КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії
(назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему: Модель оцінювання ризиків кіберінцидентів у критичній інфраструктурі

Дудинець Дмитро Олександрович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
_____
„___" _____20___ року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Модель оцінювання ризиків кіберінцидентів у критичній інфраструктурі

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач _Дудинець Дмитро Олександрович
(прізвище, ім'я та по батькові повністю)
__125 кібербезпека та захист інформації___
(спеціальність)
_Безпека інформаційних і комунікаційних систем_____
(освітня програма)
Група _____БІКСм-24_____
Керівник____Делембовский М.М._____
(прізвище та ініціали)
_____кандидат технічних наук, доцент_____
(вчене звання, науковий ступінь)
Рецензент_____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Кафедра: кібербезпеки та комп'ютерна інженерія
Освітній рівень: магістр
Спеціальність:125 кібербезпека та захист інформації
ОПП:безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
Завідувач кафедри
_____
„___"_____20___ року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР
Дудинець Дмитро Олександрович
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи Модель оцінювання ризиків кіберінцидентів у критичній інфраструктурі
затверджена наказом ректора КНУБА № 1635/23.2/25 від «30»вересня2025року
2. Керівник роботи
Делембовський Максим Михайлович кандидиат технічних наук, доцент кафедри кібербезпеки та комп'ютерної інженерії
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту 15 грудня 2025 року
4. Зміст пояснювальної записки за розділами:
Р. 1. Аналіз предметної області та постановка задачі
Р. 2. Кіберзагрози інформаційних систем об'єктів критичної інфраструктури та оцінка небезпеки їх реалізації
Р.3. Розробка метрики кіберстійкості критичної інфраструктури

5. Графічний матеріал за розділами:
Р.1. відсутні
Р. 2. рис. 10, табл. 2
Р. 3. рис. 6, табл. 5

6. Консультанти розділів кваліфікаційної випускної роботи

Розділи	Прізвища, ініціали та посади консультанта	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1.	20.10.2025 р.
Розділ 2.	16.11.2025 р.
Розділ 3.	09.12.2025 р.
Остаточне оформлення роботи	11.12.2025 р.
Направлення роботи на рецензування, перевірку на плагіат	12.12.2025 р.
Попередній захист роботи на кафедрі	15.12.2025 р.

8. Дата видачі завдання ____30 вересня 2025 року_____

Керівник _____ Делембовский М.М
(підпис) (прізвище та ініціали)

Здобувач _____ Дудунець Д.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дудунець Д.О. «Модель оцінювання ризиків кіберінцедентів у критичній інфраструктурі».

Тема дипломного проекту присвячена прийняттю систематичних та перспективних підходів до стійкості. Поточна робота приймає за гіпотезу про те, що InfraGuard Cybersecurity Framework - модель можливостей, яка вимірює зрілість кіберстійкості за допомогою трьох функціональних стовпів, Cyber as a Shield, Cyber as a Space та Cyber as a Sword - є реалізованим і зрозумілим засобом для продовження.

Основною метою роботи розробка реалістичної моделі, яка не тільки окреслює зростання зрілості процесу безпеки, але й сегментує заходи стійкості на три стратегічні напрямки: Щит, Космос та Меч. Ці виміри складаються з рівнів, які вміщують діяльність з кібербезпеки по всьому спектру, починаючи від моніторингу та профілактики до готовності та відновлення. Модель пропонує концептуальні визначення, а також оперативні вказівки для організацій, які прагнуть підвищити свою позицію стійкості в більш складних умовах загроз.

Враховано нормативно-правовий базис України, що регулює сферукібербезпеки об'єктів критичної інфраструктури, зокрема, Закон України "Прокритичну інфраструктуру" та постанову КМУ № 518 "Загальні вимоги докіберзахисту об'єктів критичної інфраструктури". Увага зосереджена навизначенні стандартів та заходів з підвищення кіберзахисту, що сприятимуть зниженню ризиків кіберзагроз.

Практичне значення роботи надає приземлені рекомендації політикам шляхом перекладу атрибутів стійкості в конкретні показники оцінки, сприяння розробці політики, інвестиційному плануванню та глобальній співпраці з кіберзахистом.

Ключові слова: кібербезпека, IoT, стійкість критичної іфраструктури, показники оцінки безпеки, вразливості, загрози, захист даних, штучний інтелект.

SUMMARY

Dudunets D.O. ‘Model for assessing cyber incident risks in critical infrastructure.’

The thesis project is devoted to the adoption of systematic and forward-looking approaches to resilience. The current work assumes that the InfraGuard Cybersecurity Framework — a capability model that measures cyber resilience maturity using three functional pillars, Cyber as a Shield, Cyber as a Space, and Cyber as a Sword — is a practical and understandable tool for further development.

