваджують вдосконалення у вигляді навчання, покращених практик і нових технологій, які забезпечують кращу стабільність і реагування. Така ретельна та цілеспрямована еволюція енергосистеми дозволила їй задовольнити рівень споживання електроенергії, який більш ніж у п'ять разів перевищує рівень споживання 50 років тому.

Однак, еволюція профілю ризиків та нові загрози для стійкості енергосистеми змушують операторів мереж готуватися до ризиків, які виходять за рамки їхнього традиційного досвіду та обов'язків. Забезпечення стійкості енергосистеми стає сферою спільної відповідальності, де вкрай необхідним є скоординований підхід галузі та уряду. У цьому розділі розглядається інфраструктура та дизайн енергосистеми, як вона функціонує в умовах регулювання, як сектор говорить про стійкість і практикує її, а також фактори, з якими стикаються енергосистеми сьогодні, і які змушують керівників компаній закликати до цілеспрямованого партнерства на високому рівні зі своїми колегами з уряду.

3.3 Проектування активів та інфраструктури.

Оскільки електроенергію не можна легко зберігати, вона повинна вироблятися і передаватися в міру її використання. Як наслідок, енергосистема управляється дуже структуровано, з використанням ринкових механізмів та скоординованої передачі електроенергії для постійного збалансування виробництва електроенергії та попиту споживачів.

Об'єкти з виробництва, передачі та розподілу електроенергії доповнюються комп'ютеризованими системами в диспетчерських центрах, які використовують різноманітні цифрові датчики та польові пристрої для моніторингу та управління мережею через різні комунікаційні мережі.

Загалом, електроенергетична інфраструктура проектується з урахуванням насамперед надійності, ефективності та економічності. Як наслідок, обладнання, як правило, фізично велике, капіталомістке і має тривалий термін експлуатації; додаткове резервне і дублююче обладнання, яке б забезпечило кращу надійність і швидше відновлення, стає дорогим і складним у розміщенні.

Наприклад, цілеспрямована атака на надвисоковольтні трансформатори викликає занепокоєння і є потенційною вразливістю системи. Окрім того, що запасні трансформатори є дуже дорогими, великими і важкими для переміщення, їх виробництво займає тривалий час. Більшість з них виробляються за кордоном і мають бути розроблені на замовлення, щоб відповідати конфігурації мережі в конкретній місцевості.

Давно усвідомлюючи цю проблему, керівники електроенергетичного сектору, з якими ми провели інтерв'ю, сказали, що вони працюють в рамках своїх комунальних підприємств та галузевих програм над кількома стратегіями пом'якшення наслідків зміни клімату. Електроенергетичний сектор вживає наступних заходів:

Зменшити спільне розташування запасних трансформаторів з блоками, які вони мають намір замінити, щоб уникнути пошкодження запасних блоків при виході з ладу робочих блоків.

Збільшити кількість запасних трансформаторів - скоординованій галузевій програмі, спрямованій на створення запасів та оптимізацію процесу доставки у випадку аварійних ситуацій.

Дослідження та розробка відновлювального трансформатора для тимчасового використання, поки новий трансформатор не буде замовлений, побудований, доставлений та встановлений.

Дослідити можливість створення стандартизованих трансформаторів, щоб зменшити кількість унікально спроектованих одиниць.

Високотехнологічні системи управління також є дорогими і мають термін служби від 10 до 20 років. Однак, зважаючи на швидкі темпи

технологічних змін, системи та обладнання швидко застарівають, а модернізація технологій вимагає додавання додаткових компонентів, а не їх суттєвої заміни. Враховуючи необхідність безперервної роботи цих систем, всі зміни повинні впроваджуватися без перебоїв. Електрична мережа розвивалася протягом багатьох десятиліть і вже не є оптимальним проектом з огляду на нові ризики, що з'являються. Якби система була перероблена сьогодні, з'явилися б можливості підвищити рівень безпеки обладнання та систем, створити критичні компоненти, такі як високовольтні трансформатори, за єдиними стандартами, краще інтегрувати розподілену та відновлювану енергію, а також легко інтегрувати передові цифрові засоби управління для "розумної" мережі.

За словами одного з керівників галузі, модернізувати електроенергетичну систему набагато складніше, ніж відбудувати її з нуля, але час і витрати на перебудову мережі унеможливлюють це. Таким чином, у міру того, як мережа стає більшою і більш досконалою, вона також може стати більш вразливою до проблем надійності через зростання складності системи, перевантаженість коридорів передачі, мінливість джерел відновлюваної генерації та постійно мінливі вимоги споживачів. Кілька керівників заявили, що для того, щоб енергосистема могла передбачати майбутні ризики та вимоги і адаптуватися до них, вони збільшили довгострокове планування до 10-20 років.

Один з керівників розповів, що інженери з передачі електроенергії його компанії використовують імітаційну модель енергосистеми для довгострокового проектування, яка використовує базовий сценарій, щоб розглянути, як будуть побудовані системи через 10 років, і визначає, де буде потрібно нове будівництво для забезпечення надійності. Хоча підвищення стійкості має відбуватися поступово через природу активів електроенергетичного сектору, ці зміни плануються для того, щоб створити цілісні, гнучкі системи, здатні задовольнити майбутні потреби.

Розроблено для надійності. Оскільки об'єднана енергосистема дуже взаємопов'язана і взаємозалежна, вона повинна бути спроектована таким чином, щоб досягти певних стандартів надійності, щоб мінімізувати можливість каскадних збоїв, запобігти пошкодженню обладнання і забезпечити безперервність роботи. Електроенергетичний сектор працює за стандартом, який зазвичай називають "N мінус один", або N-1, що означає, що кожна окрема частина системи експлуатується таким чином, що вихід з ладу будь-якого одного компонента (одна непередбачена ситуація) не порушує надійність всієї системи в цілому. Це дає системним операторам час для коригування системи, щоб підготуватися до будь-яких наступних відмов компонентів. Концепція аварійної експлуатації та планування закладена в стандартах НКРЕ щодо планування, проектування та експлуатації об'єктів, мереж, обладнання та інших компонентів об'єднаної енергетичної системи.

Керівники компаній зазначили, що у багатьох критично важливих частинах системи енергокомпанії пішли ще далі, побудувавши ділянки ліній електропередачі з подвійним резервуванням або використовуючи інші методи, щоб витримати більш серйозні непередбачувані ситуації, коли ризик виходу системи з ладу є неприйнятним. При плануванні майбутніх систем проводяться більш серйозні симуляції, які перевіряють здатність і стійкість системи протистояти численним непередбачуваним ситуаціям (N-2 або більше), не втрачаючи при цьому своєї цілісності і не зазнаючи широкомасштабних каскадних відключень.

