МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

САВЧУК Кирило Вячеславович

Методика оцінки ризиків в системах критичної інфраструктури/ Risk Assessment Methodology in Critical Infrastructure Systems

Спеціальність 125 – Кібербезпека
Освітньо-професійна програма – Кібербезпека
Кваліфікаційна робота

Виконав студент групи КБм-22
К. В.Савчук
_____
Науковий керівник:
к.т.н., доцент Н. Г. Яцків
_____

кваліфікаційну роботу допущено
до захисту
"____" _____ 2023 р.
Завідувач кафедри
_____ В.В. Яцків

Тернопіль 2023

Факультет комп'ютерних інформаційних технологій

Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

САВЧУК КИРИЛО ВЯЧЕСЛАВОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Методика оцінки ризиків в системах критичної інфраструктури / Risk Assessment Methodology in Critical Infrastructure Systems
керівник роботи к.т.н., доцент Н.Г. Яцків

затверджені наказом по університету від 1 грудня 2022 року № 491

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– важливість оцінки ризиків у критичній інфраструктурі;
– сектори діяльності, які відносятся до критичних;
– визначити загальні етапи управління ризиками;
– визначити модель оцінки ризиків;
– визначити критерії оцінки ризиків;
– виконати аналіз ризиків з використанням визначенних моделі та критеріїв.

5. Перелік графічного матеріалу у роботі:
– сектори критичної інфраструктури;
– горизонт глобальних ризиків;
– фінансові втрати від сбоїв в критичній інфраструктурі;
– типи загроз по секторам критичної інфраструктури;
– процесс управління ризиками.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз предметної області	12.2022 р. – 03.2023 р.	
2	Аналіз моделей оцінки ризиків	03.2023 р. – 05.2023 р.	
3	Приклад оцінки ризиків	05.2023 р. – 11.2023 р.	

Студент _____ Савчук К.В.
(підпис)

Керівник роботи _____ к.т.н., доцент Н.Г. Яцків
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему "Методика оцінки ризиків в системах критичної інфраструктури" обсягом 76 сторінок включає 17 ілюстрацій, 1 додаток та 37 джерел за переліком посилань.

Метою даної роботи є розробити та обгрунтувати методику оцінки ризиків в системах критичної інфраструктури (КІ) з урахуванням сучасних тенденцій у сфері інформаційних технологій та загроз, що можуть впливати на нормальне функціонування цих систем. Аналіз літературних джерел та існуючих методологій дозволить систематизувати та узагальнити інформацію, а також ідентифікувати прогалини у наявних підходах.

Основні завдання включають визначення ключових понять, таких як "критична інфраструктура" та "ризик", а також аналіз факторів, що впливають на безпеку КІ. Дослідження спрямоване на формування чіткої та ефективної методики оцінки ризиків, які враховують специфіку критичної інфраструктури, зокрема її різноманітних секторів, від енергетики та транспорту до інформаційних технологій.

Окрім теоретичних аспектів, робота спрямована на практичне використання отриманих результатів у реальних умовах. Розробка конкретних прикладів оцінки ризиків у різних секторах КІ дозволить перевірити ефективність запропонованих методик та надати практичні рекомендації для підвищення рівня безпеки та стійкості критичної інфраструктури.

Результати роботи можуть бути корисні для спеціалістів у галузі кібербезпеки та всіх, хто цікавиться захистом критиної інфраструктури

Ключові слова: КРИТИЧНА ІНФРАСТРУКТУРА, ОЦІНКА РИЗИКІВ.

ABSTRACT

The master's thesis on the topic "Methodology of risk assessment in critical infrastructure systems" of 76 pages includes 17 illustrations, 1 appendices and 37 sources for the list of references.

The method of this work is to develop and justify the methodology of risk assessment in critical infrastructure (CI) systems, taking into account modern trends in the field of information technologies and threats that can affect the normal functioning of these systems. Analysis of literary sources and existing methodologies allows systematization and generalization of information, as well as identification of gaps in existing approaches.

The main tasks include the definition of key concepts such as "critical infrastructure" and "risk", as well as the analysis of factors affecting CI security. Research is aimed at forming a clear and effective risk assessment methodology that takes into account the specifics of critical infrastructure, in particular its various sectors, from energy and transport to information technology.

open theoretical aspects aimed at the practical use of the obtained results in real conditions. The development of specific examples of risk assessment in various sectors of CI will allow to check the effectiveness of the proposed methods and give practical recommendations for increasing the level of security and stability of critical infrastructure.

The results of the work can be useful for specialists in the field of cyber security and anyone interested in the protection of critical infrastructure.

Keywords: CRITICAL INFRASTRUCTURE, RISK ASSESSMENT.

ВСТУП

Критична інфраструктура відіграє важливу роль у національній безпеці та економічному процвітанні. Останні зрушення в глобальній обстановці безпеки, такі як терористичні атаки, війни, природні катастрофи та фінансова криза, змусили країни переглянути свої підходи до безпеки критичної інфраструктури. Кризові ситуації відзначили важливу роль урядів у створенні безпечної та стійкої інфраструктури.

Такі зміни також вимагають розгляду різноманіття загроз та небезпек для національної інфраструктури. Деякі країни, вже прийняли всебічний підхід до розв'язання цих викликів. Україна також активно вдосконалює свою нормативно-правову базу та захист критичної інфраструктури. Тенденції, такі як зміни клімату та демографічні зрушення, мають потенціал впливати на інфраструктуру у майбутньому, тому важливо враховувати їх при плануванні та будівництві інфраструктурних об'єктів.

Метою цього дослідження є розробка комплексної методики оцінки ризиків в системах критичної інфраструктури (КІ) для забезпечення їхньої стійкості та захисту від потенційних загроз. Розуміння та оцінка ризиків у різних секторах КІ є критичним для розробки ефективних стратегій безпеки, які враховують сучасні виклики, включаючи кіберзагрози, природні катастрофи та інші потенційні загрози.

Об'єкт дослідження – системи критичної інфраструктури, які включають у себе ключові сектори, такі як енергетика, транспорт, комунікації та інші важливі галузі, які забезпечують стійкість та функціонування суспільства.

Предмет дослідження – методика оцінки ризиків в системах критичної інфраструктури в контексті кібербезпеки. Ми зосереджуємося на розробці ефективних та комплексних методів визначення та оцінки потенційних загроз та ризиків, які можуть виникнути у сфері кібербезпеки для систем КІ.

Методи досліджень. У дослідженні використано аналіз літературних джерел, вивчення законодавства, апробацію теоретичних концепцій, моделювання ризиків, та програмування для аналізу моделей. Також враховано

сучасні підходи до кібербезпеки та використано інформаційні технології для аналізу та оцінки потенційних кіберзагроз у системах критичної інфраструктури.

Наукова новизна одержаних результатів. Науковою новизною цього дослідження є визначення переваг та недоліків оцінки ризиків в системах критичної інфраструктури, спрямованої на забезпечення кібербезпеки. Враховані сучасні тенденції у сфері кіберзахисту та адаптовані їх до потреб оцінки ризиків у важливих секторах, таких як енергетика, транспорт та комунікації.

Практичне значення отриманих результатів. Отримані результати мають безпосереднє практичне значення для управління та забезпечення безпеки систем критичної інфраструктури. Методика може бути використана національними та місцевими органи влади, а також операторами критичної інфраструктури для ефективної оцінки та управління кіберризиками. Впровадження розроблених підходів дозволить підвищити стійкість інфраструктурних систем до потенційних кіберзагроз, забезпечуючи надійність та безпеку функціонування критично важливих секторів.

Публікації та апробація КР.

1. Савчук К.В. Проблеми захисту критичної інфраструктури. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С.64-68.

2. Савчук К.В. Підходи до оцінки ризиків. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 170-172.

1 АНАЛІЗ ПРОБЛЕМИ ТА НАЯВНІ МЕТОДОЛОГІЇ

1.1 Визначення критичної інфраструктури

Критична інфраструктура є стратегічним фактором для економічного процвітання сучасних держав. Системи, що включають енергетику, транспорт, телекомунікації та інші ключові галузі, є не лише життєвоважливими для нормального функціонування суспільства, але й визначальними для розвитку бізнесу та економічної стабільності.

Отже, взаємодія між критичною інфраструктурою та економічним процвітанням є необхідною для сучасних держав. Інвестиції у розвиток та кібербезпеку цих систем визначають безпеку суспільства та підтримують економічний розвиток та високу якість життя громадян.

Загальні підходи до управління критичною інфраструктурою. Зважаючи на високий пріоритет та важливість п’ять країн (Канада, Нова Зеландія, Сполучені Штати, Сполучене Королівство, Австралія) об’єднались навколо питання критичної інфраструктури. [16,18,20,32]

Хоча кожна з п'яти країн має унікальні особливості, мета забезпечення безпеки та стійкості важливих інфраструктурних активів та систем однакова, і всі країни спрямовані на управління ризиками. Вони всі працюють над тим, щоб встановлювати партнерства з власниками та операторами, сприяють співпраці, обміну інформацією та управлінню ризиками. Ці загальні риси надають основу для розширення безпеки та стійкості критичної інфраструктури на міжнародному рівні та зміцнюють відносини між країнами.

Кожна з п'яти країн підтримує міцні партнерства з національними, регіональними та місцевими урядовими контрагентами, а також з власниками та операторами критичної інфраструктури. Ці партнерства є ключовими, оскільки системи критичної інфраструктури належать та експлуатуються як приватними, так і публічними зацікавленими сторонами. Крім того, всі партнери визнають важливість бути національним лідером у справах безпеки та стійкості

інфраструктури, і вони загалом працюють схожим чином для побудови цих партнерств.

Обмін інформацією також важливий для стратегії безпеки та стійкості критичної інфраструктури, і кожна країна прагне ділитися своєчасною та відповідною інформацією в безпечному та довіреному середовищі. Чи то через спеціальний бізнес-урядовий форум, який включає онлайн- та офлайн-взаємодії, такий як "Мережа довіри інформаційного обміну" Австралії (TISN), роботу Великобританії щодо створення безпечних "обмінів інформацією", які надають інструменти та ресурси онлайн для власників та операторів через безпечний інтернет-сайт, чи проведення форумів з відповідними спільнотами. Кожна країна активно займається створенням таких довірених каналів обміну інформацією за допомогою публічних веб-сайтів, інформаційних порталів та шлюзів, партнерств чи різноманітних інших підходів.

На національному рівні уряди працюють над тим, щоб зробити свою критичну інфраструктуру більш безпечною та стійкою з метою збереження та поліпшення наданих цією інфраструктурою ключових послуг. Нижче подано короткий огляд загальних заходів, які уряди приймають для сприяння безпеці та стійкості критичної інфраструктури та полегшення надання ключових послуг своїм населенням:

– Перегляд регіонів та використання їхніх аналітичних ресурсів для ідентифікації національно значущих секторів критичної інфраструктури та послуг, які вони надають.

– Координація з партнерами з публічного та приватного секторів щодо того, як зробити цю інфраструктуру більш безпечною та стійкою.

– Обмін важливою та своєчасною інформацією з відповідними зацікавленими сторонами.

– Співпраця з партнерами та зацікавленими сторонами у справі обміну кращими практиками.

– Визначення міжсекторальних залежностей.

– Створення робочої сили та культури, готової вирішувати складні виклики, що впливають на критичну інфраструктуру.

– Визначення та оцінка критичності інфраструктури.

– Використання підходу до управління ризиками, який визначає способи зменшення ризику для критичної інфраструктури.

За прогнозами Cybersecurity Ventures прогнозується, що глобальні витрати на кіберзлочинність зростатимуть на 15 відсотків щорічно до 2025 року, досягаючи 10,5 трильйонів доларів США, порівняно з 3 трильйонами доларів у 2015 році. Цей тренд створює найбільшу передачу економічного багатства в історії. Витрати на кіберзахист виявляються важливими, перевищуючи збитки від стихійних лих і переважаючі прибутковість світової торгівлі всіма основними незаконними наркотиками разом взятими [2,29,24,23].

1.2 Сектори критичної інфраструктури

В Україні сектори критичної інфраструктури [21-22] визначені постановою Кабінету Міністрів України від 9 жовтня 2020 р. N 1109 (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. N 1384):

– Паливно-енергетичний сектор.
– Цифрові технології.
– Захист інформації.
– Системи життєзабезпечення.
– Харчова промисловість та агропромисловий комплекс.
– Державний матеріальний резерв.
– Охорона здоров'я.
– Ринки капіталу та організовані товарні ринки.
– Фінансовий сектор.
– Транспорт і пошта.
– Промисловість.
– Сектор громадської безпеки.
– Цивільний захист населення і територій.

– Міграція (імміграція та еміграція).
– Охорона навколишнього природного середовища.
– Сектор оборони.
– Національна безпека.
– Правосуддя.
– Тримання під вартою.
– Наукові дослідження та розробки.
– Фінансовий сектор.
– Вибори та референдуми.
– Соціальний захист.
– Інформаційні послуги.
– Державна влада та місцеве самоврядування.

В постанові також наведена методика визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури для окремих секторів [21-22].

Критична інфраструктура Нової Зеландії**.** Критична інфраструктура є одним із шести ключових факторів економічного росту в Новій Зеландії. Новозеландський уряд визначає інфраструктуру як важливого учасника у підвищенні рівня життя всіх громадян. За його бажанням, до 2030 року інфраструктура країни повинна бути стійкою, координованою та сприяти економічному зростанню та підвищенню якості життя.

У своєму підході до критичної інфраструктури, Нова Зеландія акцентує на нових точках вразливості, викликаних інтегрованим та мережевим характером національних та міжнародних інфраструктур, таких як мережі енергетики, телекомунікації, транспорту та водопостачання. Кібербезпекова стратегія з 2011 року визначає поліпшення кібербезпеки для критичної національної інфраструктури як одну з головних мет.

Однак регулятивний підхід Нової Зеландії фокусується на захисті окремих активів критичної інфраструктури в межах конкретного сектору, як от порти,

аеропорти, телекомунікаційні мережі, електростанції та водозабірні установи, регулюються ізольовано. Питання стійкості визначається головним чином власниками та операторами критичної інфраструктури, і їхні рішення визначаються тиском від споживачів, регуляторних вимог та законодавства щодо надзвичайних ситуацій.

Секторно-секторний підхід (рисунок 1.1), який допомагає досягати стійкої критичної інфраструктури, історично був досить ефективним, проте його децентралізований характер породжує проблеми в спільному розумінні ризиків, вразливостей та міжзалежностей, відсутності єдиної системи стандартів та неспроможності координовано вирішувати проблеми в цій системі.