The main goal of the work is to develop a realistic model that not only outlines the growth of security process maturity, but also segments resilience measures into three strategic areas: Shield, Space, and Sword. These dimensions consist of levels that encompass cybersecurity activities across the spectrum, from monitoring and prevention to preparedness and recovery. The model offers conceptual definitions as well as operational guidance for organisations seeking to enhance their resilience posture in more complex threat environments.

The regulatory framework of Ukraine governing the cybersecurity of critical infrastructure, in particular, the Law of Ukraine ‘On Critical Infrastructure’ and Resolution of the Cabinet of Ministers No. 518 ‘General Requirements for the Cybersecurity of Critical Infrastructure,’ has been taken into account. The focus is on defining standards and measures to enhance cyber protection that will help reduce cyber threat risks.

The practical significance of the work is to provide down-to-earth recommendations to policymakers by translating resilience attributes into specific assessment indicators, facilitating policy development, investment planning, and global cooperation on cyber protection.

Keywords: cybersecurity, IoT, critical infrastructure resilience, security assessment indicators, vulnerabilities, threats, data protection, artificial intelligence.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *здобувача українською та англійською мовами* *Дудинець Дмитро Олександрович* *Dudynets Dmytro Oleksandrovych*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Модель оцінювання ризиків кіберінцедентів у критичній інфраструктурі Model for assessing cyber incident risks in critical infrastructure		
Освітній ступінь	Магістр		
Факультет	Автоматизація і інформаційні технології		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 Кібербезпека та захист інформації		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Делембовский Максим Михайлович		
Обсяг роботи:	*Поснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	172	3	
Розділ 1	Аналіз предметної області та постановка задачі		
Розділ 2	Кіберзагрози інформаційних систем об'єктів критичної інфраструктури та оцінка небезпеки їх реалізації		
Розділ 3	Розробка метрики кіберстійкості критичної інфраструктури		
Висновки по роботі	Досліджено проблему забезпечення кіберстійкості об'єктів критичної інфраструктури в умовах зростання сучасних кіберзагроз. Запропоновано ризик-орієнтовану методику оцінки кіберстійкості, що інтегрує технічні, організаційні та управлінські аспекти кіберзахисту й підтримується інформаційно-аналітичним механізмом. Практичні результати		

	підтверджують доцільність переходу до концепції кіберстійкості для підвищення рівня захищеності та безперервності функціонування критичних систем
Ключові слова: Keywords:	кібербезпека, IoT, стійкість критичної іфраструктури, показники оцінки безпеки, вразливості, загрози, захист даних, штучний інтелект cybersecurity, IoT, critical infrastructure resilience, security assessment indicators, vulnerabilities, threats, data protection, artificial intelligence

Здобувач Дудинець Д.О.___/ _____

Керівник Делембовский М.М._____/ _____

ЗМІСТ

ВСТУП

Збільшення частоти та тяжкості кібератак на критичну інфраструктуру підкреслили необхідність прийняття систематичних та перспективних підходів до стійкості. Поточне дослідження приймає за гіпотезу про те, що InfraGuard Cybersecurity Framework - модель можливостей, яка вимірює зрілість кіберстійкості за допомогою трьох функціональних стовпів, Cyber as a Shield, Cyber as a Space та Cyber as a Sword - є реалізованим і зрозумілим засобом для продовження. Модель розглядає важливі аспекти ситуаційної обізнаності, активного захисту, управління ризиками та відновлення після інцидентів і вимірюється за допомогою глобально стандартизованих моделей зрілості, таких як ISO/IEC 15504, NIST CSF та COBIT. Внески включають багатовимірні вимірювання стійкості, забальну шкалу можливостей (0–5) та класифікацію на основі доменів, що дозволяє організаціям оцінювати та покращувати свою ситуацію з кібербезпекою формалізовано. Застосовність структури проілюстрована трьома дослідницькими налаштуваннями електромереж, систем охорони здоров'я та аеропортів, кожен з яких становить різні рівні зрілості стійкості. Це дослідження надає приземлені рекомендації політикам шляхом перекладу атрибутів стійкості в конкретні показники оцінки, сприяння розробці політики, інвестиційному плануванню та глобальній співпраці з кіберзахистом.

Дипломна робота присвячена комплексному дослідженню проблем забезпечення кіберстійкості об’єктів критичної інфраструктури в умовах інтенсивної цифровізації, глобалізації та зростання кількості і складності кіберзагроз. У сучасному світі критична інфраструктура відіграє визначальну роль у забезпеченні національної безпеки, стабільного функціонування економіки, підтриманні соціальної стабільності та життєдіяльності суспільства. Порушення її роботи внаслідок кібератак може призвести до значних економічних втрат, загроз життю та здоров’ю населення, дестабілізації державного управління та підриву обороноздатності країни.