Оскільки система передачі електроенергії несе великі електричні навантаження і є частиною магістральної енергосистеми, в систему вбудовано резервування шляхом з'єднання декількох ліній електропередачі, щоб забезпечити безперебійний потік електроенергії від місця її виробництва до місця споживання, навіть якщо деякі лінії виведені з ладу, що дозволяє забезпечити безперебійний потік електроенергії. Однак система, що приймає навантаження, може зазнати навантаження, що збільшує ймовірність

додаткового збою; кілька збоїв у сегменті передачі можуть спричинити каскадні збої і призвести до регіональних відключень електроенергії.

Фундаментальною метою надійності в електроенергетиці є запобігання каскадному поширенню локальних подій через об'єднану енергосистему та вимкненню значної частини мережі, як це сталося під час північно-східного відключення електроенергії у 2003 році. Вдосконалені технології, покращена координація, вдосконалені датчики та спеціально навчені оператори тепер працюють разом, щоб ізолювати проблеми в енергосистемі. Хоча електроенергетика побудована на концепції, що локальні збої на рівні розподілу можуть статися, ці збої ізолюються і швидко усуваються досвідченими бригадами аварійного реагування на надзвичайні ситуації. Під час екстремальних аварійних ситуацій операторам мереж може знадобитися навмисне перервати обслуговування споживачів, щоб зберегти цілісність об'єднаної енергосистеми, запобігти каскадним збоям і дати можливість комунальному підприємству швидко відновити електропостачання після повного відновлення роботи системи. Більшість відключень відбувається на розподільчому рівні через збої в роботі обладнання або природні пошкодження. Для зміцнення систем передачі та розподілу електроенергії комунальні підприємства впроваджують стандарти НКРЕ та Інституту інженерів з електротехніки та електроніки (IEEE), розроблені для забезпечення здатності різних компонентів системи витримувати значні навантаження, такі як вітрове навантаження, удари блискавки, повені, обледеніння та інші фізичні навантаження.

Ринок та регулювання

Сектор електроенергетики функціонує в умовах жорсткого регулювання. На національному рівні НКРЕ розробляє та забезпечує дотримання стандартів надійності для об'єднаної енергетичної системи (генерації та передачі). Державна комісія з регулювання енергетики здійснює нагляд за діяльністю НКРЕ та має регуляторні повноваження щодо оптової передачі та міждержавних бірж електроенергії. Регулювання тарифів

для споживачів відбувається на державному/місцевому рівні. На регульованих роздрібних ринках комунальні підприємства, що належать інвесторам, як правило, працюють на вертикально інтегрованій основі, надаючи послуги з виробництва, передачі та постачання за комплексною ціною для роздрібних споживачів. У тих державах, які запровадили роздрібну конкуренцію (дерегуляцію) на організованих оптових ринках, багато комунальних підприємств, що належать інвесторам, продали свої послуги з виробництва електроенергії та передали свої передавальні активи під операційний контроль неприбуткових операторів передачі, включаючи незалежних системних операторів (ISO) та регіональні передавальні організації. Сім існуючих ОСП/НСО мають широкий операційний контроль над більшістю передавальних активів комунальних підприємств і зобов'язані забезпечувати недискримінаційний доступ до передачі електроенергії виробникам та споживачам. Вони також керують конкурентними оптовими ринками енергетичних послуг та реагування на попит, а також мають повноваження щодо планування системи передачі.

Модернізація інфраструктури з метою підвищення стійкості часто є дороговартісною і її важко виправдати, якщо вона не забезпечує негайної або помітної вигоди для споживачів, наприклад, покращення повсякденного обслуговування. Комунальні підприємства повинні звітувати як перед регуляторними органами, так і перед інвесторами чи виборними/муніципальними посадовцями при розгляді питання про те, як справедливо розподілити витрати на підвищення надійності. Споживачі можуть бачити лише переваги стійкості модернізації у випадку кризи або стихійного лиха, які можуть не відбутися роками, якщо взагалі відбудуться. Регулювання покликане захистити споживачів від підвищення тарифів, яке вони не бажають або не можуть прийняти, і унеможливлює просте перекладання всіх необхідних витрат на модернізацію на споживачів без широких консультацій з громадськістю.

3.4 Критичні взаємозалежності об’єктів критичної інфраструктури

Хоча енергетичний сектор призначений для роботи в умовах, коли інші інфраструктури не працюють, електроенергетика залежить від паливних і транспортних мереж (у тому числі автомобільних, залізничних і трубопровідних), необхідних для отримання доступу до об'єктів і доставки палива та обладнання. Він також значною мірою залежить від телекомунікаційних та ІТ-мереж, що використовуються для управління передачею та розподілом електроенергії, які ставатимуть все більш важливими в міру інтеграції більш розумних цифрових технологій (включаючи інтелектуальні лічильники) для підвищення гнучкості та пропускної здатності енергосистеми. Ці мережі також є критично важливими для роботи бізнес-систем і забезпечення зв'язку під час надзвичайних ситуацій. Вода використовується для виробництва пари, яка приводить в рух електричні турбіни на електростанціях і охолоджує обладнання, а хімічні речовини застосовуються для обробки води і пари, а також для виробництва первинних джерел енергії. Виробничий сектор постачає мільйони одиниць обладнання, яке використовується промисловістю у повсякденній роботі, від мікрочіпів до багатотонних високовольтних трансформаторів.

Під час проведення нашого тематичного дослідження ми дізналися про кілька інцидентів в електроенергетиці, які підкреслили важливі уроки щодо стійкості та взаємозалежності. Один з таких уроків стосувався обмеженості резервних систем і того, як події можуть каскадувати між секторами. У квітні 2010 року компанія Укренерго пережила електричну пожежу на одному зі своїх кабелів, що призвело до пошкодження сусіднього кабелю і втрати обох кіловольтних ланцюгів, що спричинило відключення електроенергії в районі Ужгороду. Також було пошкоджено інші комунікації, що знаходилися в тій самій смузі відводу, в тому числі телекомунікаційні та ІТ-мережі. Компанія Укренерго змогла досить швидко відновити електропостачання споживачів.

Тим не менш, насоси на насосній станції водозабору потребували повторного заправлення, що призвело до тривалого відключення води для мешканців та підприємств у районі Ужгорода. У цьому прикладі спільне розташування інженерних комунікацій спричинило каскадний вплив події в електроенергетичному секторі на інші сектори, а електричний кабель і його резервний кабель мали єдину точку виходу з ладу.