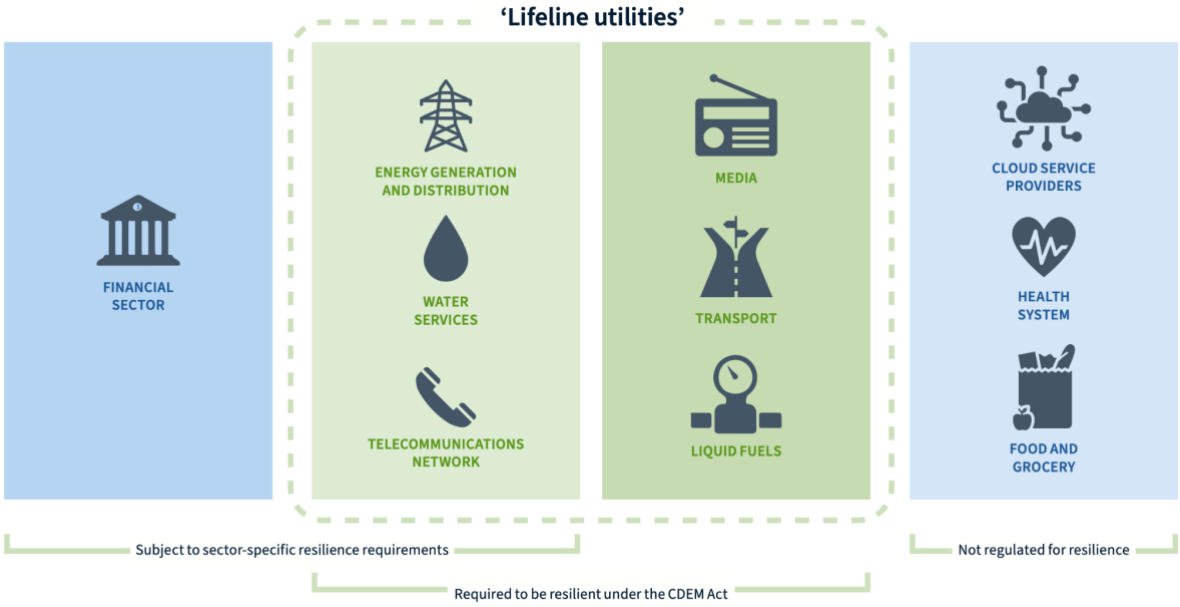

Рисунок 1.1 - Сектора КІ Нової Зеландії

Критична інфраструктура України та Нової Зеландії має 8 чітко виражених спільних секторів. Проте слід зазначити їх більшу регульованість в Новій Зеландії.

Критична інфраструктура Канади.

Проаналізувавши концепцію критичної інфраструктури в Канаді, можна визначити, що ця категорія включає в себе процеси, системи, об'єкти, технології, мережі, активи та послуги, які є важливими для здоров'я, безпеки, захисту та економічного добробуту канадців, а також ефективної роботи уряду.

Стратегічний візії Канади полягає в тому, щоб будувати безпечну, більш стійку та безпечну країну через розвиток її критичної інфраструктури. У Канаді, Emergency Management Framework for Canada [15], який визначає Національну стратегію щодо інфраструктури, визначає стійкість як "здатність системи, спільноти чи суспільства, яке відкрито ризикам, пристосовуватися до порушень, що виникають внаслідок ризиків, шляхом збереження, відновлення або зміни для досягнення і підтримання прийнятного рівня функціонування".

Національна стратегія щодо критичної інфраструктури ґрунтується на розумінні того, що "підвищення стійкості критичної інфраструктури може бути досягнуте за допомогою відповідної комбінації заходів безпеки для реагування на навмисні та випадкові події, практик для забезпечення бізнес-контингентності для подолання розладів та забезпечення продовження надання есенційних послуг, а також планування управління надзвичайними ситуаціями для забезпечення відповідних процедур реагування на непередбачені розлади та природні катастрофи". Крім того, Emergency Management Framework for Canada підкреслює важливість зменшення ризику через запобігання, пом'якшення, готовність, планування та реагування. У їхній концепції зменшення ризику від надзвичайних ситуацій закладено необхідність стійкості, яку вони визначають як "здатність системи, спільноти чи суспільства, яке відкрито ризикам, пристосовуватися до порушень, що виникають внаслідок ризиків, шляхом збереження, відновлення або зміни для досягнення і підтримання прийнятного рівня функціонування".

Критична інфраструктура Канади складається з наступних секторів:

– Energy and Utilities.
– Information and Communication Technology.
– Finance.
– Manufacturing.
– Food.
– Safety.
– Government.

– Transportation.
– Health.
– Water.

Проаналізувавши їх, можна зробити висновок що всі 10 секторів є спільними з списку секторів КІ України.

Критична інфраструктура Австралії.

Австралія визначає свою критичну інфраструктуру як фізичні споруди, ланцюги постачання, інформаційні технології та комунікаційні мережі, які, якщо б вони були знищені, зменшені або стали недоступні на тривалий період, значно вплинули б на соціальний або економічний добробут країни чи вплинули б на можливість проведення національної оборони та забезпечення національної безпеки. У визначенні враховується той факт, що деякі елементи критичної інфраструктури не є активами, а, насправді, представляють собою мережі чи ланцюги постачання.

Австралія вибрала підхід, спрямований на стійкість, до критичної інфраструктури з метою надання можливості адаптуватися до змін, зменшити експозицію країни до ризику та вивчити уроки з минулих подій. Австралія вказує, що ключовим елементом стійкості від катастроф є зміцнення "здатності витримувати та відновлюватися під час надзвичайних ситуацій і катастроф." Стратегія стійкості Австралії стимулює організації розглядати можливості бути гнучкими та адаптивними перед неочікуваними ударами. Критична стратегія стійкості критичної інфраструктури Австралії стверджує, що: "Підхід, спрямований на стійкість до управління ризиками для нашої критичної інфраструктури, підтримує організації в розвитку більш органічної здатності справлятися з раптовими ударами. Це віддає перевагу традиційному підходу до розробки планів для реагування на обмежений набір сценаріїв, особливо в умовах все більш складного середовища".

Сектори критичної інфраструктури Австралії:

– Banking and Finance.
– Communications.

– Energy.

– Food Chain.

– Health.

– Transport.

– Water Services.

– Other critical sub-sectors (Chemical manufacturing industry, Defence industries, Emergency Service).

Критична інфраструктура Сполученого Королівства.

Національна інфраструктура Сполученого Королівства включає в себе об'єкти, системи, місця та мережі, необхідні для функціонування країни та надання необхідних послуг, від яких залежить повсякденне життя. Сполучене Королівство використовує термін "критична інфраструктура" як "широкий термін для опису критичної національної інфраструктури та інших об'єктів інфраструктури національного значення, а також інфраструктури та активів місцевого значення." Уряд Сполученого Королівства визначає та регулює політику забезпечення безпеки критичної інфраструктури відносно терористичних загроз, а Секретаріат громадських надзвичайних ситуацій у Кабінеті міністрів керує політикою, спрямованою на підвищення стійкості критичної інфраструктури та зменшення впливу природних небезпек.

В рамках одного з об'єктивів Національної стратегії безпеки Сполученого Королівства передбачено "забезпечення безпеки та стійкості Великобританії - захист наших громадян, економіки, інфраструктури, території та способу життя від усіх основних ризиків, які можуть безпосередньо впливати на нас - вимагає як прямого захисту від реальних та конкретних загроз, так і стійкості у випадку природних та штучних надзвичайних ситуацій та злочинів, а також стримування менш ймовірних загроз, таких як військовий напад іншої держави."

Центр забезпечення національної інфраструктури Сполученого Королівства видає стратегічні поради, які слугують моделлю стійкості та надають найкращі практики та консультації для покращення безпеки та стійкості активів критичної інфраструктури Великобританії. В цих порадах зазначається,

що "створення стійкості в нашій інфраструктурі важливе для зменшення нашої вразливості перед природними небезпеками. Це можна досягти за допомогою поліпшення (де це необхідно) захисту; стимулювання здатності організацій та їхніх інфраструктурних мереж та систем поглиблювати удари та відновлюватися; та забезпечення ефективної локальної та національної відповіді на надзвичайні ситуації."

Визначення стійкості Сполученого Королівства визначається як "здатність активів, мереж та систем передбачати, поглиблювати, адаптуватися та/або швидко відновлюватися під час руйнівної події".

Сполучене Королівство має наступний перелік секторів інфраструктури визначений як критичний:

– Communications
– Health
– Emergency Services
– Government
– Energy
– Transportation
– Food
– Water
– Finance

Критична інфраструктура Сполучених Штатів. У Сполучених Штатах критична інфраструктура охоплює "системи та активи, будь-то фізичні чи віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів мало б пригнічувальний вплив на безпеку, національну економічну стійкість, національне здоров'я чи безпеку, або будь-яку комбінацію цих питань".

У Сполучених Штатах, в рамках президентської директиви Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, розробляється національна політика щодо сприяння безпеці та стійкості критичної інфраструктури. Критична інфраструктура нації забезпечує основні

послуги, які підтримують американське суспільство, тому критична інфраструктура повинна бути безпечною та здатною витримувати та швидко відновлюватися під час будь-яких небезпек. В PPD 21 обидві концепції - стійкість та безпека - визначаються так, де стійкість "означає здатність готуватися і адаптуватися до змінних умов та витримувати та швидко відновлюватися під час розладів. Стійкість включає здатність витримувати та відновлюватися від умисних нападів, нещасних випадків чи природних або штучних загроз чи інцидентів", а безпека вказує на "зменшення ризику для критичної інфраструктури за допомогою фізичних засобів чи захисних кіберзаходів від вторгнень, нападів чи впливу природних чи штучних катастроф".

Критична інфраструктура Сполучених Штатів нараховує 16 секторів:

– Chemical.
– Financial Services.
– Commercial Facilities.
– Food and Agriculture.
– Communications.
– Government Facilities.
– Critical Manufacturing.
– Healthcare and Public Health.
– Dams.
– Information Technology.
– Defense Industrial Base.
– Nuclear Reactors, Materials and Waste.
– Emergency Services.
– Transportation Systems.
– Energy.
– Water and Wastewater Systems.

Опис секторів цих секторів, а також інформація про відповідальний орган знаходяться на рисунку 1.2 [38].

Рисунок 1.2 - Сектора КІ та відповідальні агенції США

1.3 Глобальні ризики та загрози КІ

Аналіз звіту "The Global Risks Report 2021" [14] вказує на те, що у світових лідерів та топ-менеджменту компаній протягом наступних п'яти років особлива увага буде приділятися ризикам, пов'язаним із порушенням безпеки, витоком даних і відмовою IT-інфраструктури (рисунок 1.3). Це відображає загальний тренд, де кібербезпека та цифрові аспекти стають ключовими аспектами глобальної стратегічної стійкості.

Зростання цифрової залежності супроводжується ризиками, пов'язаними з кіберзлочинністю та кібератаками. Розгляд цих питань на високому рівні визначає важливість прийняття превентивних заходів, розвитку кібербезпекових стратегій та підвищення готовності до подібних викликів у майбутньому.

У світі, де технології стають все більш важливим чинником для економічного та соціального розвитку, реагування на ці виклики вимагатиме спільних зусиль та координації на міжнародному рівні. Тільки шляхом об'єднання зусиль можна буде забезпечити стійке та безпечне цифрове майбутнє.

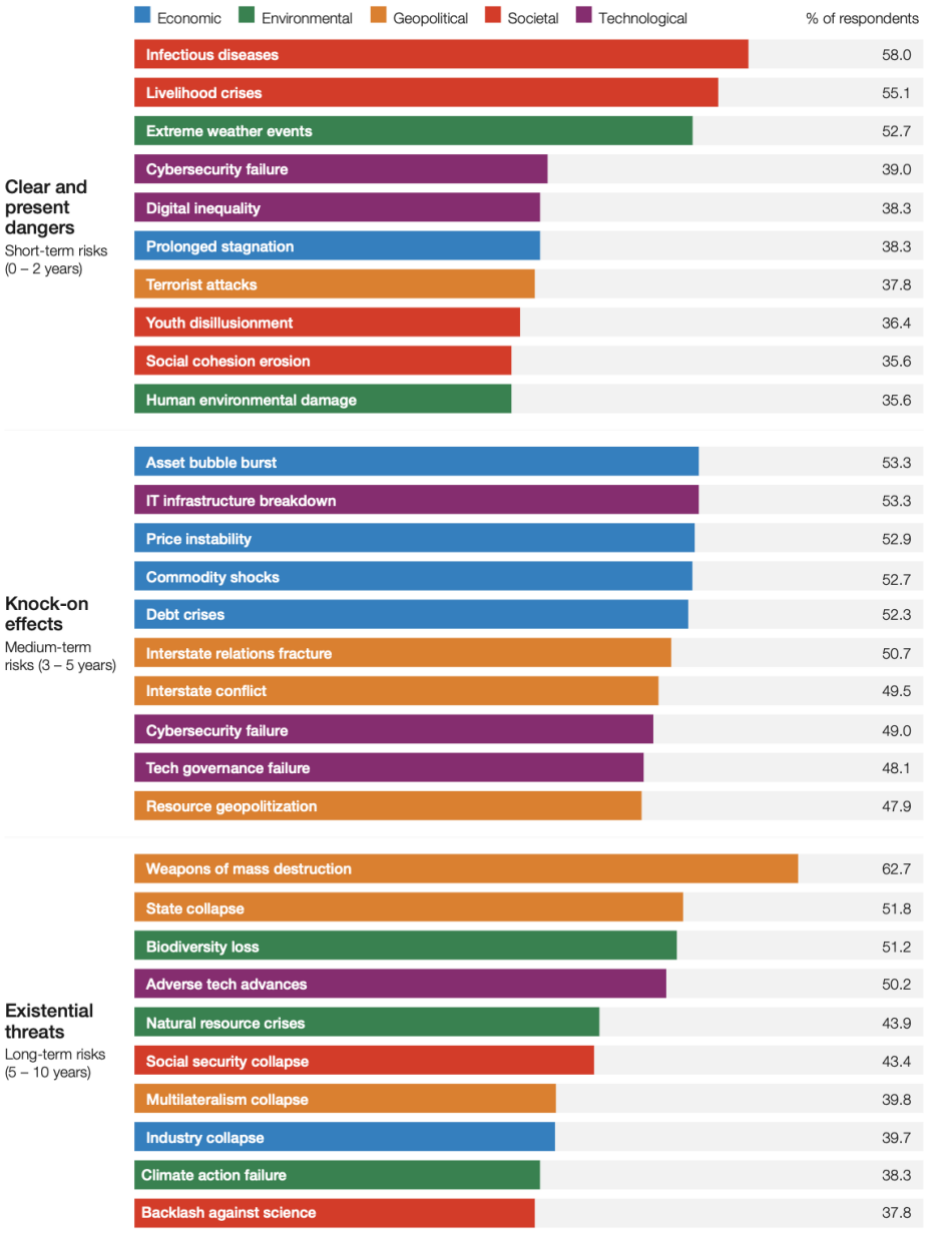

Рисунок 1.3 - Global Risks Horizon

1.4 Втрати заподіяні інцидентами на об’єктах КІ

Дані “The cost of incidents affecting CIIs” [3] свідчать, що фінансові послуги та сектори, пов'язані з енергетикою, відчули найсильніший економічний удар внаслідок кіберзлочинності.

Там зазначено с посиланням на дослідження "Energy market review", виконане компанією Willis Lihmited, що економічні втрати в енергетичному секторі Великої Британії за 2014 рік склали 545 мільйонів євро (400 мільйонів фунтів стерлінгів).

В дослідженні "2015 Cost of Data Breach Study: Global Analysis" від Ponemon аналізуються світові витрати на одну особу в різних секторах у 2015 році. Так в дослідженні приходить до висновку, що середня вартість становить приблизно 154 долари. Дослідження охоплює лише витоки даних і виявило, що в сильно регульованих областях вартість витоку даних на одну особу суттєво вища, ніж в менше регульованих або нерегульованих областях.

Дослідження "2014 Cost of Cyber Crime Study: Germany" від Ponemon показує середню річну вартість за галузевими секторами в Німеччині, порівнюючи дані з трьох різних фінансових років. Фінансові послуги та енергетика та комунальні послуги зазнали вищих витрат у всіх трьох річних дослідженнях. Крім того, сектори освіти та досліджень та громадського сектору відчули значний зріст витрат. З іншого боку, організації в галузі HoReCa, медіа та роздрібної торгівлі, здавалося, мають менший загальний економічний вплив протягом останніх років.