У роботі проаналізовано сучасний стан та тенденції розвитку критичної інфраструктури, визначено її основні складові та характерні особливості в умовах переходу до цифрових і кіберфізичних систем. Особливу увагу приділено аналізу актуальних кіберзагроз, зокрема атак на операційні технології, промислові системи управління, хмарні сервіси, мережі Інтернету речей, а також діяльності організованих кіберзлочинних угруповань та APT-груп. На основі аналізу відомих інцидентів у різних країнах світу показано реальні масштаби небезпеки та наслідки кібератак для об'єктів критичної інфраструктури.

Значну частину роботи присвячено аналізу нормативно-правового забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури в Україні. Розглянуто основні законодавчі та підзаконні акти, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», рішення Ради національної безпеки і оборони України, постанови Кабінету Міністрів України, а також стратегічні документи у сфері національної та інформаційної безпеки. Проаналізовано вимоги до створення систем інформаційної безпеки та комплексних систем захисту інформації на об'єктах критичної інфраструктури, роль оцінки ризиків відповідно до стандарту ДСТУ ISO/IEC 27005, а також значення незалежного аудиту кібербезпеки. Показано відповідність та взаємозв'язок національної нормативної бази з міжнародними стандартами та рекомендаціями (ISO/IEC 27001, NIST Cybersecurity Framework, директива NIS2 Європейського Союзу).

У межах огляду літератури проаналізовано вітчизняні та зарубіжні наукові праці, присвячені проблемам кібербезпеки та кіберстійкості критичної інфраструктури. Розглянуто сучасні підходи до оцінювання стійкості, включаючи ризик-орієнтовані моделі, багатоагентні системи, використання методів штучного інтелекту, архітектурні рішення для хмарних та розподілених систем, а також практичні інструменти самооцінки кіберстійкості. Узагальнення результатів аналізу дозволило визначити основні недоліки існуючих підходів та обґрунтувати доцільність розробки комплексної методики оцінки кіберстійкості.

Практичне значення результатів роботи полягає у можливості використання запропонованої методики та програмного інструменту органами державної влади, операторами об’єктів критичної інфраструктури, службами інформаційної та кібербезпеки для оцінки рівня захищеності, виявлення критичних вразливостей і формування обґрунтованих управлінських рішень щодо підвищення кіберстійкості. Отримані результати можуть бути використані при плануванні заходів кіберзахисту, підготовці технічних завдань на створення систем інформаційної безпеки та проведенні аудитів кібербезпеки.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Загальний опис критичної іфраструктури і її значення в сучасному світі

В епоху зростаючого домінування глобалізації та цифровізації критична інфраструктура зазнала значних перетворень, перетворившись на більше, ніж просто систему підтримки сучасного життя [1,2]. Сьогодні критична інфраструктура вже не є просто допоміжним елементом, а скоріше складною системою, яка служить життєво важливою артерією, полегшуючи життя економіки, підтримуючи соціальну стабільність та захищаючи національну безпеку [3,4,5]. Ці основні мережі охоплюють транспортні, енергетичні, чисті, банківські та телекомунікаційні системи, формуючи основу, яка підтримує фундаментальні функції повсякденного життя [6]. Безпека та стійкість критичної інфраструктури є основними рушійними силами, що стоять за пульсом прогресу та стійкості сучасного суспільства [7,8]. Вирішальна роль цієї інфраструктури впливає не тільки на суспільний добробут, але й на економічну стабільність та національний суверенітет [9,10]. Тому розуміння та оцінка важливої ролі критичної інфраструктури в повсякденному житті є обов'язковими і не можуть бути проігноровані . Однак під час все більш взаємопов'язаної та автоматизованої сучасної епохи критична інфраструктура стала вразливою мішенню для складних та пов'язаних з кібератак. Кіберзагрози більше не є просто спекуляціями; вони проявляються як реальні загрози, здатні порушити роботу нашої важливої інфраструктури. Їх вплив, схожий на ударні хвилі, може поширитися в економічний сектор, загрожувати екологічній цілісності і навіть загрожувати життю людей.