Хоча ми не повністю дослідили економічне значення стійкості в цьому тематичному дослідженні, ми дізналися про дослідження та аналіз, що проводяться в цій галузі. Моделі "витрати-випуск", моделі сумісності "витрати-випуск", економетричні моделі часових рядів, обчислювальні моделі загальної рівноваги та регіональні економічні моделі можуть допомогти в розумінні впливу інвестицій в стійкість у секторі.[3]

В одному з досліджень під керівництвом економіста Адама Роуза були змодельовані економічні наслідки терористичної атаки на енергосистему Лос-Анджелеса. За відсутності стійкості дослідники оцінили економічні втрати у 20,5 мільярдів доларів США за два тижні. Завдяки кільком формам заходів з підвищення стійкості втрати зменшилися до 2,8 млрд доларів. [4]

Хоча електроенергетичний сектор визнає важливість економічної взаємозалежності, опитані нами керівники зазначили, що вони, можливо, не повністю усвідомлюють ризики, з якими стикаються в інших секторах критичної інфраструктури, або економічні наслідки, які можуть каскадувати між секторами. У цій сфері необхідно провести додаткову роботу, що є спільною темою попередніх досліджень НІАК.

Об'єднана енергосистема На додаток до взаємозалежності з іншими важливими секторами, електрична мережа значною мірою залежить від електричних з'єднань всередині неї самої, на які покладаються комунальні підприємства для обміну електроенергією в режимі реального часу та реагування на регіональні події або перебої. В Україні основна енергосистема складається з чотирьох об'єднаних мереж: Східної, Західної, Північної та Південної об'єднаних енергосистем. Західна об'єднана енергосистема має

зв'язок з Польщею, Словаччиною а Східна та Західна об'єднані енергосистеми були інтегровані з більшою частиною Беларуссю та рф. Хоча ці об'єднання мають обмежені перетоки електроенергії між собою, в межах кожного об'єднання оператори системи передачі контролюють перетоки між окремими підприємствами. Практично всі комунальні підприємства України взаємопов'язані принаймні з одним іншим підприємством. Оптові конкурентні ринки дозволяють комунальним підприємствам знизити витрати на електроенергію, розширити можливості енергопостачання та підвищити надійність. Комунальні підприємства значною мірою покладаються на сусідні підприємства, що робить їх важливим ресурсом для швидкого реагування та відновлення. Крім угод, що регулюють торгівлю електроенергією, керівники заявили, що вони мають детальні угоди про взаємодопомогу та співпрацю, які дозволяють комунальним підприємствам швидко обмінюватися запасним обладнанням та ремонтним персоналом у надзвичайних ситуаціях. Важливість цієї взаємозалежності не сприймається легковажно; організації, що виробляють, передають і розподіляють електроенергію, щонайменше раз на рік проводять масштабні навчання на випадок надзвичайних ситуацій, щоб перевірити координацію і процедури під час надзвичайної ситуації. За словами керівників, великі комунальні підприємства часто проводять міждисциплінарні, міжгалузеві навчання щонайменше один раз, а то й чотири рази на рік.

Історичні ризики Оператори електромереж мають десятиліттями накопичений досвід реагування на надзвичайні ситуації, пов'язані з погодними умовами та стихійними лихами, і, спираючись на цей досвід, інтегрували можливості ефективного реагування та відновлення в основну роботу електромереж. Цей досвід робить загрози від старіння інфраструктури, ураганів, повеней, обмерзання та інших фізичних навантажень кількісно вимірюваними та більш керованими. Комунальні підприємства стали експертами в управлінні ризиками, оцінюючи ризики, зважуючи вартість і вигоди від підвищення надійності, і в багатьох випадках

розділяючи витрати на поліпшення інфраструктури зі споживачами, яким комунальне підприємство може надати кількісно вимірювану вигоду. Під час інтерв'ю з керівниками NIAC та обговорень у дослідницькій групі вразило те, наскільки ретельно в секторі аналізуються великі стихійні лиха та враховуються уроки, отримані в інших галузях. Публікації НКРЕ та національні огляди основних подій у секторі6 сприяють такому самоаналізу, але операційні вдосконалення, що випливають з цих подій, насамперед ініціюються керівниками компаній, які розглядають це як частину своїх основних обов'язків перед клієнтами, акціонерами та іншими зацікавленими сторонами. Детальніше про це йдеться в розділі "Адаптивність" цього розділу.

Нові ризики. Ефективне та надійне постачання електроенергії стало основою для ефективної роботи та зростання інших критично важливих секторів, включаючи транспорт, банківський та фінансовий сектори, водопостачання, охорону здоров'я та телекомунікації. Як наслідок, національна безпека, громадське здоров'я та безпека зараз тісніше, ніж будь-коли, пов'язані з роботою електроенергетичного сектору, що робить кожне відключення та збій у роботі більш масштабним. У міру того, як країна модернізує електромережу та інтегрує тисячі цифрових компонентів, з'являються нові кібернетичні та операційні вразливості, а електромережа опинилася в центрі уваги держави як потенційна мішень для добре забезпечених супротивників. Профіль ризиків в електроенергетичному секторі виходить за межі досвіду операторів та ефективного управління ризиками. Традиційні моделі ризиків не були розроблені з урахуванням цих нових загроз, а їхній вплив важко піддається кількісній оцінці, що ускладнює визначення пріоритетів та обґрунтування інвестицій у певні заходи з підвищення стійкості. Щоб працювати в майбутній економіці з такою ж надійністю, електроенергетичний сектор повинен співпрацювати зі своїми колегами в державному секторі для подолання нових ризиків, у тому числі тих, що обговорюються нижче.