"2015 Cost of Cyber Crime Study: Global" від Ponemon надає середньорічні узагальнені витрати за галузевими секторами з 252 компаній по всьому світу (рисунок 1.4).

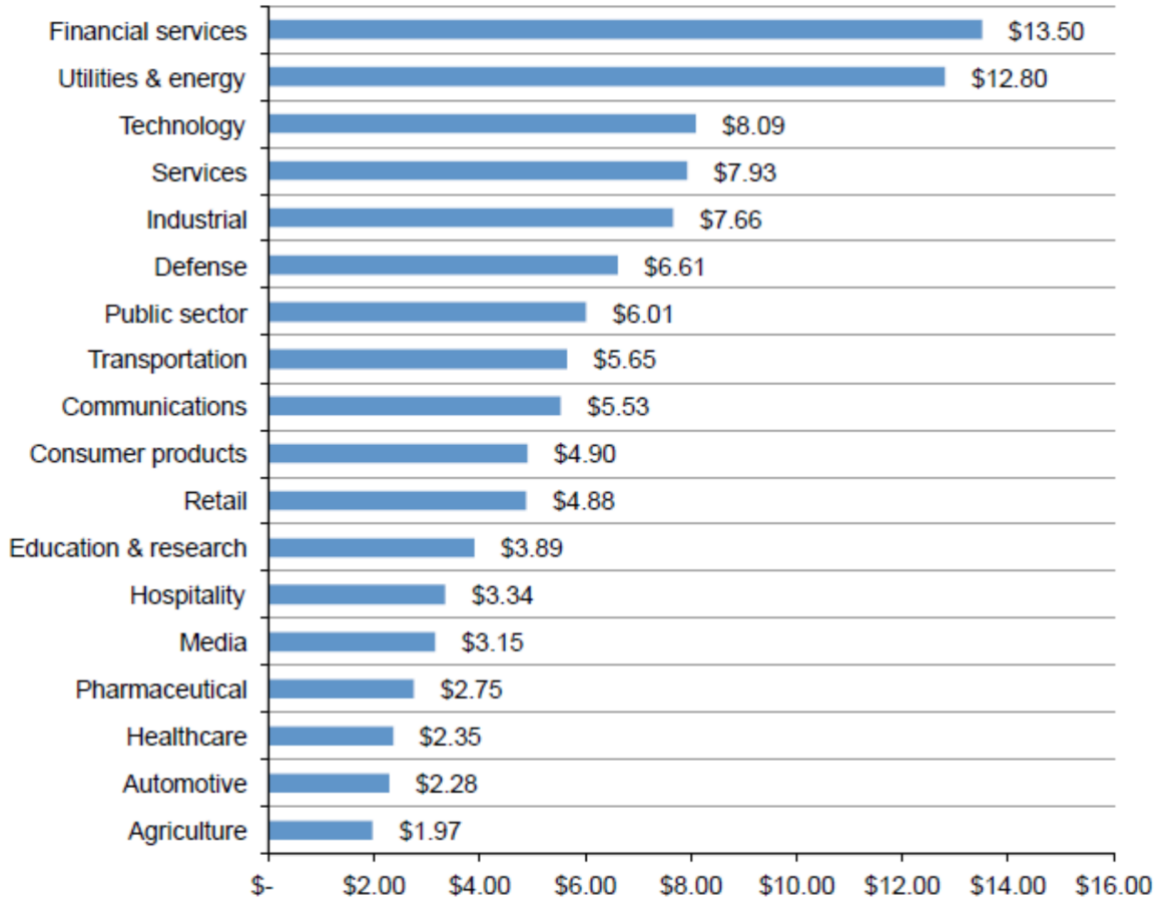

Рисунок 1.4 - Середньорічні витрати за галузевими секторами (млн.) 2015

Також наведені дані конкретних випадків для кожного сектору та середню вартість кожного типу інциденту. У більшості випадків типи інцидентів можна розглядати як загрози (рисунок 1.6).

DoS/DDoS здається найбільш поширеним типом загрози, вказаним у 13 з 17 досліджень (рисунок 1.5). Другим за частотою загрозами є: Malware (12), Insider threat (8), Phishing (9), Web-based attacks (8) та cyber-espionage (рисунок 1.7). В дослідженнях немає інформації щодо ICS/SCADA, хоча це було в центрі уваги громадськості протягом останніх років. Фізичні збитки/крадіжки/втрати також не згадуються в жодному з досліджень.

В цій роботі також наведені дані стосовно розповсюдження кіберзагроз загроз для різних секторів критичної інфраструктури.

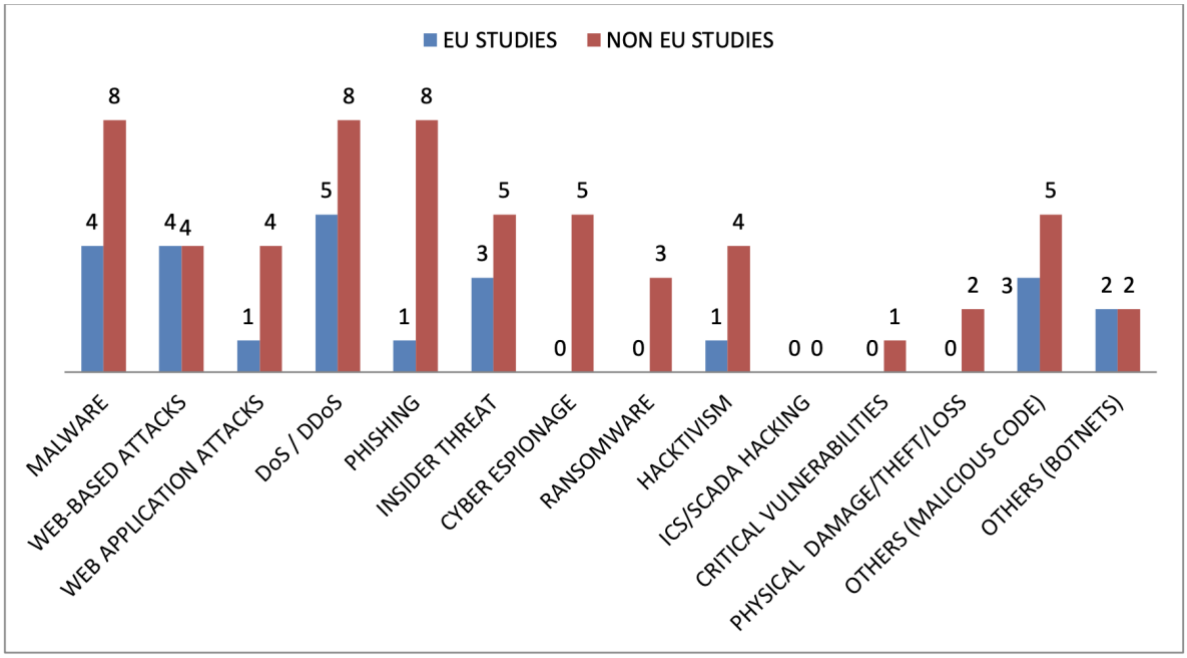

Рисунок 1.5 - Загрози, виявлені в ході досліджень

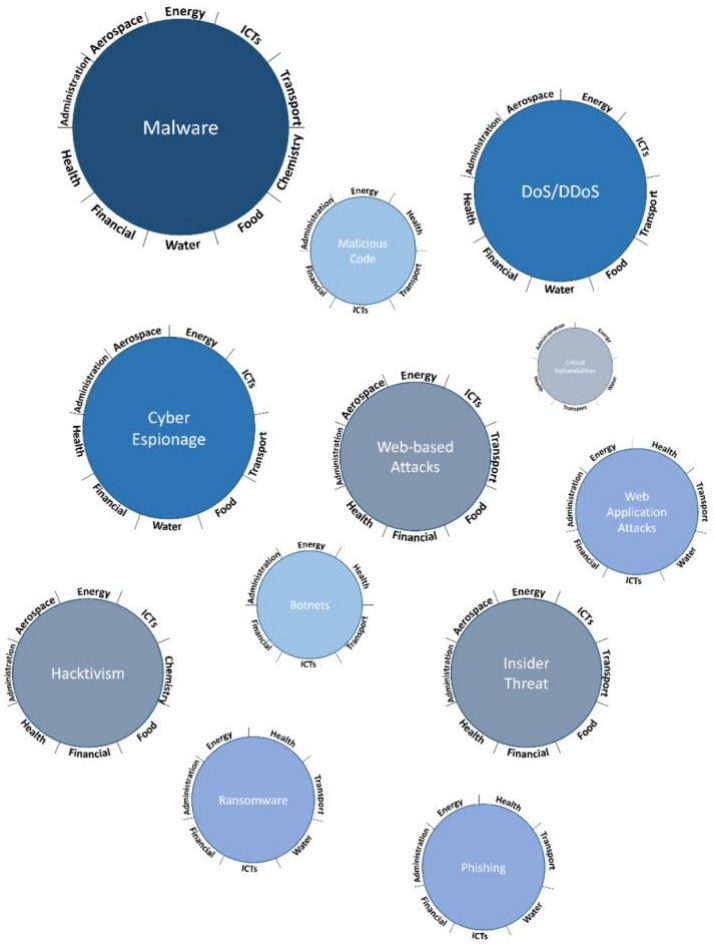

Рисунок 1.6 - Типи загроз/атаки на сектор КІ

Nr.	Attack / Threat	Number of studies per sector									
		Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

Рисунок 1.7 - Типи загроз/атаки на сектор КІ

Дослідження Deloitte [23] показує, що кібер атаки зокрема на енергетичний сектор зростають та стають все більш системними.

В публікації зазначено, що напади на системи керування промисловістю (ICS), які розвивалися протягом десятиліть, розмивають межі між кібератаками та фізичними атаками, піднімаючи питання національної безпеки у багатьох країнах. Атаки на ICS змінюються за обсягом і цілями по всьому світу (рисунок 1.8). Зловмисники використовуючи програмне забезпечення, створене для легітимних цілей, такі як Shodan та Metasploit, для виявлення компонентів та пристроїв, підключених до Інтернету, та акати на систем управління та збирання даних (SCADA) та інші програми.

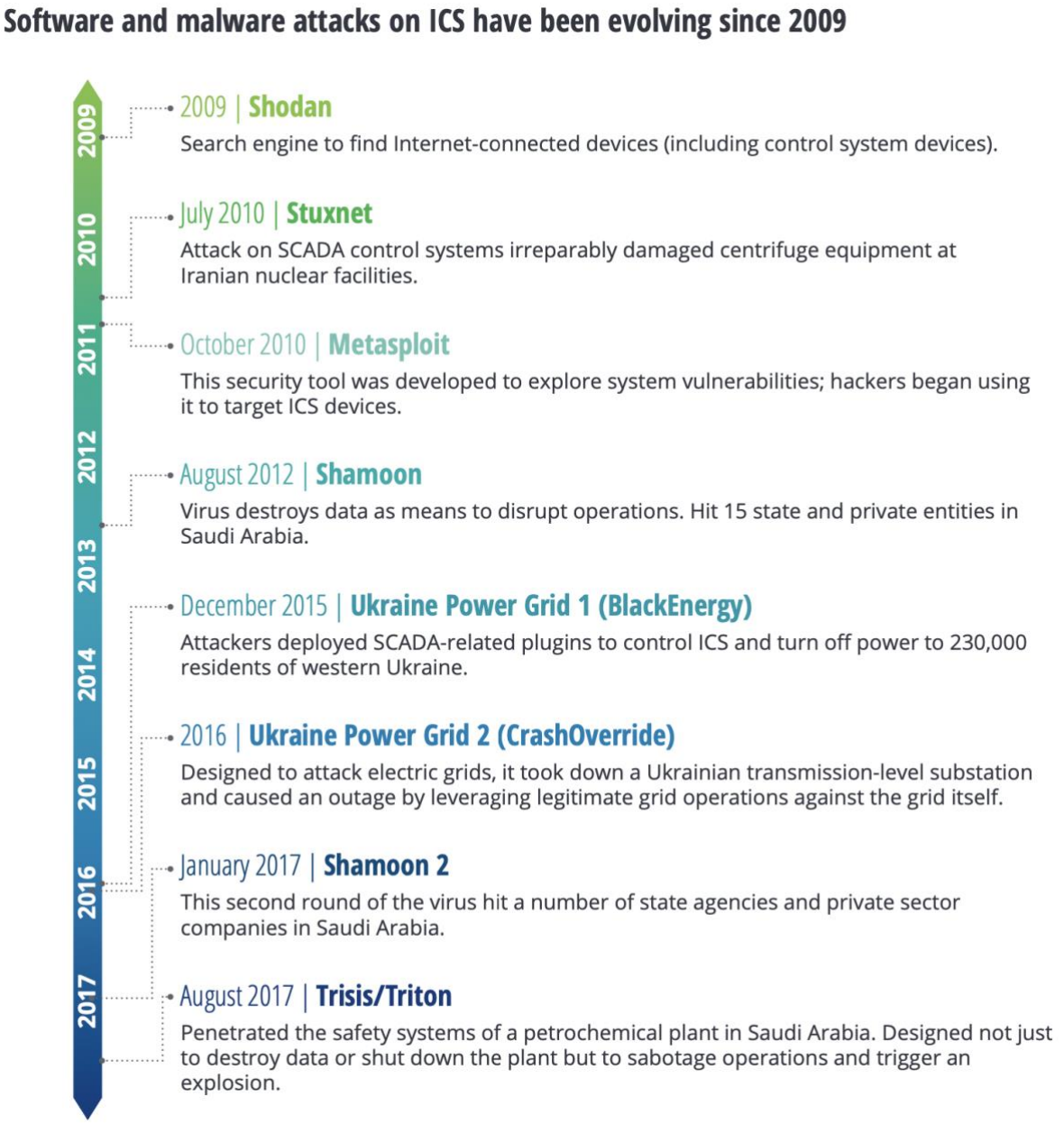

Рисунок 1.8 - Світові атаки на енергетичний сектор

В публікації також зазначено 3 основних нападника на енергетичний сектор Сполучених Штатів - це організовані злочинні групи, інші держави та внутрішній персонал (рисунок 1.9).

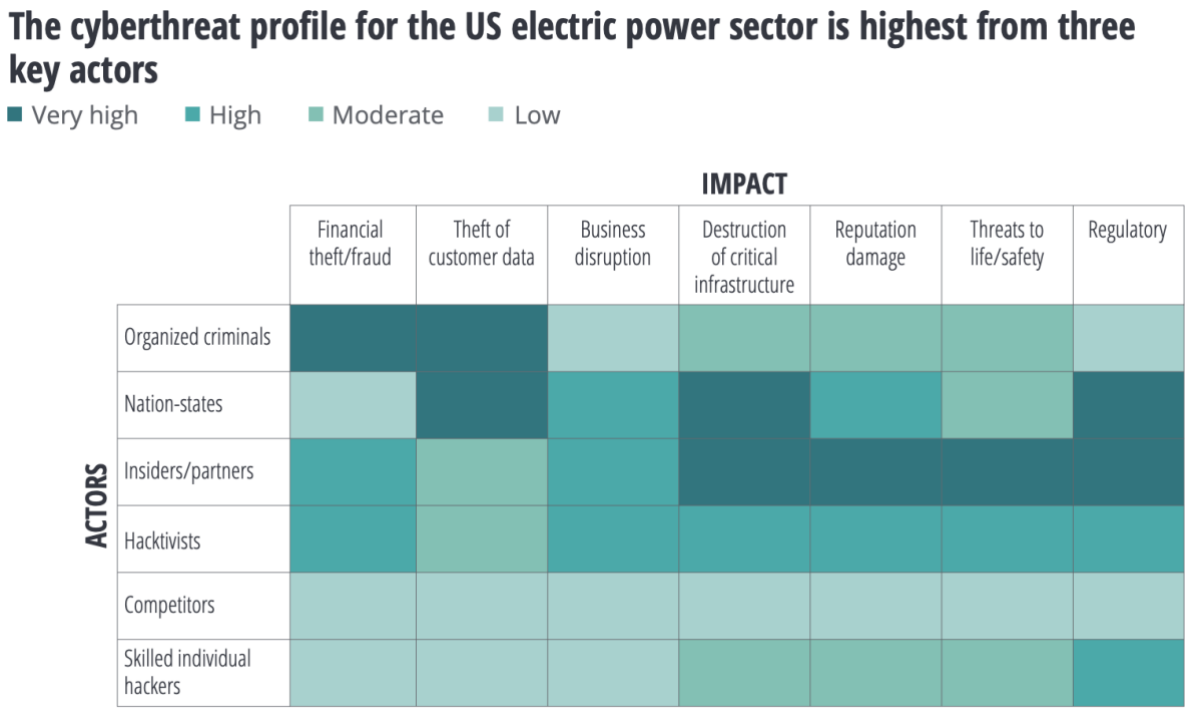

Рисунок 1.9 - Основні нападники на енергетичний сектор США

Аналізуючи ці дані та інші джерела можна зробити наступні висновки про кібер-атаки на різні сектори критичної інфраструктури.