Кілька помітних інцидентів, таких як атака Stuxnet на ядерні об'єкти Ірану, широкомасштабні відключення електроенергії в Україні [та скоординовані кібератаки в 2021 році, спрямовані на системи водопостачання та відходів у Сполучених Штатах, всі підкреслюють підвищений ризик для критичної інфраструктури. Тому розуміння та передбачення цих загроз є обов'язковими, і необхідні максимальні зусилля для захисту критичної інфраструктури від

кібератак. Інвестиції в передові технології та стратегії кібербезпеки є необхідністю для захисту нашої інфраструктури та, зрештою, забезпечення безпеки та добробуту нашого суспільства. У цьому контексті звіт Thales 2022 про загрозу для критичної інфраструктури забезпечує більш глибоке розуміння впливу кібератак на критичну інфраструктуру. Цей звіт узагальнює ключові висновки, зібрані в результаті опитувань лідерів та практиків в організаціях критичної інфраструктури, пропонуючи уявлення про пом'якшення ризиків, таких як програми-вимагачі та шкідливі програми. Цікаво, що в опитуванні зазначається, що 79% респондентів висловили стурбованість ризиками безпеки віддаленої роботи, підкреслюючи, як зміни в сучасних моделях роботи вносять нові виклики в безпеку критичної інфраструктури. Так само 44 відсотки повідомили про збільшення обсягу, тяжкості та/або масштабів кібератак за останні 12 місяців, при цьому 55% ідентифікували шкідливе програмне забезпечення як найпоширенішу причину зростання атак. Це підкреслює ескалацію загроз, з якими стикається критична інфраструктура у всьому світі.

Як конкретний приклад, Австралія повідомила про 143 кібератаки на свою критичну інфраструктуру за останній рік, порівняно з 95 інцидентами минулого року. Ці атаки охоплювали енергетичний, комунальний, телекомунікаційний та транспортний сектори. Зміни в цифровому ландшафті за останнє десятиліття також очевидні, при цьому раніше ізольовані системи операційних технологій (OT) стають все більш підключеними до Інтернету. Розумні датчики IoT живляться від водних та енергетичних систем, а державні операції глибоко вкорінені в даних. Зростаюча залежність від хмарних платформ забезпечує вразливу поверхню атаки для зловмисників та ворожих країн [42,43]. Зіткнувшись з цими викликами, розуміння та передбачення загроз стають вирішальними. Необхідні максимальні зусилля для захисту критичної інфраструктури від кібератак. Мудрі інвестиції в передові технології та стратегії кібербезпеки є необхідністю для забезпечення безпеки та добробуту нашого суспільства. Постійні оновлення та адаптація до розробок у галузі технологій та кіберзагроз є вирішальними кроками у забезпеченні

стійкості критичної інфраструктури в цю все більш взаємопов'язану та автоматизовану епоху.

1.2 Опис проблеми та постановка задачі

Критична інфраструктура (КІ) є основою стабільного функціонування держави та суспільства. До її складу належать енергетичні системи, транспортні мережі, телекомунікації, фінансовий сектор, об’єкти охорони здоров’я та інші життєво важливі галузі. Інтенсивна цифровізація цих систем, їх висока взаємозалежність та зростання кількості кіберзагроз призводять до суттєвого підвищення ризиків порушення їхньої роботи. Кіберінциденти здатні спричиняти масштабні економічні збитки, тривалі перебої у наданні послуг, соціальну нестабільність та порушення національної безпеки.

Попри значну кількість існуючих методів оцінки кіберризиків, більшість з них зосереджені на окремих аспектах безпеки: вразливостях, ймовірностях атак або прогнозуванні наслідків. Вони не враховують комплексного характеру сучасних кіберзагроз, не відображають взаємозалежність компонентів КІ та здатність системи не лише протистояти атаці, але й швидко відновлюватися після неї. У результаті оператори КІ не мають інструмента, який дозволяв би об’єктивно вимірювати рівень кіберстійкості та визначати пріоритети підвищення безпеки.

Таким чином, проблема полягає у відсутності комплексної, інтегрованої та придатної до практичного використання метрики кіберстійкості критичної інфраструктури, яка б відображала всі ключові аспекти захищеності системи.

Науково-технічна задача, що вирішується у дипломній роботі, формулюється так:розробити методику та математичну модель інтегрованої метрики кіберстійкості критичної інфраструктури, яка враховує вразливість, готовність до реагування, здатність до відновлення та рівень технологічного розвитку системи.

1.2 Нормативно-правове забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури

Основними нормативно-правовими документами на даний час, які стосуються питання забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури в Україні є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р. [1], Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 [2], Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [3], Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [4], Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 [5] та деякі інші.

Так Закон України «Про основні засади забезпечення кібербезпеки України» [1] визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У даному Законі України, серед інших, дано визначення таких термінів, як «інцидент кібербезпеки», «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «критична інформаційна інфраструктура», «об’єкти критичної інфраструктури», «об’єкт критичної інформаційної інфраструктури». Даним Законом України визначено, що об’єкти критичної інфраструктури являються об’єктами кібербезпеки, а об’єкти критичної інформаційної інфраструктури являються об’єктами кіберзахисту. Зазначені об’єкти, які можуть бути віднесені до критичної інфраструктури, сформульовані принципи забезпечення кібербезпеки,

приведений перелік заходів для функціонування національної системи кібербезпеки. Положеннями цього Закону України визначено заходи, спрямовані на забезпечення кібербезпеки та кіберзахисту, а також визначена відповідальність за порушення законодавства у сфері кібербезпеки.

Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 [2], серед іншого, передбачається формування пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту відповідних об'єктів. Крім того, передбачається протокол дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків.

Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [3], визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури. У відповідності до п.3 даних Вимог «кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю». Відповідно до п.7 зазначених Вимог «у випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не

обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об'єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури». У цьому ж пункті зазначається, що «створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки». А технічне завдання, в свою чергу, формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005. Тобто, ми можемо констатувати, що технічне завдання на створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Крім того, у даних Загальних вимогах наведено перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та вимоги до формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [4], визначає механізм формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. У відповідності до п.2 даного Порядку

«об’єкти критичної інфраструктури» - це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення. Відповідно до п.4 зазначеного Порядку, включені до переліку інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно). У п. 8 даного Порядку зазначено, що заінтересовані органи формують пропозиції до переліку з урахуванням негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему. Такими негативними наслідками є [4]:

- виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);
- негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);
- негативний вплив на стан економічної безпеки держави (Н.3);
- негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);
- негативний вплив на систему управління державою (Н.5);
- негативний вплив на суспільно-політичну ситуацію в державі (Н.6);
- негативний вплив на імідж держави (Н.7);
- порушення сталого функціонування фінансової системи держави (Н.8);
- порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);
- порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її

взаємодії з відповідними інфраструктурами інших держав (Н.10).

Крім того, у даному Порядку вказано, що до переліку не включаються інформаційно-телекомунікаційні системи, які не мають виходу каналами електрозв'язку за межі контрольованої зони [4].

Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [5], спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16 вересня 2014 року № 1678-VII, і Стратегією сталого розвитку "Україна - 2020", схваленою Указом Президента України від 12 січня 2015 року № 5. Стратегією визначено цілі Стратегії національної безпеки України, актуальні загрози національній безпеці України, основні напрями державної політики національної безпеки України. У відповідності до п.3 Стратегії актуальними загрозами, серед інших є загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсів, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, загрози безпеці критичної інфраструктури. У відповідності до п. 4.12 Стратегії одним з основних напрямів державної політики національної безпеки України є Забезпечення кібербезпеки і безпеки інформаційних ресурсів. При цьому, пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору

безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 [6] визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Доктриною визначено її мета та принципи, національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, механізм реалізації Доктрини. У відповідності до п. 3. Стратегії встановлено, що національними інтересами України в інформаційній сфері, серед іншого, є розвиток та захист національної інформаційної інфраструктури, розвиток інформаційного суспільства, зокрема його технологічної інфраструктури, розвиток системи стратегічних комунікацій України, забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України, захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом.

Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення

захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту [7-21].

1.4 Мета та завдання дипломної роботи

Метою дипломної роботи є всебічне теоретичне та прикладне дослідження проблеми забезпечення кіберстійкості об’єктів критичної інфраструктури в умовах зростаючої складності та інтенсивності кіберзагроз, а також розробка комплексної методики оцінювання рівня кіберстійкості, що враховує технічні, організаційні та нормативно-правові аспекти функціонування таких об’єктів. Робота спрямована на формування системного підходу до оцінки здатності інформаційних та кіберфізичних систем критичної інфраструктури запобігати кібератакам, своєчасно виявляти інциденти, ефективно реагувати на них і відновлювати працездатність з мінімальними втратами.

У межах досягнення поставленої мети передбачається проведення аналізу сучасного ландшафту кіберзагроз, зокрема загроз для промислових систем управління, операційних технологій, хмарних та розподілених інформаційних систем, а також дослідження практик і вимог міжнародних стандартів у сфері кібербезпеки та кіберстійкості. Особлива увага приділяється оцінці відповідності існуючих підходів до захисту об’єктів критичної інфраструктури вимогам національного законодавства України та директивам Європейського Союзу, що регламентують забезпечення безпеки критичних сервісів.

Досягнення мети також передбачає розробку структури критеріїв, показників та метрик оцінки кіберстійкості, які дозволяють кількісно та якісно характеризувати рівень захищеності, надійності та адаптивності інформаційних систем об’єктів критичної інфраструктури. На основі запропонованих критеріїв планується створення алгоритму інтегрованого оцінювання та інформаційно-

аналітичного інструменту, що забезпечує автоматизацію процесів аналізу кіберризиків, виявлення критичних вразливостей і підтримку прийняття управлінських рішень щодо підвищення кіберстійкості.