Кібербезпека та "розумні" мережі Удосконалені системи управління та комп'ютерні мережі і компоненти, включаючи тисячі інтелектуальних датчиків, "розумних" лічильників і польових пристроїв, дозволять здійснювати управління в режимі реального часу, що обіцяє підвищити ефективність сьогоднішніх мереж і забезпечити швидку, безпечну, надійну і самовідновлювану мережу майбутнього. Якщо раніше ці системи управління були приватними та ізольованими, то зараз вони стають все більш інтероперабельними і підключаються до бізнес-, бездротових та інших мереж, щоб забезпечити ефективну і надійну роботу та інтегрувати технології "розумних" мереж. Але ці досягнення призвели до появи нових вразливостей і створили проблеми з кібербезпекою - це повсюдно є однією з найбільших сфер занепокоєння в електроенергетичному секторі, як виявила Дослідницька група, і попередні дослідження NIAC та подібні звіти високого рівня підтверджують це. Кілька членів Дослідницької групи висловили занепокоєння тим фактом, що виробництво систем управління та програмного забезпечення для ключового обладнання, яке використовується в центрах управління, часто передається на аутсорсинг за кордон, створюючи вразливість ланцюга поставок і надаючи можливість зловмисникам вставляти "лазівки" або зловмисні коди. Нещодавно виявлене шкідливе програмне забезпечення Stuxnet, спеціально розроблене для зараження промислових систем управління Siemens, що використовуються в енергетичній, ядерній та інших критично важливих галузях, демонструє потенційну здатність зловмисників розгортати цілеспрямовані зловмисні кібератаки. Stuxnet, який спочатку поширюється через заражену флешку, використовує комбінацію вразливостей, щоб отримати доступ до своєї цілі та впровадити код, який змінює технологічний процес. Енергокомпанії співпрацюють з національними лабораторіями та постачальниками систем, щоб оцінити свої системи на наявність вразливостей і розробити виправлення або пом'якшення наслідків, а багато великих комунальних підприємств беруть активну участь у федеральних науково-дослідних ініціативах, спрямованих на посилення

захисту сектору від кібер-атак. Деякі керівники розповіли нам, що у них є підземні бункери та резервні або дублюючі центри управління, щоб забезпечити продовження критично важливих операцій під час кіберзбою. Внутрішні навчання на випадок кіберподій стали звичним явищем, і багато керівників галузі беруть участь у національних навчаннях, таких як Cyber Shockwave 2010 і Cyber Storm III, що моделюють кібератаки, покликані перевірити, як уряд України та його партнери з приватного сектору реагуватимуть у режимі реального часу на масштабну кіберкризу. Зрозуміло, що ефективне подолання цих ризиків у національному масштабі вимагатиме скоординованого підходу в електроенергетичному секторі та з урядом країни.

Але кілька керівників заявили, що нинішні зусилля з координації між державним і приватним секторами є недостатніми. Хоча уряд співпрацює з промисловістю з питань кібербезпеки з 2020-х років, промисловість все ще не знає, які державні установи та посадові особи відповідають за кібернетичну надзвичайну ситуацію та які повноваження вони мають. Хоча національні розвідувальні служби відстежують кіберзагрози, неадекватні канали обміну інформацією позбавляють промисловість можливості ефективно виявляти свої вразливості та оцінювати наслідки атак. Дослідницька група дійшла висновку, що кібербезпека заслуговує на підвищену увагу як з боку NIAC, так і в рамках федеральних досліджень і розробок. Керівники компаній визначили її як пріоритетну тему для обговорення під час зустрічей на рівні керівництва між представниками промисловості та уряду.

Дослідження НКРЕ, проведене в червні 2013 року, визначило три високоімпульсні низькочастотні події, з якими наразі стикається об'єднана енергосистема, і зробило ці події пріоритетними для менеджерів з управління ризиками та осіб, відповідальних за розробку політики. Серед них - скоординована кібернетична, фізична або комбінована атака на північноамериканську об'єднану енергосистему; масштабна пандемія, що спричиняє втрату персоналу, критично важливого для роботи

електроенергетичної системи; геомагнітні збурення, спричинені або сонячною погодою, або висотним вибухом великої ядерної або електромагнітної зброї, що призводить до широкомасштабних перебоїв в роботі системи або деградації обладнання.9 У липні 2009 року під час навчань Secure Grid '09, проведених Національним університетом оборони, подібні події були визначені як значні ризики.10 Окрім потенційного далекосяжного впливу, події HILF викликають особливе занепокоєння, оскільки конкретні ризики недостатньо вивчені, їх пом'якшення коштує дорого, а відповідні ролі промисловості та уряду у протидії цим загрозам є незрозумілими. Хоча сектор має за плечима столітній досвід боротьби зі стихійними лихами, він має обмежений досвід боротьби з техногенними катастрофами - тероризмом, скоординованими атаками, кіберзлочинцями та пандемічними хворобами, - які можуть суттєво вплинути на великі регіони країни. Також мало або взагалі відсутній досвід координації між галузями та урядом, який може знадобитися під час події HILF. Наприклад, у випадку зловмисної атаки відсутній досвід координації дій для забезпечення захисту ремонтних бригад та доступу до місця злочину з метою швидкого відновлення послуг. Оператори електромереж також потребують кращих інструментів для вимірювання впливу тривалих відключень на споживачів на національному рівні.

В рамках процесу дослідження група взяла участь у "стресових вправах", організованих компанією Baltimore Gas & Electric, щоб оцінити здатність великого комунального підприємства реагувати на значні події, що виходять далеко за рамки звичайної підготовки, і це дало змогу отримати кілька важливих уроків: Інженерні швидкі рішення можуть спрацювати, але система буде нестабільною, і для повної реконструкції доведеться демонтувати тимчасове обладнання. Промисловість, уряд і споживачі повинні будуть пристосуватися до нових реалій серйозно пошкодженої мережі та змінити очікування щодо відновлення обслуговування. Високовольтні трансформатори є найбільш вразливим місцем; сама по собі

програма STEP не є довгостроковим рішенням. Уряд може сприяти відновленню, але має бути обережним, щоб не перешкоджати роботі галузі. Відновлювальні рішення, такі як резервні генератори, сонячні батареї, вимкнення кондиціонерів та віялові відключення, можуть зменшити навантаження на пошкоджену систему, але не існує панацеї для повного відновлення послуг за короткий проміжок часу. Угоди про взаємодопомогу та підрядники можуть допомогти у відновленні, але їхнє обладнання може бути несумісним з місцевими специфікаціями. Щоб полегшити координацію дій в умовах реальної надзвичайної ситуації, співробітники федеральних, регіональних і місцевих органів влади повинні регулярно брати участь у подібних навчаннях приватного сектору.

Недосконаліть механізмів обміну інформацією Не будучи загрозою сама по собі, відсутність своєчасної, дієвої та контекстуальної інформації про загрози заважає електроенергетичному сектору вживати належних заходів для протидії відомим ризикам. Особливо непослідовним є потік розвідувальної інформації про ризики, загрози та вразливості від уряду до керівників приватного сектору. Згідно зі звітом Управління урядової підзвітності за липень 2017 року, 98% приватного сектору очікують від уряду своєчасної та дієвої інформації про кіберзагрози, але лише 27% приватного сектору вважають, що така інформація надається.