Економічні:

– Найбільше шкоди завдають зловмисники всередині організацій, атаки на відмову в обслуговуванні та веб-атаки.

– Збитки від кіберзлочинності для організацій продовжують зростати, причому їхня вартість залежить від розміру організації.

– Витрати на кіберзлочинність можуть досягати 1,6% ВВП для деяких країн на рік.

– Країни будуть терпіти зловмисну діяльність до тих пір, поки вона залишатиметься на прийнятному рівні, менше 2% національного доходу.

– Перебої в бізнесі є найбільшим зовнішнім збитком, за ними йдуть витрати, пов'язані з втратою інформації.

– Кіберзлочинність уповільнює темпи глобальних інновацій, знижуючи віддачу для інноваторів та інвесторів.

– Потреба в підготовці та інвестуванні в реагування на інциденти зазвичай виникає лише після події зі значним впливом.

– Вартість кіберзлочинності продовжуватиме зростати, оскільки більше бізнес-функцій переходить на онлайн-платформи, а більше компаній і споживачів у всьому світі підключаються до Інтернету.

– Виявлення інцидентів є найдорожчим внутрішнім видом діяльності, за яким слідує відновлення.

– Впровадження практик управління безпекою підприємства зменшує вартість кіберзлочинності.

– Стимули в кіберзлочинності сприяють атакам і перешкоджають захисту.

– Найкращі дані, пов'язані з кіберзлочинністю, надходять від фінансового сектору, який є регульованим, приділяє серйозну увагу кібербезпеці, може легко виміряти втрати, будучи також однією з найбільш атакованих галузей.

– Час, необхідний для виявлення та стримування порушення даних, прямо впливає на його вартість.

Організаційні:

– Компанії потребують кваліфікованого персоналу, але в деяких випадках його повністю відсутній.

– Наймання недостатньо кваліфікованих працівників означає більший ризик.

– Компанії, які не зможуть належним чином захистити свої мережі, опиняться у все більш невигідному становищі.

Управлінські:

– Участь правління, придбання кіберстрахування та політики управління безперервністю бізнесу можуть знизити вартість порушення даних.

– Урядам необхідно збирати та публікувати дані про кіберзлочинність, а також допомагати країнам і компаніям робити кращий вибір щодо ризиків і політики.

Технічні:

– Найбільш постраждалими секторами КІ є фінансовий, телекомунікаційни та енергетичний.

– Більшість організацій досі не впровадила основні елементи керування безпекою.

– Зловмисники вдосконалюють свої методи, тоді як компанії використовують старі тактики боротьби.

– Час виявлення інцидентів триває довше, ніж час компрометації.

– У більшості випадків зловмисники можуть скомпрометувати організацію протягом кількох хвилин.

– Хакери та зловмисники всередині організації є причиною більшості порушень даних.

– Використання вразливостей браузера, операційної системи та іншого стороннього програмного забезпечення (наприклад, Flash і Java) для зараження систем кінцевих користувачів є звичайним першим кроком для зловмисників.

– Впровадження систем обміну даними про загрози безпеки є ефективним.

– Велика кількість вразливостей були використані через рік або більше після того як про них стало відомо; patch management все ще лишається найслабшою ланкою захисту.

2 АНАЛІЗ МОДЕЛЕЙ ОЦІНКИ РИЗИКІВ

2.1 Еволюція ризик-менеджменту та формування стандартів

Історія ризик-менеджменту налічує багато століть, і за цей час було розроблено безліч методів оцінки ризиків. Перші спроби управління ризиками були зроблені ще в Стародавньому Римі. Римські легіонери використовували метод аналізу ризиків для оцінки ймовірності перемоги в битві. Вони враховували такі фактори, як чисельність військ, їхній досвід, а також місцеві умови.

У Середні віки ризик-менеджментом займалися переважно торговці. Вони використовували метод імовірнісного аналізу для оцінки ризику фінансових операцій.

У 17 столітті в Європі почали розвиватися страхові компанії. Вони використовували метод статистичного аналізу для оцінки ризику страхових випадків.

У 20 столітті розвиток ризик-менеджменту отримав новий імпульс. Це було пов'язано з появою нових технологій, таких як авіація, атомна енергія та інформаційні технології. Ці технології створювали нові ризики, які вимагали нових методів управління.

У другій половині 20 століття в США був розроблений метод управління ризиками за проектом (Project Management Institute Risk Management Body of Knowledge). Цей метод був заснований на принципах системного підходу до управління ризиками.

У 1990-х роках у міжнародній спільноті почалися роботи зі стандартизації методів оцінки ризиків. У 2009 році була опублікована перша версія міжнародного стандарту ISO 31000:2009 "Менеджмент ризиків. Принципи та настанови". Цей стандарт став основою для розробки національних стандартів оцінки ризиків у багатьох країнах світу. [36]

У 2018 році була опублікована друга версія стандарту ISO 31000:2018. Ця версія стандарту внесла ряд удосконалень, зокрема:

– більший акцент на системному підході до управління ризиками.

– більшу увагу до інтеграції управління ризиками з іншими процесами організації.

– більшу увагу до управління ризиками в контексті сталого розвитку.

З розвитком кібербезпеки також з’явились спеціалізовані стандарти оцінки ризиків. Одним з найважливіших стандартів є ISO/IEC 27005:2018. Цей стандарт визначає процес управління ризиками інформаційної безпеки, який заснований на принципах стандарту ISO 31000.

Інші важливі стандарти оцінки ризиків у кібербезпеці включають:

– NIST SP 800-30: Risk Management Guide for Information Technology Systems.

– PCI DSS v3: Payment Card Industry Data Security Standard.

– ISO/IEC 27019: Information security management. Information security for the protection of personal data. [37]

– ISACA Risk IT Framework.

Стандарти оцінки ризиків є важливим інструментом для ефективного управління ризиками. Вони забезпечують уніфікований підхід до оцінки ризиків, що дозволяє порівнювати результати оцінки ризиків, проведені в різних організаціях.

Підхід на основі оцінки ризиків є критичним для надання довгострокової стійкості та конкурентоспроможності в сучасному цифровому ландшафті. Розуміння ризиків та їхнє систематичне управління допомагають організаціям не лише пристосовуватися до непередбачуваних викликів, але і активно формувати стратегії, спрямовані на зменшення ймовірності та наслідків можливих загроз. Завдяки цьому підходу, компанії можуть забезпечити високий рівень безпеки, довіри та стабільності, забезпечуючи успішний розвиток у цифровому віці.

У кібербезпеці стандарти оцінки ризиків є невід'ємною частиною системи управління інформаційною безпекою. Вони допомагають організаціям оцінювати ризики, пов'язані з інформаційною безпекою, і розробляти ефективні заходи щодо їх мінімізації.

2.2 Загальні етапи управління ризиками

Управління ризиками є невід'ємною складовою ефективного управління будь-якою організацією чи проектом. Цей процес визначається загальними етапами, які допомагають ідентифікувати, аналізувати, контролювати та мінімізувати можливі негативні впливи на досягнення мети.

Перший етап полягає в визначенні можливих ризиків, які можуть вплинути на організацію чи проект. Це включає в себе огляд всіх можливих джерел ризиків, таких як внутрішні та зовнішні фактори, технічні проблеми, фінансові небезпеки та інші аспекти, які можуть призвести до негативних наслідків.

На другому етапі вивчаються індивідуальні ризики, їх ймовірність та вплив на проект чи діяльність. Це дозволяє визначити пріоритети та визначити ті ризики, які можуть мати найбільший вплив на досягнення цілей.

З урахуванням ідентифікованих та проаналізованих ризиків розробляється стратегія управління ризиками. Це включає в себе розробку плану дій для кожного визначеного ризику, визначення відповідальних осіб та виділення ресурсів.

На цьому етапі реалізується розроблений раніше план дій. Команди вживають конкретних заходів для мінімізації або усунення ризиків, а також встановлюють системи моніторингу для вчасного виявлення змін у ситуації.

Останній етап включає в себе постійний моніторинг ризиків та відстеження ефективності заходів з управління. Всі зміни в середовищі або в самому проекті перевіряються, і, при необхідності, коригуються стратегії управління ризиками.

Важливою передумовою ефективного управління ризиками є визначення контексту, в якому діє організація чи реалізується проект. Цей етап включає у себе аналіз зовнішнього середовища та внутрішніх факторів, що можуть впливати на досягнення цілей. Зовнішні фактори можуть включати економічні, політичні, соціокультурні та технологічні аспекти, тоді як внутрішні – це структура організації, її культура, ресурси та процеси. Визначення контексту

надає змогу зрозуміти обставини, в яких приймаються управлінські рішення, що є ключовим для визначення та ефективного управління ризиками.

Всі ці етапи (рисунок 2.1) спільно створюють систему управління ризиками, що дозволяє організаціям ефективно адаптуватися до невизначеності та мінімізувати ймовірність виникнення негативних наслідків.

Рисунок 2.1 - Робочий процес управління ризиками

2.2 Аналіз стандартів та фреймворків оцінки ризиків

ISO 31000:2018 - Risk management.

Стандарт ISO 31000 відіграє ключову роль у систематизації та управлінні ризиками в різних сферах діяльності. У сучасному світі, де невизначеність та змінність стали неотримуваними факторами, управління ризиками є важливою складовою стратегічного планування. Стандарт ISO 31000 визначає загальноприйняті принципи та підходи до управління ризиками, що сприяє створенню стабільних та ефективних систем управління в усіх галузях.

Процес стандартизації управління ризиками визначеною мірою почався у середині XX століття. Проте, ефективна система, яка б охоплювала різні сфери діяльності та враховувала глобальні виклики, виявилася дуже потрібною лише у динамічному сучасному середовищі. У цьому контексті виникла необхідність

створення стандарту, який би визначав єдині принципи управління ризиками, застосовні в усіх областях.

Стандарт ISO 31000 був вперше опублікований в 2009 році Міжнародною організацією зі стандартизації (ISO). Його створення було спрямовано на визначення загальних та універсальних принципів, які допомагають підприємствам та організаціям ефективно управляти ризиками.

З того часу стандарт пройшов кілька оновлень та вдосконалень. Різноманітні сектори економіки та галузі діяльності активно впроваджують ISO 31000 для покращення стратегічного управління та забезпечення стабільності в умовах невизначеності.

Розвиток стандарту свідчить про його актуальність в умовах постійних змін у світі бізнесу та технологій. Запровадження ISO 31000 допомагає не тільки підвищити рівень безпеки та стабільності, але і сприяє вдосконаленню стратегічного планування в організаціях всіх масштабів.

Стандарт ISO 31000 визначає ряд основних принципів, які є ключовими для ефективного управління ризиками в будь-якій сфері діяльності. Розглянемо ці принципи:

– ISO 31000 рекомендує інтегрувати управління ризиками в усі аспекти стратегічного та операційного управління підприємством. Це сприяє створенню єдиної системи, яка враховує ризики на всіх рівнях.

– Стандарт рекомендує дотримуватися системного підходу при оцінці та управлінні ризиками. Це означає розгляд ризиків як частини великої системи, де взаємодія компонентів може впливати на загальний результат.

– Для ефективного управління ризиками важливо визначити контекст, в якому працює організація. Розуміння зовнішнього та внутрішнього середовища допомагає адаптувати стратегії та заходи безпеки.

– Принцип оцінки вирогідності та впливу визначає, що оцінка ризиків повинна враховувати імовірність виникнення загрози та можливі наслідки. Це дозволяє приділяти увагу найбільш значущим ризикам.

– ISO 31000 рекомендує використання постійного процесу оцінки ризиків, оскільки ситуації та умови можуть змінюватися. Постійне вдосконалення системи управління ризиками важливо для адаптації до нових умов.

– Управління ризиками ефективне лише в тому випадку, якщо воно є спільним зусиллям всіх учасників організації. Залучення керівництва та працівників на всіх рівнях є важливим елементом управління ризиками.

– Прозорість та ефективна комунікація стосовно ризиків є необхідним елементом. Стандарт рекомендує регулярне звітування та обмін інформацією для забезпечення взаєморозуміння між всіма сторонами.

Управління ризиками за стандартом ISO 31000 включає в себе кілька етапів, які сприяють системному та ефективному управлінню ризиками в організації.

Перший етап полягає в ретельному визначенні контексту, в якому працює організація. Це включає в себе розгляд зовнішнього та внутрішнього середовища, визначення цілей та ідентифікацію зацікавлених сторін.

На другому етапі проводиться оцінка ризиків. Це включає в себе ідентифікацію потенційних загроз та визначення вразливостей, що можуть вплинути на досягнення цілей. Для кожного ризику визначається його імовірність та можливі наслідки.

Принцип постійної оцінки ризиків передбачає, що цей процес повинен бути постійним. Оскільки умови можуть змінюватися, необхідно регулярно проаналізовувати ризики та адаптувати стратегії управління.

Виконується розробка сценаріїв управління ризиками. На цьому етапі розробляються конкретні сценарії управління ризиками для кожного ідентифікованого ризику. Визначаються конкретні заходи та стратегії, які дозволять зменшити імовірність виникнення ризику чи пом'якшити його наслідки.

Наступний етап обробки ризиків. На цьому етапі обираються методи обробки ризиків. Це може включати у себе уникнення ризиків, їх прийняття, зменшення, передачу чи взяття на себе.

Прозора звітність та ефективна комунікація щодо ризиків є ключовим елементом процесу. Організація повинна регулярно звітувати про результати оцінки ризиків та спілкуватися із зацікавленими сторонами.

Останній етап включає в себе постійне вдосконалення системи управління ризиками. Це вимагає аналізу результатів, виявлення слабких місць та вдосконалення стратегій для максимальної ефективності.

Спроектований процес управління ризиками за ISO 31000 надає організаціям системний та адаптивний підхід до управління потенційними загрозами та забезпечує стабільність та стійкість в умовах невизначеності.

До переваг стандарту можна віднести:

– Стандарт може бути використаний в будь-якій галузі та типі організації.

– Легко інтегрується з існуючими системами управління.

– Допомагає створити довіру серед стейкхолдерів шляхом ефективного управління ризиками.

Також варто зазначити наступні недоліки:

– Загальність. Завдяки своїм загальним принципам, стандарт може вимагати додаткових конкретизацій для адаптації до конкретного контексту.