Реалізація поставленої мети дипломної роботи спрямована на підвищення ефективності управління кібербезпекою об’єктів критичної інфраструктури, зниження ймовірності порушення їх функціонування внаслідок кібератак та забезпечення безперервності надання критично важливих послуг. Отримані результати мають наукову та практичну цінність і можуть бути використані при розробці політик кібербезпеки, плануванні заходів із захисту інформаційних систем, проведенні аудитів кібербезпеки та формуванні стратегій підвищення кіберстійкості на національному і галузевому рівнях.

1.5 Об’єкт та предмет дослідження

Об’єктом дослідження у дипломній роботі є складні інформаційні, кіберфізичні та організаційно-технічні системи об’єктів критичної інфраструктури, а також процеси їх функціонування та управління в умовах цифрової трансформації та зростання кіберзагроз. До об’єкта дослідження належать системи інформаційних технологій та операційних технологій (IT/OT), засоби комунікації, управлінські та технологічні процеси, а також механізми забезпечення кібербезпеки, які реалізують запобігання, виявлення, локалізацію, реагування та відновлення після кіберінцидентів. Об’єкт дослідження охоплює як технічні компоненти, так і організаційні та регламентні аспекти діяльності об’єктів критичної інфраструктури, що забезпечують їхню стійкість і безперервність надання критично важливих послуг.

Предметом дослідження є сукупність науково-методичних підходів, моделей, методів та алгоритмів оцінювання кіберстійкості об’єктів критичної інфраструктури, а також критерії, показники та метрики, що дозволяють кількісно й якісно оцінити рівень захищеності, надійності та адаптивності інформаційних і кіберфізичних систем. Предмет дослідження включає методи аналізу кіберризиків,

моделювання загроз і вразливостей, підходи до інтегрованого оцінювання стійкості, а також інформаційно-аналітичні та програмні засоби, призначені для автоматизації процесів збору, обробки й інтерпретації даних, необхідних для підтримки прийняття управлінських рішень у сфері кібербезпеки.

Визначення об’єкта та предмета дослідження у такому вигляді дозволяє чітко окреслити межі дипломної роботи, забезпечити системний підхід до аналізу проблеми кіберстійкості та створити методологічну основу для розробки ефективної методики оцінювання, орієнтованої на практичне застосування в діяльності операторів об’єктів критичної інфраструктури та органів управління у сфері кібербезпеки.

1.6 Огляд літератури

Протистояючи ескалації кіберзагроз критичній інфраструктурі, кілька досліджень зробили значний внесок у розуміння та вирішення цих проблем. Ці дослідження охоплюють різні аспекти, починаючи від використання штучного інтелекту (ШІ) для виявлення та протидії загрозам до розробки моделей стійкості громади та практичних інструментів, які допомагають організаціям більш ефективно протистояти кіберзагрозам. Тому дуже важливо усвідомлювати, що різноманітні та інноваційні підходи вкрай необхідні для вирішення все більш складних та динамічних проблем кібербезпеки.

Одним з основних факторів нашого розуміння та поводження з кіберзагрозами для критичної інфраструктури є дослідження Абухаселя [9]. У своїй роботі Абухасель запропонував конструктивну модель стійкості, спричинену штучним інтелектом (AI-CRM), як прогресивний крок для посилення кібербезпеки критичної інфраструктури. Ця модель не тільки враховує потенційний вплив, який противники можуть мати на елементи інфраструктури, але й обчислює ймовірності на основі впливу попередніх атак на збої інфраструктури та реакції на оперативне