Вразливість "Аврори", унікальна для генеруючого обладнання і виявлена національною лабораторією Міністерства енергетики у 2017 році, стала яскравим прикладом для опитаних нами керівників галузі. У той час як засекречені брифінги принесли ядерному сектору критично важливу інформацію про вразливість і способи її зменшення, відсутність допуску в електроенергетичному секторі залишила керівників компаній з обмеженими брифінгами, які містили мало інформації про проблему, а лише інформацію про те, як її виправити. Багато членів Дослідницької групи висловили велике розчарування з боку промисловості і дійшли висновку, що допуск на рівні вищого керівництва в усіх великих компаніях має вирішальне значення для

ефективного обміну інформацією - питання, добре задокументоване в попередніх дослідженнях NIAC. Хоча один з керівників заявив, що федеральні і розвідувальні агентства старанно інформують про конкретну загрозу тих, хто може бути зачеплений, передача інформації про загальні загрози і вразливості відбувається в мережах Міністерства національної безпеки і оборони штату, які, як очікується, мають передавати цю інформацію підприємствам, що надають послуги з енергопостачання, але їм бракує надійного і широко використовуваного каналу зв'язку. Однак, окрім допусків, цілеспрямована і контекстуалізована інформація з відкритих джерел може мати велику цінність для ширшої аудиторії менеджерів і операторів галузі. Насправді, один керівник, який був присутній на секретному брифінгу, що проводився Міністерством національної безпеки, повідомив, що найбільшу цінність для нього мала несекретна інформація з відкритих джерел, яку він отримав на цьому брифінгу. Центри злиття в розвідувальному співтоваристві почали залучати представників бізнесу для вирішення питань обміну інформацією. уряд країни також пропонує механізми та інструменти, такі як Інформаційна мережа національної безпеки - критичні сектори, які значно полегшують обмін інформацією між власниками та операторами критичної інфраструктури і різними державними установами. Регулярні новини з відкритих джерел, орієнтовані на кожен сектор, економлять час керівників на просіювання інформації та надають їм корисну і дієву інформацію без допуску до неї. Два приклади новинних звітів з відкритих джерел, доступних для електроенергетичного сектору, включають Щоденний звіт про інфраструктуру з відкритих джерел, підготовлений Управлінням захисту інфраструктури, та Звіт про поточну ситуацію, щотижневий аналіз кіберризиків, підготовлений Управлінням постачання електроенергії та енергетичної надійності Міністерства енергетики України, який надається окремим представникам галузі та науковцям. Усередині галузі компанії мають добре налагоджені механізми комунікації через взаємопов'язаність мереж та їхню взаємозалежність. В

останні роки сектор також рухається в напрямку впровадження внутрішніх засобів для безпечного та конфіденційного обміну інформацією про нововиявлені вразливості, кращі практики, уроки, винесені з інцидентів, тощо. Міжнародний форум з питань передачі (NATF), створений за зразком Інституту ядерної енергетики (INPO) в ядерному секторі, є конфіденційним форумом для 16 операторів систем передачі, які відверто обмінюються інформацією про події, кращими практиками та конструктивним зворотним зв'язком.

3.5 Практика забезпечення стійкості в електроенергетичному секторі

Розуміння стійкості в електроенергетичному секторі Переважною концепцією управління ризиками в електроенергетичному секторі є надійність, про що більш детально йдеться у Розділі 2. Коротко кажучи, надійність - це здатність задовольняти потреби в електроенергії кінцевих споживачів, навіть якщо певні події зменшують кількість доступної електроенергії - іншими словами, "підтримувати світло увімкненим". Хоча опитані нами керівники поділяють спільні концепції надійності, їхні погляди на визначення стійкості в електроенергетичному секторі різняться, коли їх просять дати визначення стійкості. Одні розглядали її як здатність швидко відновлюватися після відключення світла; інші - як набагато ширшу концепцію, що охоплює всі аспекти надійності. Дехто говорив про стійкість як про здатність переносити події та відновлювати роботу об'єктів після них. Стійкість також описували як елемент загального дизайну електричної системи: здатність великої взаємопов'язаної мережі поглинати удари. Конкретні визначення стійкості, однак, є менш важливими, ніж фундаментальні концепції стійкості, які в концепції стійкості NIAC включають надійність, винахідливість, швидке відновлення та адаптивність.

Ці концепції знаходять своє відображення у щоденних операційних та бізнес-практиках, які пронизують галузь. Нижче наведено огляд поточних

стратегій і практик у кожній із сфер стійкості, отриманий в результаті інтерв'ю з керівниками галузі, обговорень у дослідницькій групі та огляду літератури.

Надійність: Практики планування та управління ризиками Управління ризиками є невід'ємною частиною процесів, планування, практики та культури електроенергетичного сектору. Воно характеризується здатністю кількісно оцінити ймовірність та вплив атаки, оцінити вартість невдачі у порівнянні з вартістю пом'якшення наслідків та визначити пріоритетність варіантів пом'якшення наслідків. Компанії використовують різноманітні інструменти оцінювання для вивчення та оцінки ризиків, враховуючи такі фактори, як геологічна зона, стан активів та обладнання, взаємозв'язки та взаємозалежності, а також відомі загрози. Один з керівників повідомив, що використовує інструмент управління інвестиціями підприємства, який виставляє бали на основі вартості, потреб, ризиків та впливу на клієнтів, що допомагає компаніям визначати пріоритети потреб та інвестицій в інфраструктуру. Інші повідомили, що вони залучають комітети з управління ризиками в рамках компанії для прогнозування ризиків на основі минулого досвіду компанії та досвіду інших, щоб визначити як відомі, так і потенційні ризики та стратегії їх пом'якшення. Для довгострокового планування комунальні підприємства використовують моделі довгострокового планування, які прогнозують потреби в електроенергії та потенційні вразливості на 10 років і далі.

Періодичні загрози, такі як старіння обладнання та стихійні лиха, піддаються управлінню; досвід робить їх кількісно вимірюваними, більш передбачуваними і пропонує наочні приклади споживчих переваг інвестицій у пом'якшення наслідків стихійних лих. Однак традиційні інструменти управління ризиками виявляються неадекватними для сценаріїв подій HILF і зловмисних атак, таких як тероризм, кібератаки або внутрішній саботаж, де загрози, цілі, ймовірність і наслідки недостатньо зрозумілі. Наприклад, цілеспрямовані зловмисні атаки вимагають нових методів управління

ризиками, оскільки вони знижують цінність надмірності системи. За словами двох керівників, щоб протистояти зростаючому профілю ризиків, стратегії управління ризиками змінюються. Розбудова можливостей реагування та відновлення є дешевшою і гнучкішою, ніж зміцнення або резервування, оскільки дозволяє комунальним підприємствам реагувати на широкий спектр збоїв.