– Суб'єктивність. Процеси, які вимагають суб'єктивної оцінки ризиків, можуть варіюватися залежно від сприйняття та досвіду керівників.

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Стандарт ISO/IEC 27005 виник в контексті широкого інтересу до проблем інформаційної безпеки, який з'явився на початку XXI століття. Зростання кількості цифрової інформації та її важливість для різних галузей стало супроводжуватися збільшенням загроз та ризиків для її конфіденційності, цілісності та доступності.

Перший варіант стандарту ISO/IEC 27005 був прийнятий в 2008 році з метою надання організаціям інструменту для систематичного виявлення та управління ризиками інформаційної безпеки. У той час стандарт фокусувався на визначенні загальних принципів та підходів до оцінки ризиків, не обмежуючись конкретними технічними деталями.

З роками, з урахуванням змін в інформаційному середовищі та досвіду використання стандарту, ISO/IEC 27005 був підданий кільком ревізіям. Вдосконалення стандарту дозволило враховувати сучасні технології, змінювані загрози та вдосконалення методик управління ризиками.

У 2020 році опубліковано останню версію стандарту ISO/IEC 27005, яка враховує найновіші вимоги та рекомендації у сфері інформаційної безпеки. Його розвиток продовжується відповідно до змін в технологічному та інформаційному ландшафті, надаючи організаціям засоби для ефективного управління ризиками та захисту їхніх інформаційних активів.

Стандарт ISO/IEC 27005 визначає принципи управління ризиками інформаційної безпеки, які є фундаментом для впровадження ефективної системи управління ризиками. Основні принципи включають системний підхід та контекст організації, спрямованість на запобігання та зменшення ризиків, узгодженість та прозорість заходів, впровадження контрольованих змін, врахування змін в оточенні, та взаємодію зі стейкхолдерами.

Системний підхід вимагає, щоб оцінка ризиків була частиною загальної системи управління інформаційною безпекою. Контекст організації підкреслює необхідність враховувати унікальний характер та особливості конкретної організації.

Принципи, спрямовані на запобігання та зменшення ризиків, передбачають вжиття заходів для попередження виникнення ризиків та мінімізації їх впливу. Узгодженість та прозорість заходів включає взаємодію з усіма сторінками та забезпечення доступності і зрозумілості інформації щодо ризиків.

Взаємодія з зацікавленими сторонами визначається діалогом та співпрацею для ефективного обміну інформацією та спільного вирішення ризиків. Ці принципи становлять невід'ємну основу для розробки та впровадження системи управління ризиками інформаційної безпеки в організації.

Процес управління ризиками за стандартом ISO/IEC 27005 полягає у систематичному та стратегічному керуванні потенційними загрозами інформаційній безпеці.

Під час визначення контексту, аналізуючи організаційне оточення, враховуються стратегічні цілі та існуючі процеси, які можуть вплинути на безпеку інформації.

Після ідентифікації ризиків проводиться комплексний аналіз загроз, вразливостей та можливих втрат інформації, враховуючи різноманітні аспекти діяльності організації.

Оцінка ризиків визначає ймовірність виникнення загроз та їх вплив на інформаційну безпеку, використовуючи різні методи оцінки – якісні чи кількісні моделі.

На основі отриманих результатів формується стратегія управління ризиками, спрямована на зниження впливу виявлених ризиків та підвищення загального рівня безпеки інформації.

Реалізація заходів управління ризиками включає впровадження конкретних заходів та контролів з метою забезпечення безпеки інформації та зменшення можливих загроз.

Завершальним етапом є постійний моніторинг та аудит системи управління ризиками для забезпечення ефективності вжитих заходів та постійного вдосконалення.

Процес управління ризиками за ISO/IEC 27005 сприяє створенню ефективної системи інформаційної безпеки, адаптованої до змін і викликів сучасного інформаційного середовища.

Загальний висновок є те, що ISO/IEC 27005:2011 є важливим інструментом для сучасних організацій у формуванні стійких та надійних стратегій управління ризиками в умовах швидко змінюючогося цифрового ландшафту. Даний стандарт грає важливу роль у забезпеченні ефективного управління ризиками інформаційної безпеки.

NIST Special Publication (SP) 800-30. Стандарт NIST Special Publication (SP) 800-30, розробленим Національним інститутом стандартів і технологій США (NIST), щодо забезпечення ефективного управління ризиками в інформаційній безпеці. Початково розроблений для задоволення потреб у сфері федеральних установ, стандарт відтоді отримав широкий розповсюдження в різних галузях та країнах.

Історія стандарту розпочалася у середині 1990-х років, коли зростання комп'ютеризації та використання інформаційних систем стало визначальним для численних секторів. У зусиллях забезпечити стійкість інформаційних ресурсів, NIST визначив потребу в системному підході до оцінки та управління ризиками.

Спочатку спрямований на задоволення потреб федерального сектору, стандарт швидко став об'єктом зацікавлення галузей приватного сектору, де висока залежність від інформаційних технологій також вимагала ефективного управління ризиками. З часом NIST SP 800-30 став загальновизнаним стандартом, що надає конкретні методи та процедури для проведення оцінки ризиків.

Розвиток стандарту продовжується, відзначаючи внесення змін та оновлень відповідно до зростаючих викликів та змін у сфері інформаційної безпеки. Усе це сприяє удосконаленню та адаптації стандарту до сучасних вимог та тенденцій у сфері інформаційної безпеки.

В основі, NIST SP 800-30 ґрунтується на кількох ключових принципах, які визначають його сутність та ефективність у сфері управління ризиками. Принципи ці становлять важливий фундамент для оцінки та керування ризиками в інформаційній безпеці.

NIST SP 800-30 покладає основний акцент на інтегрованість та системний підхід до оцінки ризиків. Це означає врахування всіх компонентів системи та їх взаємодії для повноти та об'єктивності оцінки.

Стандарт визнає, що контекст та урахування особливостей конкретного середовища є ключовими факторами для точної оцінки ризиків. Підходить до кожного випадку індивідуально, забезпечуючи адаптованість до конкретних умов.

Ефективна оцінка ризиків вимагає співпраці та залучення всіх зацікавлених сторін. NIST SP 800-30 стимулює активну участь усіх стейкхолдерів для отримання повноцінної інформації.

Стандарт визнає змінливість умов та динаміку загроз, тому він побудований з урахуванням гнучкості та здатності адаптуватися до нових сценаріїв ризиків у реальному часі.

Ці принципи, злагоджені між собою, формують основу для ефективного управління ризиками в інформаційній безпеці згідно зі стандартом NIST SP 800-30. [31]

ISACA Risk Framework. ISACA Risk Framework є ключовим інструментом для управління ризиками в інформаційній безпеці та виник у контексті зростаючої потреби в ефективному керуванні загрозами та вразливостями в організаційних інформаційних системах.

ISACA (Information Systems Audit and Control Association) виникла в 1969 році, висловивши турботу професіоналів із системного аудиту та контролю. Протягом часу, зі зростанням ролі технологій, організація розширила свою діяльність, включаючи аспекти управління ризиками в інформаційній безпеці.

Перші кроки у створенні ISACA Risk Framework були здійснені відповідно до зростаючого впливу технологічних ризиків та загроз інформаційній безпеці. Фреймворк спрямований на надання організаціям інструменту для оцінки та керування ризиками, пов'язаними з використанням технологій та обробкою інформації.

З розвитком технологій та появою нових загроз фреймворк ISACA вдосконалювався. Він адаптувався до змін у кіберпросторі, враховуючи еволюцію атак, ризиків та вимог до інформаційної безпеки.

Сучасний ISACA Risk Framework висвітлює актуальні виклики в галузі інформаційної безпеки, такі як кіберзагрози, соціальна інженерія та вимоги до дотримання регуляторних стандартів. Він став необхідним інструментом для комплексного управління ризиками та забезпечення стійкості організаційних інформаційних систем у сучасному цифровому середовищі.

Історія та розвиток ISACA Risk Framework свідчать про постійне вдосконалення та адаптацію до зростаючих викликів у сфері інформаційної безпеки, роблячи його важливим інструментом для сучасних організацій.

Вибачте за непорозуміння. Давайте розглянемо процес управління ризиками за ISACA Risk Framework, використовуючи менше пунктів для суцільного тексту.

Процес управління ризиками в рамках ISACA Risk Framework є ключовим компонентом ефективного корпоративного управління. Однією з основних особливостей цього підходу є інтеграція управлінських принципів з інформаційною безпекою.

Початковим етапом є ідентифікація ризиків, включаючи загрози та вразливості в інформаційному середовищі.

Після ідентифікації ризиків проводиться їх оцінка з урахуванням ймовірності та можливих втрат для організації.

Далі в процесі управління ризиками важливим є розробка та впровадження стратегій мінімізації ризиків, включаючи заходи безпеки та вдосконалення бізнес-процесів.

Ключовим завданням є постійне вдосконалення системи управління ризиками, враховуючи зміни в бізнес-середовищі та результати попередніх оцінок ризиків.

Отже, процес управління ризиками за ISACA Risk Framework є цільовим та поетапним підходом до забезпечення сталої інформаційної безпеки в організації.

COSO Enterprise Risk Management. Стандарт COSO ERM започаткувався в 2004 році, коли Committee of Sponsoring Organizations of the Treadway Commission (COSO) представив свою першу версію управлінських рамок для ефективного внутрішнього контролю.

У 2007 році COSO оновив свої рамки, вводячи поняття управління ризиками. Це визначило новий етап у розвитку COSO ERM, орієнтований на інтеграцію процесів управління ризиками в загальні стратегічні зусилля підприємств.

Останнє значуще оновлення COSO ERM відбулося в 2017 році. Новий документ, під назвою "Enterprise Risk Management – Integrating with Strategy and Performance" (Управління Ризиками - Інтеграція зі Стратегією та Результативністю), враховує зміни в бізнес-середовищі та пропонує підходи до вдосконалення управління ризиками.

Сучасний розвиток COSO ERM віддзеркалює відповідь на глобальні виклики, такі як кібербезпека, економічна нестабільність та зростаюча складність бізнес-процесів. COSO продовжує вдосконалювати свої рамки, щоб забезпечити їхню актуальність у сучасному світі. Історія розвитку COSO ERM свідчить про постійну адаптацію до змін у середовищі та визначає його ключові кроки у напрямку покращення управління ризиками.

Основні принципи COSO Enterprise Risk Management (ERM) є керівними засадами, які спрямовані на вдосконалення управління ризиками в організації та досягнення стратегічних цілей. Ці принципи визначають рамки для впровадження ефективного процесу управління ризиками та інтеграції його в загальний стратегічний контекст підприємства.

1. Підтримка створення цінності: Організація повинна спрямовувати свої зусилля на створення, збереження та підвищення цінності для всіх зацікавлених сторін.

2. Визначення стратегії: Передбачення ризиків та можливостей повинно бути вбудоване в процес визначення та формулювання стратегії підприємства.

3. Забезпечення всебічного огляду: Впровадження ефективного управління ризиками повинно відбуватися в межах всієї організації та включати всі рівні керівництва.

4. Визначення різноманітності інтересів сторін: Важливо розуміти та враховувати інтереси різних зацікавлених сторін під час управління ризиками.

5. Визначення внутрішнього середовища: Розгляд внутрішнього середовища дозволяє ідентифікувати та оцінювати внутрішні фактори, що впливають на досягнення цілей.

6. Оцінка ризиків: Ефективний процес оцінки ризиків визначає ідентифікацію, оцінку та реагування на ризики, що впливають на досягнення цілей.

7. Визначення зрозумілих інформаційних та комунікаційних структур: Забезпечення ефективної обміну інформацією та сприяння внутрішньому контролю.

8. Забезпечення відповідальності керівництва: Керівництво повинно приймати на себе відповідальність за ефективне управління ризиками та досягнення цілей підприємства.

Ці принципи COSO ERM визначають ключові напрями для впровадження та підтримки ефективного управління ризиками в організації. [12-13,34]

MEHARI. MEHARI (Методологія Оцінки та Управління Ризиками) є фреймворком, розробленим французьким інститутом CLUSIF (Club de la Sécurité de l'Information Français) для комплексної оцінки та управління інформаційними ризиками в організаціях. Розпочавши свій шлях у 1990 році, MEHARI став визнаним методологічним інструментом в галузі управління інформаційною безпекою.

MEHARI враховує специфіку кожної організації, визначаючи її структуру та особливості як важливі фактори впливу на інформаційні ризики. Оцінка та

класифікація інформаційних активів, а також оцінка їхньої важливості для бізнесу, є ключовим етапом в роботі фреймворку.

Загрози та вразливості ідентифікуються та оцінюються MEHARI з урахуванням можливих наслідків. Визначення ризиків базується на ймовірності та важливості наслідків, враховуючи при цьому рівень прийнятності ризиків.

MEHARI також враховує сценарії ризиків для конкретизації ситуацій та їхньої реалізації, а його інструменти дозволяють ефективно управляти та знижувати ризики. Методологія передбачає систему моніторингу ризиків та оновлення стратегій управління для підтримки сталої інформаційної безпеки в організаціях. MEHARI є важливим інструментом для компаній, які прагнуть ефективно управляти інформаційними ризиками та забезпечувати сталу безпеку в цифровому середовищі. [8-10]

OWASP Risk Rating Methodology. OWASP Risk Rating Methodology – це методологія оцінки ризиків, розроблена Відкритим проєктом з безпеки вебзастосунків (Open Web Application Security Project). Основна ідея полягає в наданні структурованого підходу до визначення ймовірності та впливу можливих загроз, а також визначенні загального рівня ризику. [4]

Методологія враховує різні аспекти безпеки веб-додатків, такі як існуючі вразливості, потенційні загрози та можливі наслідки. Процес включає в себе оцінку ймовірності виникнення загрози та визначення можливих наслідків у вигляді впливу на конфіденційність, цілісність та доступність.

Оцінка ймовірності базується на різних факторах [5-7,11,25-28], таких як складність атаки, наявність вразливостей та рівень мотивації атакувальника. Оцінка впливу базується на визначені технічних та бізнес наслідків. До технічних відноситься втрата конфіденційності, цілісності та доступності та можливості ідентифікувати користувача. Оцінка бізнес наслідків проводиться використовуючи фактори як фінансові, репутаційні втрати, невиконання законодавста та розголошення персональної інформації.

Після визначення ймовірності та впливу, застосовується спеціальна шкала для призначення кінцевого рівня ризику. Цей рівень може вказати, наскільки

критичним є конкретний ризик і які заходи слід прийняти для його управління. OWASP Risk Rating Methodology надає командам розробників та безпеки структурований інструмент для оцінки та пріоритизації ризиків, пов'язаних з веб-додатками.

2.2 Висновки та обгрунтування обраного напряму

Для проведення оцінки був обраний ISACA Risk Framework з кількох ключових причин:

– Фреймворк спрощує інтеграцію процесів управління ризиками у загальний корпоративний управлінський процес та взаємодіє з ключовими аспектами корпоративного управління.

– ISACA Risk Framework ставить акцент на розумінні взаємозв'язків між ризиками та бізнес-цілями, що дозволяє вирішувати проблеми, які можуть виникнути в контексті конкретної діяльності організації.

– Враховуючи рекомендації і вимоги стандартів та регуляторів, ISACA Risk Framework сприяє відповідності організації до необхідних нормативних актів.

– Фреймворк допомагає уникнути суб'єктивності управлінських оцінок та сприяє об'єктивності в процесі управління ризиками.

– Розробником ISACA Risk Framework є ISACA, авторитетна міжнародна організація, що спеціалізується на області управління IT та інформаційної безпеки, що надає вагому стандарту відомості та досвіду.