обслуговування. Завдяки такому підходу стійкість можна покращити, додавши заходи безпеки, які реагують на вплив атак. Прохоренко та Бабар [53] також роблять свій внесок, пропонуючи комплексний архітектурний підхід до підвищення стійкості хмарних, туманних та крайових систем у контексті критичної інфраструктури. Вони впроваджують структуру, засновану на можливостях, призначену для зміцнення загальної стійкості системи. Окрім вирішення питань довіри в контексті стійкості та надійності системи, це дослідження надає поглиблене уявлення про існуючі рішення для підвищення стійкості розподілених систем. Каріас та ін. [54] використовують практичний підхід, розробляючи веб-операційний інструмент, щоб допомогти організаціям реалізувати кіберстійкість у критичній інфраструктурі. Цей інструмент не тільки надає організаціям можливість слідувати комплексному процесу, включаючи впровадження системи кіберстійкості, але й інтегрує інструмент самооцінки кіберстійкості (CR-SAT), протестований за допомогою тематичних досліджень. Таким чином, це дослідження підкреслює, як веб-інструменти та технології можуть полегшити та зміцнити кіберстійкість в організаціях. Кларк і Зонуз [55] обговорюють надійну роботу кіберфізичної інфраструктури в потенційно змагальних екологічних ситуаціях. Вони представляють формальне визначення показників стійкості та оцінки, які вимірюють здатність системи відновлюватися після атак протягом певного проміжку часу та вартість відновлення. Цей підхід ілюструє, як стійкість передбачає, що складні атаки можуть обійти механізми захисту та виявлення, і, таким чином, надійна система повинна мати можливість реагувати за допомогою реактивних та проактивних механізмів толерантності до атак. Валінежад та Мілі [14] привносять концепцію стійкості громади до розуміння стійкості. Вони розробляють багатоагентну модель, яка об'єднує кібер, фізичні та соціальні аспекти, щоб зрозуміти готовність та адаптивність перед обличчям загроз. Це дослідження підкреслює, що співпраця в громаді може мати значний позитивний вплив на індивідуальну поведінку і що міцні відносини в громаді є ключовим фактором зміцнення стійкості. Домінгес-Дорадо та ін. [56] підкреслюють важливість впровадження еталонної моделі в управлінні кібербезпекою на

нижчому рівні критичної інфраструктури. Вони пропонують процес, який вони називають CyberTOMP для управління кібербезпекою на цьому рівні, і надають методологічні елементи, що підтримують його реалізацію. Це дослідження вказує на те, що управління кібербезпекою вимагає комплексного та цілісного підходу. Кумар, Альварес та Кумар [57] провели відповідні дослідження щодо стійкості безпеки в комерційних розумних пристроях у контексті критичної інфраструктури. У їхньому дослідженні обговорюється, як атаки на кібербезпеку можуть вплинути на операції та цілісність даних цих розумних пристроїв, які відіграють центральну роль у все більш важливій мережі розумної мережі. Ешлі та ін. [6] б'ють тривогу про актуальність кібербезпеки в критичній інфраструктурі та представляють Network Defense Training Game (NDTG) як навчальну платформу з кібербезпеки. NDTG використовує наративи на основі сценаріїв, засновані на історичних кіберінцидентах, і призначений для навчання користувачів їх розумінню та навичкам у вирішенні подій кібербезпеки та інцидентів у критичній інфраструктурі. Макракіс та ін. [45] забезпечують комплексне обстеження загроз та атак на промислові системи управління та критичну інфраструктуру. Це опитування забезпечує глибоке розуміння різних загроз та вразливостей, з якими стикається критична інфраструктура. Сімоне та ін. [58] представляють інноваційний підхід, який поєднує модель STAMP з системно-теоретичним аналізом процесів для безпеки (STPA-Sec) та симуляцією для виявлення вразливого контролю в соціально-технічних системах в контексті критичної інфраструктури. Цей метод був застосований у тематичному дослідженні водоочисних споруд і допоміг підвищити стійкість цієї інфраструктури до кіберзагроз.

Загалом, ці дослідження значно сприяють розумінню та підвищенню стійкості та кібербезпеки в контексті критичної інфраструктури. Завдяки різноманітним підходам, починаючи від моделі AI-CRM до навчання кібербезпеці на основі ігор, а також аналізу кібератак на розумні лічильники та промислові системи управління, ці дослідження спрямовані на зміцнення стійкості критичної інфраструктури до загроз, що розвиваються. Ці дослідження відіграють ключову роль у підтримці безперервності операцій та безпеки систем, життєво важливих для

сучасного суспільства та економіки. Це демонструє, що дослідження та інновації в цій галузі мають вирішальне значення для забезпечення безпеки та стійкості нашої критичної інфраструктури.

1.7 Висновок до першого розділу

Проведений аналіз показує, що об’єкти критичної інфраструктури є ключовим елементом стабільності суспільства та економіки, однак зростаюча цифровізація робить їх вразливими до складних кіберзагроз. Значну увагу приділено нормативно-правовим аспектам – визначено основні закони та стандарти (українські та міжнародні), що регламентують захист інформаційних систем ОКІ. Обґрунтовано, що забезпечення кіберстійкості цих об’єктів потребує комплексних заходів, які охоплюють не лише технічні, а й організаційні та процесні рішення. Враховуючи зростання ризиків від програм-вимагачів, APT-груп та атак на операційні технології, висвітлено необхідність розробки нової методики оцінки кіберстійкості, що базується на ризик-орієнтованому підході та міжнародних стандартах.