Попередження та захист від конкретної події може бути дорогим і залишає комунальні підприємства вразливими до інших ризиків. Опитані нами керівники повідомляють, що все більше уваги приділяється ефективному реагуванню та відновленню як стратегії управління ризиками. У галузі також докладаються спільні зусилля для покращення нагляду за ризиками з боку рад директорів, які, як правило, контролюють обов'язки генеральних директорів з управління ризиками. Тип інформації про ризики, що надається радам, має вирішальне значення; ради мають мало часу для вивчення 20-30 корпоративних ризиків, з якими їм часто доводиться стикатися, тому оператори і менеджери розробляють різні інструменти, такі як теплові карти, щоб допомогти членам ради у визначенні пріоритетності цих ризиків.

Наглядові ради також борються з відповідальністю за міжгалузеві або міжвідомчі ризики, оскільки відповідальність не є однозначною і чітко визначеною.

Винахідливість: Тренінги, навчання та тренування В електроенергетичному секторі широко використовуються тренінги, навчання та тренування не лише для покращення та вдосконалення існуючих планів реагування на кризові ситуації, але й для визначення активів та обладнання, які можуть отримати вигоду від підвищення надійності. Окремі компанії використовують схожі підходи до тренінгів, навчань та тренувань, хоча кожна компанія адаптує свій підхід до унікальних умов роботи, включаючи географічне розташування, найбільші ризики, розмір компанії та територію обслуговування, а також наявні ресурси, такі як доступ до національних

лабораторій. Опитані нами керівники розповіли, що вони застосовують різноманітні тренінги, вправи та навчання: Навчання з безперервності бізнесу, часто з використанням "гарячої точки" для дублювання реальних умов.

Стресові вправи для навмисного "зламу" системи з метою виявлення прогалин у стійкості Настільні навчання з ускладнюючими ефектами, що поширюються вглиб компанії та на сусідні зони обслуговування Оголошені та неоголошені навчання Спільні навчання з міськими та окружними установами Щорічні координаційні наради з реагуючими службами для обговорення нещодавніх подій та визначення отриманих уроків і найкращих практик

Настільні навчання для ситуацій "чорного старту" з метою відновлення після повного Використання груп реагування на вразливості для тестування та відпрацювання планів реагування на надзвичайні ситуації по всій компанії

Навчання "Ураган" на кожній операційній одиниці Плани відновлення енергосистеми, які відпрацьовуються для навчання операторів та підготовки всіх учасників для уточнення ролей та обов'язків Участь у національних навчаннях для забезпечення координації місцевих планів реагування на надзвичайні ситуації з Національною структурою реагування та Національною системою управління інцидентами.

Швидке відновлення: Реагування на аварійні ситуації Електромережа спроектована з урахуванням неминучості локальних збоїв, і кожна компанія готується до швидкого реагування та відновлення, виходячи з її розміру та ризиків, пов'язаних з географічним розташуванням об'єктів.

Реагування на надзвичайні ситуації та відновлення - це не план на випадок надзвичайних ситуацій, а невід'ємний аспект роботи електромережі.

Один з керівників визначив наступні ключові фактори, що сприяють швидкому відновленню:

Навчання в реальному часі та імітаційне моделювання.

Проектування резервування Забезпечення достатньої кількості запасних частин.

Добровільні та офіційні угоди про взаємодопомогу з іншими комунальними підприємствами

Хоча регіони готуються, наскільки це можливо, до відомих регіональних ризиків, сильні та історичні стихійні лиха навряд чи очікуються. До них важко підготуватися, і вони значно ускладнюють можливості реагування та відновлення місцевих електроенергетичних компаній, як показали повені в Закарпатті у 2010 році. Реагування та відновлення в умовах як відомих загроз, так і можливих серйозних подій вимагає ретельної підготовки, планів і процедур.

Нижче наведені практики, до яких, за словами керівників, вони вдаються для забезпечення швидкого та ефективного відновлення:

Коли погодні умови змінюються, компанії попереджають своїх постачальників, запасаються матеріалами та готують аварійні бригади. Хоча це може коштувати дорожче, один представник комунального підприємства сказав, що компанія заздалегідь розміщує бригади і керівників у стратегічних географічних зонах, щоб забезпечити швидке реагування.

Компанії, які мають власний будівельний і ремонтний персонал на місцях, переводять його в режим очікування. Інші комунальні підприємства починають працювати з контрактними службами, щоб привести їх у бойову готовність. Один з керівників повідомив, що його комунальне підприємство тримає під рукою список працівників, які нещодавно вийшли на пенсію і можуть бути мобілізовані для надання допомоги. Інший повідомив, що на підприємстві працює 600-800 працівників без залучення сторонніх спеціалістів.

Комунальні підприємства співпрацюють з постачальниками для попереднього пакування спеціальних комплектів, що містять аварійні запчастини та інше обладнання, і готують їх на комунальних складах для швидкого розподілу в разі потреби. Вводяться в дію попередні інженерні

плани заміни, і персонал починає готувати резервні ділянки для встановлення обладнання.

Формальні та неформальні угоди про взаємодопомогу, заздалегідь укладені з сусідніми комунальними службами та постачальниками, приводяться в оперативну готовність. Угоди про взаємодопомогу, як правило, організовані на регіональному рівні в Україні, вводяться в дію. Багато компаній створюють надлишкові запаси критично важливих матеріалів та обладнання на випадок, якщо заміна буде недоступна. Керівник невеликого комунального підприємства повідомив, що його компанія має запаси на суму 12 мільйонів гривень, тоді як більша компанія має власний склад запчастин вартістю 40-50 мільйонів гривень. Багато комунальних підприємств тримають під рукою мобільні запасні трансформатори і за певних обставин розгортають їх заздалегідь. Один представник великої компанії розповів, що компанія має 12 однофазних трансформаторів, які мають просту мобільну конструкцію. За можливості, комунальні підприємства залучають мобільні офіси або загальносистемні штормові центри по всьому регіону. За словами одного з керівників, він розгортає персонал реагування на вантажівках, оснащених найсучаснішими засобами зв'язку, тоді як інші залучають підрядників, які працюють у регіоні, а не працівників.

Комунальні служби зустрічаються з місцевою владою, щоб скоординувати реагування та відновлення, активувати плани реагування на надзвичайні ситуації та увімкнути лінії зв'язку для забезпечення безперервного потоку інформації.