3 ПРИКЛАД ОЦІНКИ РИЗИКІВ

3.1 Процес проведення оцінки ризиків

Оцінка ризиків полягає у визначенні ризиків, які є характерними для конкретного середовища, і визначенні рівня виявлених ризиків. Основні етапи оцінки ризиків (рисунок 3.1) - ідентифікація ризиків, аналіз ризиків та визначення заходів протидії ризикам.

Рисунок 3.1 - Процес проведення оцінки ризиків

3.2 Визначення області та рамки оцінки ризиків

Визначення області та рамок оцінки ризиків є стратегічно важливим етапом для ретельного аналізу та управління потенційними небезпеками. У контексті даного аналізу, акцент розміщується виключно на кіберзагрозах та ризиках, пов'язаних із використанням інформаційно-технологічних систем.

Обмеження області оцінки до кіберзагроз та IT-ризиків визначає параметри, які будуть враховуватися під час аналізу. Це включає в себе загрози для інформаційної безпеки, можливі атаки на системи, витоки конфіденційної інформації та інші аспекти, пов'язані із цифровою інфраструктурою.

Такий деталізований підхід допомагає точно скерувати увагу на конкретні аспекти кібербезпеки та інформаційно-технічних ризиків, що робить аналіз більш точним та ефективним у контексті визначених параметрів.

3.3 Вибір моделі оцінки ризиків

Обравши модель оцінки ризиків "Оцінка сценаріїв" на основі Risk IT Framework та керуючись руководством Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure, було здійснено обґрунтований та стратегічно обдуманий вибір для проведення аналізу потенційних загроз та визначення ризиків.

Модель "Оцінка сценаріїв" надає можливість ретельно вивчити та визначити можливі становища та події, які можуть впливати на організацію. Цей підхід дозволяє уникнути загальних або стандартних підходів, а замість цього, фокусується на унікальних сценаріях, які конкретним чином можуть впливати на інформаційну безпеку та технічні аспекти.

Risk IT Framework [1] допомагає структурувати цей вибір, надаючи фреймворк, що враховує ключові аспекти ризик-менеджменту та визначає елементи, які важливі для організації. Вибір даної моделі віддзеркалює стратегічний підхід до оцінки ризиків, забезпечуючи глибокий і адаптований підхід до аналізу сценаріїв у контексті конкретних умов та потреб організації.

Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure [25] надає рекомендації по вибору критеріїв оцінки для критичної інфраструктури, а також зазаначає розмір матриці ризиків.

Такий вибір є кроком у напрямку ефективного управління ризиками, де аналіз сценаріїв дозволяє глибше розуміти унікальні аспекти та потенційні виклики, з якими може стикатися організація в галузі кібербезпеки та IT.

3.4 Вибір критеріїв оцінки

Визначення ризику. Різні стандарти трактують інформаційні та кібер ризики дещо по різному. Таким чином, перед тим як докладніше досліджувати

процес оцінки ризиків, важливо встановити загальне визначення кібер-ризику. У цьому дослідженні ризик визначається як функція (рисунок 3.2):

– Ймовірності виникнення певної загрози, яка впливає на вразливість активу; та

– Наслідків виникнення загрози.

Рисунок 3.2 - Визначення ризику

Визначення толерантність до ризиків. Джерела, такі як ISACA Risk IT Framework [1] та Risk Appetite — Critical to Success [34] визначають допустимий рівень ризику як "припустимий рівень відхилення, який керівництво готове допустити для будь-якого конкретного ризику підприємства, з метою реалізії своїх цілей", та використовують термін "апетит до ризику" для посилання на "кількість ризику, на загальному рівні, яку суб'єкт готовий прийняти для досягнення своєї місії". У цьому документі не робиться різниці між допустимим рівнем ризику та апетитом до ризику, оскільки ми розглядаємо їх обидва як схожі поняття (тобто, скільки ризику організація готова прийняти).

Чітко визначені рівні ризику повинні формулювати:

– Очікування щодо обробки та зменшення та конкретних типів ризику

– Межі та пороги прийнятного ризику

В Таблиця 3.1 наведено визначення рівнів ризику для даної роботи. На основі якої буде побудовано карти ризиків. Це дасть змогу менеджменту проаналізувати ризики та обрати необхідні заходи відповідно до їх можливого негативного впливу на системи підприємства.

3.5 Ідентифікація загроз та складання сценаріїв

Для ідентицікації ризиків складемо реєстр ризиків згідно прикладу (рисунок 3.3) із стандарту NISTIR 8286B. Червоним прямокутником відзначено колонки які необхідно заповнити для виконання аналізу [7].

Таблиця 3.1 - Рівні ризику

Рівні ризику	Опис рівня
Дуже сильний	Рівень ризику який не можна прийняти, і він спричинить настільки сильний вплив, що пов'язану з ним діяльність необхідно буде негайно припинити. В якості альтернативи необхідно негайно вжити стратегії пом'якшення або перенесення.
Сильний	Такий рівень ризику не можна прийняти. Стратегії спрямовані на зниження рівня ризику, повинні бути розроблені та впроваджені протягом наступного 1 місяця.
Помірний	Такий рівень ризику не можна прийняти. Стратегії спрямовані на зниження рівня ризику, повинні бути розроблені та впроваджені протягом наступних 3-6 місяців.
Другорядний	Цей рівень ризику можна прийняти, якщо немає стратегій зниження ризику, які можна було б легко та економічно реалізувати. Необхідно регулярно контролювати ризик, щоб переконатися, що будь-яка зміна його виявлена та вжито необхідних заходів.
Незначний	Цей рівень ризику можна прийняти, якщо немає стратегій зниження ризику, які можна було б легко та економічно реалізувати. Необхідно періодично контролювати ризик, щоб переконатися, що будь-яка зміна виявлена та вжито необхідних заходів.

Рисунок 3.3 - Шаблон реєстра кібер-ризиків

Реєстр ризиків надає легко зрозумілий передік для аналізу та дослідження ризиків, а також додаткову важливу інформацію як наприклад відповідального за конкретний ризик. Проте ефективна комунікація ризиків вимагає багато додаткових деталей, які не помістяться в цю компактну таблицю.

Таблиця 3.2 - Реєстр ризиків

ID	Опис ризика
R01	Зловмисник виконав атаку за допомогою SQL ін’єкції на застарілий web-додаток та завантажив конфіденційні дані.
R02	В результаті фішингової атаки, зловмисник отримав доступ до корпоративного облікового запису співробітника та використав його для завантаження конфіденційної інформації.
R03	Неуповноважений працівник отримав доступ до мережевого обладнання використовуючи логін та пароль по замовченню та виконав команди для скидання на заводські налаштування.
R04	Невдоволений працівник може завдати компанії значних збитків через саботаж та розголошення конфіденційних даних.
R05	У співробітника викрали ноутбук дані на якому містились фінансові звіти та сберігались у незашифрованому вигляді, копії цих даних на інших носіях відсутні.
R06	Зловмисники виконують DDoS атаку на систему, роблячи її недоступною та призводячи до переривання роботи.
R07	Компрометація веб-додатка за допомогою перебору паролів або використання коду з метою створення простою бізнеса чи витоку даних.
R08	Неправильна конфігурація, нездатність поновити сертифікати, термін дії яких закінчився, неправильна публікація та інші помилки співробітників, які призвели до недоступності сервісів.
R09	Атака з використанням ransomware, призначена для тиску на компанію, щоб вона сплатила викуп, шляхом шифрування та припинення доступу до систем або файлів.
R10	Сбій в роботі провайдера, що призвів до часткової або повної втрати доступу до IT системи на 2-4 години

3.6 Аналіз ризиків

Аналіз ризиків полягає у вивченні елементів, які становлять кожен сценарій ризику для визначення:

– ймовірності виникнення сценарію ризику; та

– наслідків (тобто масштабу збитків), які виникають внаслідок виникнення сценарію ризику.

Визначення вирогідності. Традиційно використовувалася історична чи очікувана подія як метрика для вимірювання ймовірності ризику (наприклад, очікується, що подія відбудеться один раз на рік або трапилася один раз протягом минулого року). Однак використання такої метрики для вимірювання ймовірності кібербезпекових ризиків може бути несприятливим через динамічну природу кіберзагроз. Те, що система раніше не була скомпрометована, не означає, що це не може трапитися у майбутньому.

Загальною рекомендацією є оцінка ймовірності кібер ризиків з точки зору загроз та вразливостей. Один із методів визначення ймовірності кібер ризиків полягає у врахуванні таких факторів:

– Виявленість (Discoverability) - Наскільки легко ворог може виявити вразливість активу? Це залежить від доступності інформації щодо вразливості та експозиції вразливого активу.

– Можливість застосування (Exploitability) - Наскільки легко ворог може використовувати вразливість активу? Це залежить від прав доступу, складності інструментів, а також технічних навичок, необхідних для здійснення атаки.

– Відтворюваність (Reproducibility) - Наскільки легко зловмисник може відтворити атаку на актив? Це залежить від складності налаштування експлойту та умов середовища, необхідних для виконання атаки.

Таблиця 3 приводить критерії оцінок за якими буде визначатись ймовірності ризику кіберзагрози на основі описаних факторів. Для отримання ймовірності сценарію ризику будуть виконані наступні кроки:

– Надана оцінка для кожного з 3 факторів ймовірності (тобто 1-5).

– Знайдена середня оцінку та округлена до найближчого цілого числа.

– Остаточна оцінка буде ймовірністю ризикового сценарію; 5 - "Дуже ймовірно" та 1 - "Рідко".

Таблиця 3.3 - Таблиця для оцінки вирогідності ризику

Рейтинг вірогідності	**Виявленість**	**Можливість застосування**	**Відтворюваність**
Дуже ймовірно (5)	Уразливість цілі: • можна виявити шляхом пошуку/сканування опублікованої інформації у відкритому доступі (наприклад, Shodan, ExploitDB); • можуть бути виявлені та атаковані із зовнішніх мереж (включаючи Інтернет)	Атака(у): • може виконуватися без прав доступу цілі; • можна виконувати за допомогою загальнодоступних інструментів без технічних знань	Атаку: • можна повторювати за бажанням без будь-яких конкретних умов (конфігурація чи подія); • можна повторювати за бажанням без будь-яких налаштувань опублікованих експлойтів
Ймовірно (4)	Вразливість цілі: • може бути виявлений зондування цілі (наприклад, сканування портів); • можуть бути виявлені і використано з сусіднього підмережі або іншого мережого сегменту	Атаку: • можна виконувати з обмеженими правами доступу (наприклад, користувач); • можна виконати з загальнодоступними інструментами з загальними технічними знання	Атака(у): • може бути повторена за певної конфігурації в цілі; • можна повторити з мінімальними налаштуваннями опублікованих експлойтів (наприклад, зміна параметрів)
Можливо (3)	Уразливість цілі: • можна виявити шляхом вивчення відповідей, поведінки та комунікацій цільового пристрою (наприклад, змішування мережевих пакетів, мережевий аналіз);	Атака: • може бути виконано з привілейованими правами доступу цілі (наприклад, admin/SYSTEM/root); • можна виконувати за	Атака: • може повторюватись за умови певної передбачуваної події; • можна повторити з індивідуальними налаштуваннями для цілі

	• можуть бути виявлені та атаковані з тієї самої підмережі чи сегмента мережі	допомогою загальнодоступних інструментів, що вимагає помірних технічних знань	
Малоймовірно (2)	Уразливість цілі: • можуть бути виявлені шляхом роботи та взаємодії з фактичною або подібною установкою цілі; • можна виявити та атакувати за допомогою логічного локального доступу	Атака: • можна виконувати з привілейованими правами доступу (наприклад, admin/SYSTEM/root); • можна виконувати за допомогою загальнодоступних/спеціалізованих інструментів, які вимагають передових технічних знань; • може знадобитися ланцюжок кількох експлойтів	Атака: • може повторюватись за умови певної випадкової події; • можна повторити теоретично або з опублікованим доказом використання концепції
Рідко (1)	Уразливість цілі: • можна виявити, вивчивши проект (наприклад, вихідний код); • можуть бути виявлені та атаковані за допомогою фізичного доступу	Атака: • можна виконувати з привілейованими правами доступу (наприклад, admin/root/SYSTEM) і необхідною багатофакторною автентифікацією;	Атака: • не можна відтворити на мішені; • можна повторити з неопублікованим експлойтом, специфічним для цілі

		• можна виконувати за допомогою спеціалізованих інструментів, що вимагає експертних технічних знань; • вимагає ланцюжка кількох експлойтів	

Визначення впливу. Загальною рекомендацією є оцінка ймовірності кібер-ризиків з точки зору загроз та вразливостей. Один із методів визначення ймовірності кібер-ризиків полягає у врахуванні таких факторів.

Загалом, проявлення сценарію ризику може піддавати компрометації конфіденційність, цілісність та/або доступність активів (наприклад, даних, обладнання, операцій). В таблиці 3 наведена таблиця оцінки для визначення впливу ризику на шкалі від 1 до 5 (5 - "Дуже сильний", 1 - "Нечначний"). Кожен ризиковий сценарій може мати різні рейтинги впливу на конфіденційність, цілісність та доступність.

В даній роботі оцінюється найвищий рейтинг впливу, який вважається остаточним балом.

Таблиця 3.4 - Таблиця для оцінки впливу ризику

Рейтинг впливу	**Конфіденційність**	**Цілісність**	**Доступність**
Дуже сильний (5)	Несанкціоноване розголошення інформації матиме надзвичайно серйозні негативні наслідки для організації.	Несанкціонована модифікація або знищення інформації матиме надзвичайно серйозні негативні наслідки для організації.	Переривання доступу до інформації чи комп'ютерної системи або використання інформації чи комп'ютерної системи матиме надзвичайно серйозні негативні наслідки для організації.
Сильний (4)	Несанкціоноване розголошення інформації матиме серйозний негативний вплив на організацію.	Несанкціоноване модифікація або знищення інформації матиме серйозний негативний вплив на організацію.	Переривання доступу до інформації чи комп'ютерної системи матиме серйозний негативний вплив на організацію.
Помірний (3)	Несанкціоноване розголошення інформації матиме певний негативний вплив на організацію.	Несанкціоноване модифікація або знищення інформації матиме певний негативний вплив на організацію.	Переривання доступу до інформації чи комп'ютерної системи матиме певний негативний вплив на організацію.
Другорядний (2)	Несанкціоноване розкриття інформації матиме обмежений негативний вплив на організацію.	Несанкціоноване модифікація або знищення інформації матиме обмежений негативний вплив на організацію.	Переривання доступу до інформації чи комп'ютерної системи матиме обмежений негативний вплив на організацію.
Незначний (1)	Несанкціоноване розкриття інформації матиме незначний вплив	Несанкціоноване модифікація або знищення інформації матиме	Переривання доступу до інформації чи комп'ютерної системи матиме незначний вплив

	на організацію чи окремих осіб.	незначний вплив на організацію чи окремих осіб.	на організацію чи окремих осіб.

Складання карти ризиків.