ВИСНОВКИ

Основним принципом нашої стратегії національної безпеки є те, що вона є спільною відповідальністю приватного сектору, уряду, громад та окремих громадян. Це особливо стосується критично важливих об'єктів інфраструктури: вони здебільшого будуються, належать і експлуатуються приватним сектором; їхніми послугами та продуктами користуються підприємства, громадяни, громади та уряд; їхня громадська безпека та економічна стабільність забезпечується державним регулюванням і наглядом. Ми повинні творчо залучати та інтегрувати можливості всіх цих партнерів, щоб забезпечити стійкість критичної інфраструктури нашої країни.

Безперервність критичної інфраструктури є ключовим завданням для приватного і державного секторів. Компанії приватного сектору виділяють значні ресурси для забезпечення безперебійного обслуговування клієнтів, захисту інтересів акціонерів, виконання фідуціарних зобов'язань та захисту інвестицій у корпоративні активи. В електроенергетиці мільйони гривень і годин витрачаються на мінімізацію наслідків відключень і підготовку до всіх видів катастроф: природних явищ, аварій і зловмисних атак.

Для уряду безперервність роботи цих інфраструктур, зокрема електроенергетики, є критично важливою для виконання багатьох його основних місій: економічної стабільності та зростання, національної безпеки, громадської безпеки та якості життя.

У новому безпековому середовищі приватний сектор потребує міцного партнерства з урядом, щоб отримувати найкращу інформацію про загрози заздалегідь і в міру розгортання катастрофи, щоб забезпечити високий рівень стійкості, якого потребують і очікують клієнти.

Хоча всі партнери зацікавлені в безперервності критично важливих послуг і функцій, приватний сектор і місцеві громади, яким він служить, є партнерами на місцях під час кризи. Однак дуже часто державна політика та

нормативно-правові акти ігнорують, а не інтегрують найкращі практики, процеси та людей приватного сектору для забезпечення безперервності інфраструктури.

Рада вважає, що державно-приватне партнерство є фундаментальною стратегією для забезпечення захисту та стійкості нашої критичної інфраструктури. Цитуючи наше попереднє дослідження про партнерство, "воно являє собою найкращу довгострокову стратегію захисту наших критично важливих об'єктів інфраструктури, на відміну від регуляторних підходів, які є менш ефективними, менш дієвими і створюють антагонізм між суб'єктами державного і приватного секторів, які повинні співпрацювати для досягнення успіху". Стратегія національної безпеки, не лише визнає важливість стійкості інфраструктури для національної безпеки, але й посилює роль, яку відіграє державно-приватне партнерство у підвищенні стійкості.

Важливим контекстом наших висновків і рекомендацій є те, що спільна відповідальність не обов'язково означає однакову відповідальність або історичну відповідальність. Наші тематичні дослідження електроенергетичного сектора висвітлили окремі функції та унікальні можливості приватного сектору у проектуванні, будівництві, експлуатації та підтримці дедалі складнішої інфраструктури.

Держава допомагає зміцнювати і підтримувати ці функції, обмінюючись інформацією про ризики, забезпечуючи посилення регуляторного середовища, створюючи необхідні стимули для залучення інвестицій і надаючи ключові ресурси під час екстремальних катастроф, коли можливості приватного сектору вичерпуються.

Тематичні дослідження також показали, як зміна ландшафту ризиків змушує приватний сектор переосмислити традиційні межі між постачальниками послуг, клієнтами, громадами та урядом у забезпеченні надійності та стійкості електроенергетичного сектору. Наведені нижче висновки та рекомендації ґрунтуються на переконанні, що партнерський

підхід може об'єднати особливі можливості та досвід державного і приватного секторів для мінімізації інфраструктурних ризиків та підвищення стійкості.

Стійкість в електроенергетичному секторі

Електроенергетичний сектор України є вразливим від повітряних атак. Однак масштаби та глибина практик забезпечення стійкості, які регулярно застосовуються в цієї галузі, недостатньо зрозумілі та широко висвітлені. Це стало можливим завдяки суворим вимогам до планування, будівництва та експлуатації; взаємопов'язаній високовольтній об'єднаній енергосистемі, в якій виробництво та передача електроенергії динамічне управляються у високо структурований спосіб; а також завдяки сильній культурі прихильності до надійності та взаємодопомоги.

Місцева система розподілу електроенергії також є високонадійною і має історію швидкого відновлення після відключень, залучаючи ресурси інших комунальних підприємств у разі масових відключень. Надійність і стійкість секторів частково ґрунтується на їхній здатності вміло інтегрувати уроки, отримані під час минулих відключень електроенергії. Наше дослідження виявило сотні прикладів того, як енергокомпанії знижують ризики в повсякденній діяльності, використовуючи передові технології, процеси планування, практики відновлення, управління ланцюгами поставок, організацію компанії, навчання персоналу та системну архітектуру.

Багато з цих практик настільки вкоренилися в операційну діяльність і культуру комунальної енергетики, що багато хто в галузі називає їх не стійкістю, а радше основними принципами надійності, необхідними засобами безпеки або раціональними методами ведення бізнесу. Дехто за межами галузі може вважати, що стійкість електроенергетичного сектору означає, що світло ніколи не вимикається, і може не знати про значні ресурси, які витрачаються на мінімізацію ризиків усіх видів небезпек. Брак знань про роботу енергосистеми та відсутність спільної мови щодо стійкості створюють прогалину в розумінні стійкості в галузі та уряді.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Auerswald, Philip, and Debra van Opstal, “Coping with Turbulence: The Resilience Imperative,” Innovations: Special Edition for the World Economic Forum Annual Meeting 2019, (2019): 203–218. Cambridge, MA: Davos-Klosters. www.compete.org/images/uploads/File/PDF%20Files/INNOVATIONS-Davos-2009_Auerswald-vanOpstal.pdf.
2. Australian Government. Critical Infrastructure Resilience Strategy. Barton, Australia: Australian Government, 2019. www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF.
3. Australian Government. Critical Infrastructure Resilience Strategy Supplement: An overview of activities to deliver the Strategy. Barton, Australia: Australian Government, 2019. www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF.
4. Baker, Scott, Shaun Waterman, and George Ivanov. In the Crossfire: Critical Infrastructure in the Age of Cyber War – A global report on the threats facing key industries. Santa Clara, CA: McAfee, Inc., 2020. http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.

5. Baldor, Lolita C. “Computer hackers look to take over power US plants.” Alpharetta, GA: SecurityInfoWatch.com. August 4, 2021. www.securityinfowatch.com/Utilities+%2526+Public+Works/1317096.
6. Bast, Gautam. “Supply Chain Risk Management: A Delicate Balancing Act.” Somers, NY: IBM, 2008. ftp://ftp.software.ibm.com/common/ssi/rep_wh/n/GBW03015USEN/GBW03015USEN.PDF.
7. Behr, Peter. “Md.'s veto of advanced meter deployment stuns smart grid advocates.” The New York Times. June 23, 2020. www.nytimes.com/cwire/2010/06/23/23climatewire-mds-veto-of-advanced-meter-deployment-stuns-95998.html.
8. Behr, Peter. “Regulators assess the ultimate blackout threat.” ClimateWire. (July 2, 2010). www.eenews.net/public/climatewire/2020/07/02/1.
9. Borg, Scott. “Securing the Supply Chain for Electronic Equipment: A Strategy and Framework.” Internet Security Alliance. www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf.
10. Briggs, Rachel, and Charlie Edwards. The Business of Resilience: Corporate security for the 21st century. London: Demos, 2016. www.demos.co.uk/files/thebusinessofresilience.pdf.
11. Brown, Theresa. “Dependency Indicators.” Wiley Handbook of Science and Technology for Homeland Security, edited by John G. Voeller. Hoboken, NJ: Wiley, 2019. www.sandia.gov/nisac/docs/Dependency%20Indicators%20article%20w%20figs.doc.
12. Chang, Stephanie E. “Infrastructure Resilience to Disasters.” The Bridge 39, 4 (2019): 36–41. Washington, D.C.: National Academy of Engineering. www.nae.edu/File.aspx?id=17673.

13. Council on Competitiveness. Transform – The Resilient Economy: Integrating Competitiveness and Security. Washington, D.C.: Council on Competitiveness, 2017. www.tisp.org/index.cfm?pk=download&id=11018&pid=10261.
14. CSIS Commission on Cybersecurity for the 44th Presidency. Securing Cyberspace for the 44th Presidency. Washington, D.C.: Center for Strategic and International Studies, December 2022. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.
15. Daly, Sue. "NARUC's Critical Infrastructure Efforts." Presented to National Association of Regulatory Utility Commissioners Summer 2006 Water Committee Meetings, San Francisco, July 31, 2021, www.narucmeetings.org/Presentations/water_daly_s06.pdf.
16. Edison Electric Institute. "EEI Principles for Cyber Security and Critical Infrastructure Protection." Washington, D.C.: Edison Electric Institute, September 9, 2021.
17. Electric Power Research Institute. Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant's Structural Strength. Palo Alto, CA: Electric Power Research Institute, December 2022. www.stpnoc.com/EPRI%20study.doc.
18. Electric Power Research Institute. Nuclear Power Plant Risk Analysis and Management for Critical Asset Protection (RAMCAP) Trial: Applications Summary Report. Palo Alto, CA: Electric Power Research Institute, December 2015. http://my.epri.com/portal/server.pt?Abstract_id=000000000001011767.
19. Emergency Management and Response Information Sharing and Analysis Center. "The Concept of Resiliency." EMR-ISAC INFOGRAM 16-10. Emmitsburg, MD: U.S. Fire Administration, April 22, 2019. www.usfa.dhs.gov/downloads/pdf/infograms/16_10.pdf.
20. Fedora, Philip A. "Reliability Review of North American Gas/Electric System Interdependency." Presented by the Northeast Power Coordinating

Council. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Track 2, 2021. www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2004.1265195.

21. Flynn, Stephen E. "America the Resilient: Defying Terrorism and Mitigating Natural Disasters." Foreign Affairs. Tampa, FL: Council on Foreign Relations, March/April 2021. www.foreignaffairs.com/articles/63214/stephen-e-flynn/america-the-resilient.
22. Flynn, Stephen E. "We're still not ready for another Hurricane Katrina." Washington Post. August 29, 2021: B2.
23. Florida Reliability Coordinating Council. *FRCC System Disturbance and Underfrequency Load Shedding Event Report*. FRCC Event Analysis Team, October 20, 2008.
24. Fujii, Andrea. "Pumping Station Repaired, Water Pumped Into System." Channel 13 WJZ. April 8, 2021. http://wjz.com/local/Northern.Baltimore.County.2.1616420.html.
25. Gas/Electricity Interdependency of the NERC Planning Committee Task Force. Gas/Electricity Interdependencies and Recommendations. Princeton, NJ: North American Electric Reliability Council June 15, 2014. www.nerc.com/docs/docs/pubs/Gas_Electricity_Interdependencies_and_Recommendations.pdf.
26. Gaynor, Jeff. "The Resilience Imperative: The Case for Transforming National Infrastructure and Preparedness Policy, Programs and Standards to Ensure Critical Infrastructure and National Resilience." Paper presented to 2008 TISP Corporate, Community, and Government Resilience Day conference, Washington, D.C., January 24, 2018. www.tisp.org/index.cfm?pk=download&id=11040&pid=10261.
27. George Mason University School of Law, Critical Infrastructure Protection Program. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. Arlington, VA: George Mason University School of Law, Critical Infrastructure Protection Program Discussion Paper Series,

February 2017, http://cip.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf.

28. Geospatial Information and Technology Association. “Electric Sector Infrastructure Interdependencies.” The Geospatial Dimensions of Critical Infrastructure and Emergency Response: White Paper Series. Geospatial Information and Technology Center, Aurora, CO: July 7, 2019. www.gita.org/ciper/InterdependenciesElectric.pdf.
29. Goble, Gregg, Howard Fields, and Richard Cocchiara. Resilient infrastructure: Improving your business resilience. Somers, NY: IBM, September 2002. www.synergisticonline.com/files/resiliancy.pdf.
30. Greenberg, Michael R., Michael L. Lahr, and Nancy Mantell. “Understanding the Economic Costs and Benefits of Catastrophes and Their Aftermath: A Review and Suggestions for the U.S. Federal Government.” Risk Analysts 27, no 1. (2019): 83–96. http://policy.rutgers.edu/faculty/lahr/specialissuekatrina_4-21-06-mrg-1.pdf.
31. Heyman, David, and James Jay Carafano. Homeland Security 3.0: Building a National Enterprise to Keep America Free, Safe, and Prosperous. Washington, D.C.: CSIS, September 18, 2018. http://csis.org/files/media/csis/pubs/080918_homeland_sec_3dot0.pdf .
32. Homeland Security Studies and Analysis Institute. Resilience – Concept Development: An Operational Framework for Resilience. Arlington, VA: Homeland Security Studies and Analysis Institute, August 27, 2019. www.homelandsecurity.org/hsireports/Resilience_Task_09-01.pdf.
33. Hussey, Laura. “Utility Security & Resiliency: Working Together.” Edison Electric Institute PowerPoint presentation, before the Federal Utility Partners Working Group (FUPWG), November 19, 2018. www1.eere.energy.gov/femp/pdfs/fupwg_fall08_hussey.pdf.