Як зазначено в розділі 3.3 Визначення ризиків, ризик - це функція ймовірності виникнення певної загрози, яка використовує потенційну вразливість активу, і наслідків, які від цього виникають. Це може бути представлено діаграмно за допомогою матриці ризиків. В таблиці 5 нижче наведена матриця ризиків 5 на 5 для визначення рівня ризику для кожного ризикового сценарію, де рівень ризику є множенням "Ймовірності" і "Впливу", визначених на етапі аналізу ризиків. [30]

Таблиця 3.5 - Матриця ризиків 5-на-5 для визначення рівня

Дуже сильний (5)	Середній (5)	Значний (10)	Високий (15)	Неприйнятний (20)	Неприйнятний (25)
Сильний (4)	Низький (4)	Середній (8)	Значний (12)	Високий (16)	Неприйнятний (20)
Помірний (3)	Низький (3)	Середній (6)	Середній (9)	Значний (12)	Високий (15)
Другорядний (2)	Низький (2)	Низький (4)	Середній (6)	Середній (8)	Значний (10)
Незначний (1)	Низький (1)	Низький (2)	Низький (3)	Низький (4)	Середній (5)
	Рідкісний (1)	**Малоймовірно (2)**	**Можливо (3)**	**Ймовірно (4)**	**Дуже ймовірно (5)**

Для кожного отриманого рівня ризику буде проведено порівняння його із рівнем терпимості до ризику, визначеним організацією. Ризикові сценарії з рівнями ризику вище рівня терпимості повинні бути пріоритетними для обробки, поки рівні ризику не зменшаться до рівня терпимості. При визначенні пріоритету ризику також важливо встановити очікуваний строк.

3.7 Результати оцінки ризиків

Для автоматизації обчислення оцінок створемо Google таблицю зі всіма необхідними колонками (рисунок 3.4).

ID	Опис ризика	Рейтинг вірогідності			Оцінка вірогідності	Рейтинг впливу			Оцінка впливу	Загальна оцінка
		Виявленість	Мож. застосування	Відтворюваність		Конфіденційність	Цілісність	Доступність		
R01	Зловмисник виконав атаку за допомогою SQL ін'єкції на застарілий web-додаток та завантажив конфіденційні дані.	1	2	1	1	1	2	1	2	2
R02	В результаті фішингової атаки, зловмисник отримав доступ до корпоративного облікового запису співробітника та використав його для завантаження конфіденційної інформації.									
R03	Неуповноважений працівник отримав доступ до мережевого обладнання використовуючи логін та									

Рисунок 3.4 - Оцінка реєстру ризиків

Для оцінки вирогідності спочатку знайдемо середнє значення, потім заокруглимо до найближчого цілого числа. Для цього використаємо формулу приведену на рисунку 3.5.

```
=ROUND(AVERAGE(C3:E3); 0)
```

Рисунок 3.5 - Формула обчислення ймовірності

Для оцінки впливу, необхідно визначити критерій з максимальною оцінкою. Для цього використаємо формулу наведену на рисунку 3.6

```
=MAX(G3:I3)
```

Рисунок 3.6 - Формула обчислення впливу

Для розрахунку загальної оцінки ризика використаємо формулу множення Впливу на Ймовірність (рисунок 3.7).

```
=F3*J3
```

Рисунок 3.7 - Формула обчислення загальної оцінки

Виконавши підготовчі дії, заповнимо таблицю ризиками та проставимо оцінки згідно критеріїв визначених обраною моделлю оцінки ризиків.

Таблиця 3.6 - Реєстр ризиків з оцінками

ID	Опис ризика	Критерії вірогідності			Вірогідності	Критерії впливу			Вплив	Загальна оцінка
		Виявленість	Можл. застосування	Відтворюваність		Конфіденційність	Цілісність	Доступність		
R01	Зловмисник виконав атаку за допомогою SQL ін’єкції на застарілий web-додаток та завантажив конфіденційні дані.	5	5	3	4	4	1	1	4	16
R02	В результаті фішингової атаки, зловмисник отримав доступ до корпоративного облікового запису співробітника та використав його для завантаження конфіденційної інформації.	5	5	3	4	4	1	1	4	16
R03	Неуповноважений працівник отримав доступ до мережевого обладнання використовуючи логін та пароль по замовченню та виконав команди для скидання на заводські налаштування.	4	4	4	4	1	1	1	1	4
R04	Невдоволений працівник може завдати компанії значних збитків через саботаж та розголошення конфіденційних даних.	5	1	3	3	5	1	1	5	15

R05	У співробітника викрали ноутбук дані на якому містились фінансові звіти та сберігались у незашифрованому вигляді, копії цих даних на інших носіях відсутні.	1	1	2	1	5	5	5	5	5
R06	Зловмисники виконують DDoS атаку на систему, роблячи її недоступною та призводячи до переривання роботи.	4	5	2	4	1	1	5	5	20
R07	Компрометація веб-додатка за допомогою перебору паролів або використання коду з метою створення простою бізнеса чи витоку даних.	2	4	4	3	3	1	4	4	12
R08	Неправильна конфігурація, нездатність поновити сертифікати, термін дії яких закінчився, неправильна публікація та інші помилки співробітників, які призвели до недоступності сервісів.	3	1	2	2	1	1	2	2	4
R09	Атака з використанням ransomware, призначена для тиску на компанію, щоб вона сплатила викуп, шляхом шифрування та припинення доступу до систем або файлів.	2	2	1	2	1	5	5	5	10

R10	Сбій в роботі провайдера, що призвів до часткової або повної втрати доступу до IT системи на 2-4 години	1	1	2	1	1	1	3	3	3

В результаті отриманої таблиці 3.6 можна зробити висновки про найбільші загрози та підготувати заходи для зниження ризиків. Для більш інформативності та візуального розуміння ризикового середовища побудуємо карту ризиків, яка відображена в таблиці 3.7 [30].

Таблиця 3.7 - Карта ризиків з оцінками

Дуже сильний (5)	R05	R09	R04	R06	
Сильний (4)			R07	R01, R02	
Помірний (3)	R10				
Другорядний (2)		R03, R08			
Незначний (1)					
	Рідкісний (1)	**Малоймовірно (2)**	**Можливо (3)**	**Ймовірно (4)**	**Дуже ймовірно (5)**

3.8 Ескалація та звітність про ризики

Ескалація та звітність щодо ризиків є важливою частиною ефективного управління ризиками в організації. Цей процес визначає, які заходи слід приймати, якщо ризики досягають певного рівня, та визначає, як повідомляти про ці ризики. Таблиця ескалації і звітності допомагає визначити, кому необхідно повідомити про ризики і хто має владу приймати рішення щодо їхнього прийняття чи управління. Це сприяє забезпеченню ефективності процесів управління ризиками та забезпечує своєчасні та вірогідні втручання для запобігання негативним наслідкам.

У таблиці 3.8 наведено ескалації та звітності про ризики. Вона визначає, хто повинен бути поінформований та має повноваження приймати ризик на основі його впливу.

Таблиця 3.8 - Ескалація та звітність про ризики

	Ескалація та звітність для кожного рівня ризиків
Неприйнятний	Рада правління
Високий	Директор
Значний	Вище керівництво та дериктори напрямків
Середній	Седеній менеджмент
Низький	Вахівці на місцях

Використовуючи картку ризиків наведену в таблиці 3.7 маємо змогу ескалювати та своєчасно сповіщати про всі зміни та вжиті заходи на відповідному рівні менеджменту згідно таблиці 3.8.

ВИСНОВОК

У кваліфікаційній роботі було розглянуто та детально проаналізовано методологію оцінки ризиків з метою підвищення рівня стійкості компанії до кіберзагроз. Процес оцінки ризиків включав декілька ключових аспектів, включаючи визначення області та рамок оцінки, вибір критеріїв, ідентифікацію загроз, а також розробку сценаріїв ризиків для об‘єктів критичної інфраструктури.

Перший аспект оцінки ризиків описує визначення області та рамок оцінки, що включає в себе вибір об‘єктів дослідження та встановлення меж оцінки ризиків.

Другий аспект стосується вибору моделі оцінки ризиків, включаючи підхід до оцінки ймовірності та впливу загроз. Цей аспект важливий для забезпечення точності та релевантності результатів оцінки.

Третій аспект оцінки ризиків включає в себе ідентифікацію та аналіз потенційних загроз для критичної інфраструктури, що дозволяє розробити ефективні стратегії зниження ризиків.

Четвертий аспект розглядає процес створення сценаріїв ризиків, які використовуються для аналізу можливих наслідків та розробки відповідних заходів реагування.

П’ятий аспект описує взаємодію цих елементів, спрямовану на створення цілісної та ефективної системи управління ризиками.

У цілому, усі ці аспекти роботи сприяють підвищенню рівня кібербезпеки та зміцненню стійкості компаній і організацій у відношенні до кіберзагроз, а також забезпечують надійний підхід до оцінки та управління ризиками в системах критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Risk IT Framework, 2nd Edition. ISBN 978-1-60420-820-7. ISACA, 2016.
2. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 [Електронний ресурс] / Sausalito, Calif. – 13.11.2020. – Режим доступу до ресурсу: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
3. The cost of incidents affecting CIIs. European Union Agency For Network And Information Security, 2016 – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/@@download/fullReport
4. OWASP Risk Rating Methodology – Режим доступу до ресурсу: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.
5. Risk Taxonomy (O-RT), Version 3.0.1. ISBN: 1-947754-66-9 – Режим доступу до ресурсу: https://pubs.opengroup.org/security/o-rt/#_Toc87862702
6. BSI-Standart 100-3. Risk analysis based on IT-Grundschutz. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008. – Режим доступу до ресурсу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf
7. NISTIR 8286A. Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. National Institute of Standards and Technology, 2021. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.IR.8286A
8. MEHARI 2010 - Overview. CLUSIF, 2010 – Режим доступу до ресурсу: https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-overview.pdf
9. MEHARI 2010 - Processing guide for risk analysis and management. CLUSIF, 2011 – Режим доступу до ресурсу: https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-processing-guide.pdf
10. MEHARI 2010 - Risk analysis and treatment guide. CLUSIF, 2010 – Режим доступу до ресурсу: https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-risk-analysis-and-treatment-guide.pdf

11. Conducting an IT Security Risk Assessment. ISACA Whitepaper, 2020.

12. Risk Assessment in Practice. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2021 – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-grc-coso-riskassessment-102312.pdf

13. Understanding and implementing Enterprise Risk Management. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), October 2020.

14. The Global Risks Report 2021, 16th Edition. World Economic Forum. Сторінка 11 – Режим доступу до ресурсу: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

15. An Emergency Management Framework for Canada Third Edition. ISBN: 978-0-660-07186-2. Emergency Management Policy and Outreach Directorate, 2017

16. CRS Report for Congress: RL32561. Risk Management and Critical Infrastructure Protection. Congressional Research Service, 2005 – Режим доступу до ресурсу: https://sgp.fas.org/crs/homesec/RL32561.pdf

17. Study on cyber security in the energy sector of the Energy Community. Blueprint Energy Solutions GmbH, 2019 – Режим доступу до ресурсу: https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

18. Security of Critical Infrastructure Act. The Office of Parliamentary Counsel, Canberra, 2018 – Режим доступу до ресурсу: https://www.legislation.gov.au/Details/C2022C00160

19. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

20. Critical Infrastructure Resilience Strategy. Cyber and Infrastructure Security Centre, February 2023 – Режим доступу до ресурсу:

https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

21. Про критичну інфраструктуру. Закон України від 16.11.2021 № 1882-IX – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20

22. Деякі питання об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

23. Managing cyber risk in the electric power sector. Deloitte Insights, 2018 – Режим доступу до ресурсу: https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

24. Green Paper on Critical Infrastructure Protection in Ukraine: Analytical Report / D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia. - Kyiv. NISS, 2015.

25. Guide To Conducting Cybersecurity Risk Assessment For Critical Information Infrastructure. CSA Singapore, 2021 – Режим доступу до ресурсу: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf

26. Risk Assessment Methodology for Critical Infrastructure Protection. ISBN 978-92-79-28181-5. Joint Research Centre. European Union, 2013 – Режим доступу до ресурсу: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC78292/lbna25745enn.pdf

27. Executing A Critical Infrastructure Risk Management Approach. Department of Homeland Security, 2013 – Режим доступу до ресурсу: https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

28. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. ISBN 978-92-79-49246-4. Joint Research Centre. European Union, 2015

29. Tenth annual EY/IIF global bank risk management survey. Ernst & Young, 2019. Сторінка 25 – Режим доступу до ресурсу: https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2020/01/Global-Risk-Survey_A4_v18-FINAL.pdf

30. Risk IT Practitioner Guide, 2nd Edition. ISBN 978-1-60420-823-8. ISACA, 2020

31. NIST Special Publication 800-30: Guide for Conducting Risk Assessments. National Institute of Standards and Technology (NIST), 2012 – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

32. 2021-2023 Action Plan for Critical Infrastructure. ISBN: 978-0-660-38395-8. Her Majesty the Queen in Right of Canada, 2021

33. Forging a Common Understanding for Critical Infrastructure. Shared Narrative, 2014 – Режим доступу до ресурсу: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

34. Risk Appetite — Critical to Success. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2020

35. GAO-18-62: Critical Infrastructure Protection. GAO, 2017. Сторінка 12 – Режим доступу до ресурсу: https://www.gao.gov/assets/gao-18-62.pdf

36. ISO 31000:2018. Risk management – Режим доступу до ресурсу: https://www.iso.org/obp/ui/ru/#iso:std:iso:31000:ed-2:v1:en

37. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Режим доступу до ресурсу: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27001:ed-3:v1:en

ДОДАТОК А
Копії публікацій

ГРОМАДСЬКЕ ОБЄДНАННЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2023
Тернопіль

УДК 004.056.5

САВЧУК К.В.
Західноукраїнський національний університет

ПІДХОДИ ДО ОЦІНКИ РИЗИКІВ

Вступ. У сучасному світі, де динамічні зміни та несприятливі події можуть впливати на різноманітні сфери діяльності, важливо визначати та оцінювати ризики. Це визначається як ключовий аспект успішного управління, спрямованого на досягнення стійкості та стратегічного розвитку.

Мета: Дослідити сучасні методи та підходи до оцінки ризиків, визначення їх переваг та обмежень, особливо в контексті стрімкого розвитку технологій та глобальних змін у соціально-економічному середовищі.

1. Сучасні та інтегровані підходи до оцінки ризиків

З появою сучасних технологій в сфері управління ризиками з'явилися нові можливості та високоефективні інструменти для виявлення та зниження ризиків. Один із важливих сучасних підходів - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), що спрямований на виявлення та зменшення ризиків в інформаційних системах. OCTAVE дозволяє оцінювати загрози, оцінювати вразливості та визначати критичні активи, щоб розробити стратегії для зниження ризиків [1, 2].

Ще однією важливою методологією є Risk IT Framework, розроблений ISACA. Цей фреймворк надає інтегрований підхід до управління ризиками в контексті IT-галузі. Risk IT Framework визначає ключові принципи та практики для оцінки, управління та мінімізації ризиків, пов'язаних з використанням інформаційних технологій.

Factor Analysis of Information Risk (FAIR) - це підхід, розроблений спеціально для оцінки ризиків в інформаційній безпеці. FAIR використовує кілька ключових категорій, таких як події, активи, вразливості та вплив, для кількісної оцінки ризиків. Цей метод дозволяє керівництву приймати обґрунтовані рішення щодо ефективного та доцільного використання ресурсів на зменшення ризиків.

Однією з найбільш визнаних міжнародних стандартів є ISO 27001, який визначає вимоги до систем управління інформаційною безпекою. Цей стандарт надає засади для визначення, впровадження, управління та покращення систем управління інформаційною безпекою в контексті загального управління ризиками інформаційної безпеки.

COSO ERM (Enterprise Risk Management) визначає принципи та загальні вказівки для впровадження системи управління ризиками на рівні всієї організації. Його фокус на взаємодії між стратегічним управлінням та управлінням ризиками сприяє створенню комплексного підходу до оцінки та управління ризиками [3].

ISO 31000 є міжнародним стандартом, який надає загальні принципи та настанови з управління ризиками. Його фокус на визначенні, оцінці та обробці ризиків робить його важливим інструментом для будь-якої організації, незалежно

від галузі чи розміру.

Ці підходи та стандарти відображають різноманіття інструментів, які сучасні організації можуть використовувати для ефективного управління ризиками в глобальному бізнес-середовищі. Їх інтеграція в управлінські практики дозволяє організаціям впевнено крокувати в майбутнє, забезпечуючи стійкість та успішність у невизначеному світі бізнесу.

2. Процес аналізу та обробки ризиків

Процес аналізу ризиків – це систематичний підхід до визначення, оцінювання та керування потенційними подіями, які можуть впливати на досягнення цілей організації. Ключові елементи аналізу ризиків включають ідентифікацію, оцінку, обробку та моніторинг ризиків.

Існує кілька методів обробки ризиків, які організації можуть використовувати для зменшення чи управління впливом негативних ризиків та вдосконалення можливостей. Ось деякі з них:

– Уникнення ризиків - полягає в ухилі від ситуацій або дій, які можуть стати причиною негативних наслідків.

– Прийняття ризиків - організація вирішує не вживати додаткові заходи для управління ризиками та приймає їх в тому вигляді, в якому вони є.

– Зменшення ризиків - підприємство приймає заходи для зниження ймовірності виникнення ризиків чи їхнього впливу.

– Передача ризиків - передача відповідальності за ризик іншій стороні, часто через страхування чи контракти.

Ці методи можуть використовуватися окремо чи в комбінації, в залежності від конкретних потреб та характеру організації. Окремо треба відмітити, що ігнорування ризиків, не є підходом обробки ризиків та сигналізує про погану культуру управління ризиками в організації.

Висновки.

Проведені дослідження дозволяють зробити висновок, що в умовах невизначеності та глобальних змін ефективне управління ризиками вимагає інтеграції різноманітних методик використання передових технологій. Основні переваги запровадження управління ризиками включають:

– Попередження загроз. Аналіз ризиків дозволяє організаціям передбачати та уникати можливих проблем, а також зменшувати незаплановані витрати із-за сбоїв.

– Ефективне управління ресурсами. Спрямовування ресурсів на найбільш критичні аспекти діяльності та прозорість у повернення інвестицій.

– Підвищення гнучкості. Забезпечення готовності реагувати на зміни у середовищі.

– Підвищення прозорості. Чітка відповідальність у разі настання сбоя чи бажаної події.

Тільки такий комплексний підхід може забезпечити стійкість та успішність в умовах сучасного бізнес-середовища.

Перелік використаних джерел.

1. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments

2. COSO ERM Risk Assessment in Practice Thought Paper October 2012.

3. Introduction to the OCTAVE Approach 2003.

УДК 004.056

СИГИДЕНКО М.М., БАСІСТИЙ В.П.

Західноукраїнський національний університет

МЕТОД ЗАХИЩЕНОЇ МАРШРУТИЗАЦІЇ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Вступ. Маршрутом називається список елементів мережі або ліній та каналів зв'язку, вузлів комутації (ВК), трактів передавання повідомлень (ТПП), що починається з вузла-джерела (ВД) передаваної інформації і закінчується у вузлі-отримувачі (ВО) [1]. Маршрутизація – це набір процедур, що дають змогу визначити й установити оптимальний за заданими параметрами маршрут на мережі зв'язку між ВД та ВО [2].

У мультисервісних мережах (МСМ) функції маршрутизації покладено на мережевий рівень. Цей рівень зручно представити у вигляді підрівнів. На другому, верхньому підрівні проводиться моніторинг стану мережі зв'язку і формування таблиць маршрутизації (ТМ).

Мета: розробити метод захищеної маршрутизації в мультисервісних мережах.

1. Локально-хвильовий метод маршрутизації в мультисервісних мережах

"Локально-хвильовий" метод маршрутизації полягає в тому, що для знаходження оптимального маршруту в мережі між парою вузлів з ВД організовується "Лавинний" пошук, але не в усіх напрямках, а лише в бік ВО. Хвиля пошуку поширюється в деякій зоні у вигляді смуги, що охоплює пару з'єднуваних вузлів (рисунок 1).

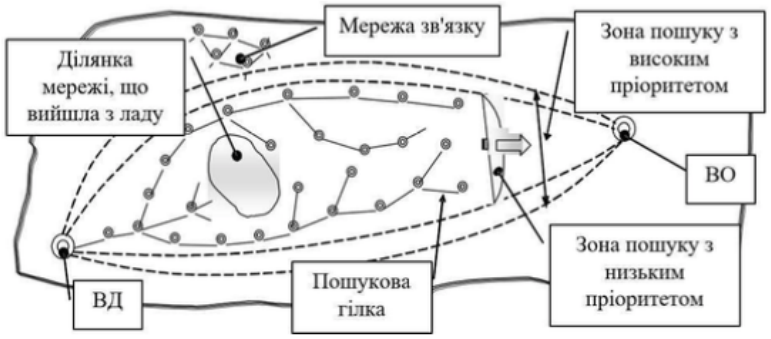

Рисунок 1 - Пошук маршруту "Локально-хвильовим" методом



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2023)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2023
Тернопіль

УДК 004.056.5

***Савчук К.В.*[1]**

[1]Західноукраїнський національний університет

ПРОБЛЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. Критична інфраструктура відіграє важливу роль у забезпеченні національної безпеки, економічного процвітання та загального добробуту країн. Ця стаття має на меті надати загальний огляд значення та важливості критичної інфраструктури, визначаючи спільність визначень, підходів та реалізації серед таких країн - Австралії, Канади, Нової Зеландії, Сполученого Королівства та Сполучених Штатів [1].

Мета: Дослідження еволюції розуміння критичної інфраструктури серед деяких країн, аналіз загальних пріоритетів, підходів та методологій.

1. Еволюція обстановки в галузі безпеки

Кожна з п'яти країн залучалася до розвитку та забезпечення своєї інфраструктури протягом десятиліть. Однак у глобальній обстановці безпеки відбулися значущі зрушення, які змусили кожну з країн переглянути свій підхід до безпеки та стійкості інфраструктури. Виникла ця нестабільність у безпеці в перше десятиріччя нового тисячоліття (внаслідок подій, таких як терористичні атаки 11 вересня 2001 року, вибухи в Балі у 2002 році, вибухи в Лондоні у 2005 році, надзвичайні руйнування внаслідок природних катастроф та глобальна фінансова криза), що змусило кожну з країн зосередитися на безпеці та стійкості критичної інфраструктури. Кожен кризовий випадок продемонстрував важливу роль національних урядів у сприянні створенню безпечної та стійкої критичної інфраструктури [2].

Катастрофи та зміни в глобальній обстановці безпеки також підштовхнули країни думати ширше про різноманіття загроз та небезпек, які стоять перед їхньою національною інфраструктурою. П'ять країн - Австралії, Канади, Нової Зеландії, Сполученого Королівства та Сполучених Штатів прийняли всебічний підхід до вирішення сучасних та майбутніх викликів, з якими стикається їхня інфраструктура. Зокрема, тенденції, такі як зміни клімату та демографічні зрушення, ймовірно, будуть набирати обертів у майбутньому та впливатимуть на системи та активи інфраструктури. Оскільки розрив послуги має серйозні наслідки, важливо, щоб країни враховували ці тенденції як частину безпеки та стійкості критичної інфраструктури. У багатьох випадках найкращий час для врахування цих тенденцій та інших можливих факторів, що можуть порушити, - це час проектування та будівництва інфраструктурних систем та активів. Критична інфраструктура, зокрема, будівельні системи та активи, може мати дуже довгий термін служби, тому кожна з п'яти країн визнає важливість планування для майбутніх зрушень, які можуть порушити надання інфраструктурних послуг.

2. Критична інфраструктура та економічне процвітання

Кожна з п'яти країн визначила, наскільки важливою є критична інфраструктура для сприяння економічному процвітанню та економічній безпеці. Уряди інвестують у критичну інфраструктуру - чи то безпосередньо, чи через

партнерства - з метою зміцнення своїх економік та сприяння процвітанню суспільства. Критична інфраструктура є основою сучасного суспільства, надаючи ключові послуги, які допомагають підприємствам рости і процвітати, такі як високошвидкісний зв'язок, сучасні транспортні мережі та надійна енергія, які сприяють торгівлі та економічному зростанню. Послуги критичної інфраструктури є важливими для економічного зростання, тому уряди працюють над тим, щоб забезпечити, що ці послуги максимально безпечні та стійкі. Забезпечуючи безпеку та стійкість критичної інфраструктури, уряди можуть захищати та збільшувати міцність та життєздатність своїх економік. Як відзначено в національній стратегії Канади, "стійка критична інфраструктура стимулює економічний ріст, привертає та утримує бізнес та створює можливості для зайнятості."

Коли уряди акцентують на зробленні критичної інфраструктури більш безпечною та стійкою шляхом управління ризиками, довіра та впевненість зміцнюються у відносинах державно-приватного секторів, що полегшує економічний ріст. Ця довіра та впевненість в критичній інфраструктурі є ключовою для досягнення безпечного, стійкого та процвітаючого суспільства. Наприклад, Нова Зеландія визнає, що критична інфраструктура є важливим чинником економічного зростання саме з цієї причини Нова Зеландія вказує, що "для того щоб сприяти росту та інвестиціям, компанії повинні мати впевненість в тому, що інфраструктурні системи, що підтримують їхні бізнеси, є безпечними та стійкими." Цей концепт безпечної та стійкої інфраструктури, яка надає впевненість інвесторам та їхнім бізнесам, акцентується в стратегічних настановах всіх п'яти країн.

3. Загальні підходи до управління критичною інфраструктурою

Хоча кожна з п'яти країн має унікальні особливості, мета забезпечення безпеки та стійкості важливих інфраструктурних активів та систем однакова, і всі країни спрямовані на управління ризиками. Вони всі працюють над тим, щоб встановлювати партнерства з власниками та операторами, сприяють співпраці, обміну інформацією та управлінню ризиками. Ці загальні риси надають основу для розширення безпеки та стійкості критичної інфраструктури на міжнародному рівні та зміцнюють відносини між країнами.

Кожна з п'яти країн підтримує міцні партнерства з національними, регіональними та місцевими урядовими контрагентами, а також з власниками та операторами критичної інфраструктури. Ці партнерства є ключовими, оскільки системи критичної інфраструктури належать та експлуатуються як приватними, так і публічними зацікавленими сторонами. Крім того, всі партнери визнають важливість бути національним лідером у справах безпеки та стійкості інфраструктури, і вони загалом працюють схожим чином для побудови цих партнерств.

Обмін інформацією також важливий для стратегії безпеки та стійкості критичної інфраструктури, і кожна країна прагне ділитися своєчасною та відповідною інформацією в безпечному та довіреному середовищі. Чи то через спеціальний бізнес-урядовий форум, який включає онлайн- та офлайн-взаємодії, такий як "Мережа довіри інформаційного обміну" Австралії (TISN), роботу

Великобританії щодо створення безпечних "обмінів інформацією", які надають інструменти та ресурси онлайн для власників та операторів через безпечний інтернет-сайт, чи проведення форумів з відповідними спільнотами. Кожна країна активно займається створенням таких довірених каналів обміну інформацією за допомогою публічних веб-сайтів, інформаційних порталів та шлюзів, партнерств чи різноманітних інших підходів.

На національному рівні уряди працюють над тим, щоб зробити свою критичну інфраструктуру більш безпечною та стійкою з метою збереження та поліпшення наданих цією інфраструктурою ключових послуг. Нижче подано короткий огляд загальних заходів, які уряди приймають для сприяння безпеці та стійкості критичної інфраструктури та полегшення надання ключових послуг своїм населенням [3, 4]:

- Перегляд регіонів та використання їхніх аналітичних ресурсів для ідентифікації національно значущих секторів критичної інфраструктури та послуг, які вони надають.
- Координація з партнерами з публічного та приватного секторів щодо того, як зробити цю інфраструктуру більш безпечною та стійкою.
- Обмін важливою та своєчасною інформацією з відповідними зацікавленими сторонами.
- Співпраця з партнерами та зацікавленими сторонами у справі обміну кращими практиками.
- Визначення міжсекторальних залежностей.
- Створення робочої сили та культури, готової вирішувати складні виклики, що впливають на критичну інфраструктуру.
- Визначення та оцінка критичності інфраструктури.
- Використання підходу до управління ризиками, який визначає способи зменшення ризику для критичної інфраструктури.

4. Спільні сектори критичної інфраструктури

Усі країни визначають сектори критичної інфраструктури. З метою обговорення також корисно визначити спільні та відмінні риси серед визначених секторів критичної інфраструктури.

Кожна з п'яти країн визначила наступні сектори як критичні [5, 6]:

- Зв'язок
- Енергетика
- Охорона здоров'я та громадське здоров'я
- Транспортні системи
- Вода (включаючи системи стічних вод і дощових вод)

Крім того, кілька країн також визначають наступні сектори як критичні:

- Банківські та фінансові послуги
- Критичне виробництво
- Екстрені служби
- Харчова та сільськогосподарська сфери
- Установи уряду
- Інформаційні технології

З цього огляду видно, що існує значна взаємодія між країнами. В той же

час кожна країна надає пріоритет важливим послугам, які лежать в основі безпеки та стабільності їхніх відповідних населень. Працюючи над стратегіями зміцнення міжнародних зв'язків, партнери можуть використовувати це розуміння того, як сектори взаємодіють, як вихідний пункт для обговорення того, як можно співпрацювати та мати плідний, корисний відносини.

Висновок. Проведені дослідження дозволяють зробити висновок, що країни розробляють стратегії для вирішення проблем безпеки та стійкості критичної інфраструктури, спираючись на існуючі плани, стратегії та настанови. Щоб створити основу для спільного розуміння та сприяти скоординованому підходу до підвищення безпеки та стійкості важливих інфраструктур прийняті наступні визначення:

- Критична інфраструктура: системи, активи, об'єкти та мережі, які надають основні послуги і є необхідними для національної безпеки, економічної безпеки, процвітання, охорони здоров'я та безпеки відповідних країн (також відомі як інфраструктура національного значення).
- Стійкість: системи мають здатність бути гнучкими та адаптованими до мінливих умов, як передбачуваних, так і неочікуваних, а також здатні швидко відновлюватися після збоїв.
- Безпека: використання заходів фізичного, кадрового та/або кіберзахисту для зменшення як ризику для критичної інфраструктури, так і ризику втрат через перебої в наданні основних послуг шляхом мінімізації вразливості об'єктів, систем і мереж критичної інфраструктури.

Дослідження виявило не лише спільні визначення, але й спільні підходи та типи інфраструктури, які кожна країна-член вважає важливими. Кожна з країн-членів отримає користь від цієї фундаментальної оцінки, яка допоможе їм знайти спільні точки дотику та сприятиме подальшому обговоренню важливих питань, що становлять взаємний інтерес.

Перелік використаних джерел.

1. Centre for the Protection of National Infrastructure. [Електронний ресурс].- Режим доступу: http://www.cpni.gov.uk/about/

2. Treasury. Higher Living Standards. [Електронний ресурс].- Режим доступу: http://www.treasury.govt.nz/abouttreasury/higherlivingstandards

3. HM Government, Resilience in Society: Infrastructure, Communities and Businesses. [Електронний ресурс].- Режим доступу: https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses

4. Australian Government, Critical Infrastructure Resilience Strategy, (Australian Government, 2010). стр. 4-7, 11-13

5. An Emergency Management Framework for Canada. Third Edition. [978-0-660-07186-2] сторінки 7-12

6. The White House Office of the Press Secretary, Presidential Policy Directive 21. [Електронний ресурс].- Режим доступу: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy- directive-critical-infrastructure-security-and-resil