Описано значення критичної інфраструктури та її складових, підкреслено роль ключових секторів у функціонуванні держави й суспільства.Встановлено, що через глибинну взаємопов’язаність і автоматизацію сучасних систем критична інфраструктура піддається потужним кіберзагрозам, наслідки яких можуть поширюватись на економіку й безпеку.Проаналізовано діюче законодавство та стандарти (зокрема українські закони, директиви ЄС, ISO/NIST), що визначають вимоги до захисту КІ, зазначено обов’язкові процедури аудиту та оцінювання ризиків.Сформульовано мету та основні завдання роботи – створити методику оцінки кіберстійкості ОКІ з урахуванням сучасного ландшафту загроз і норм. Пропонований підхід передбачає розробку критеріїв та метрик стійкості, а також інформаційно-аналітичного інструменту для їх застосування.Проведено огляд наукових робіт, що підтверджують необхідність інтеграції інноваційних засобів

(штучний інтелект, моделі стійкості, навчальні платформи тощо) для підвищення стійкості критичної інфраструктури.

Таким чином, сформована у вступі структура дослідження обґрунтовує актуальність теми та визначає чітку послідовність подальших етапів роботи. Реалізація поставлених завдань сприятиме розробці ефективних механізмів оцінки та підвищення кіберстійкості критичної інфраструктури, що відповідають сучасним вимогам національної й міжнародної безпеки.

2 КІБЕРЗАГРОЗИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ОЦІНКА НЕБЕЗПЕКИ ЇХ РЕАЛІЗАЦІЇ

2.1 Сучасні підходи до оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Проведений аналіз показує, що у науковій літературі розглядаються і досить детально аналізуються методи оцінювання ризику, у тому числі для систем SCADA. Проведений аналіз методів оцінки ризиків інформаційної безпеки показав [22], що метод на основі побудови «Матриці СУІБ» дозволяє оцінити ступінь захисту вже існуючої СЗІ та ступінь виконання всіх вимог по забезпеченню інформаційної безпеки. Однак, даний метод не завжди застосуємо до інформаційної системі, яка створюється. Також для удосконалення даного методу необхідно додати декілька якісних шкал або можливість самостійно створювати шкали за обраним критерієм оцінювання. Метод оцінки ризиків інформаційної безпеки на основі теорії нечітких множин навіть при недостатньому обсязі вхідних даних дозволяє побудувати адекватну модель впливу загроз на ресурс, який підлягає захисту. При цьому можливо розглядати кілька розгалужень реалізації загрози або безлічі загроз на ресурс. Таким чином, можна оцінити найбільш ймовірні загрози на ІС і, на базі отриманої інформації, створити або модернізувати систему захисту інформації. Однак і цей метод має свої недоліки, оскільки не враховує час реалізації загрози, а бере до уваги тільки суб'єктивну ймовірність реалізації загрози або безлічі загроз. Реалізація загрози може зайняти час більший, ніж інформаційний ресурс буде мати цінність. Тому, для вдосконалення даного методу пропонується ввести коефіцієнт нормування за часом згідно з думкою експерта при складанні опитувальних листів і проведенні оцінювання ризиків ІБ [22].

Так, у [23] показано, що незважаючи на те, що просування в галузі інформаційних технологій підвищило ефективність транспортної інфраструктури, це, у свою чергу, створило більш високий ризик, пов'язаний з кіберсистемами. Мета цього дослідження - інформувати транспортну політику та управління в США шляхом виявлення перешкод на надійному ринку кіберстрахування та підвищення кіберстійкості транспортної інфраструктури. Це здійснюється за допомогою змішаного підходу, що включає аналіз даних про кібер-інциденти в США для транспортних систем та серію інтерв'ю з менеджерами транспортної інфраструктури та страховиками. Внески включають нові погляди на природу кібер-ризику для транспортної інфраструктури та рекомендації щодо науково-дослідних потреб для покращення управління кібер-ризиками та страхування. Результати показують, що щорічно збільшується кількість транспортних компаній, що постраждали від кіберінцидентів та пов'язаних з цим витрат. Найчастіші випадки пов'язані з порушенням даних, тоді як випадки порушення конфіденційності мають найвищий середній збиток за інцидент. Оцінка кібер-ризиків, заходи щодо пом'якшення наслідків та безпеки та страхування в різній мірі впроваджуються в транспортних інфраструктурних системах, але, як правило, недостатньо. Наразі менеджери інфраструктури не мають інструментів для жорсткої оцінки та управління кібер-ризиком. Обмежені дані та моделі також гальмують точне моделювання кібер-ризику для страхових цілей. Навіть після розробки вдосконалених інструментів та моделювання придбання страхування може стати важливою стратегією управління ризиками, щоб дати змогу системам транспортної інфраструктури відновитися після кібер-інцидентів [23].

Деякі автори зазначають [24], що кібер-ризики належать до порядку денного бізнесу кожної компанії, однак їх важко оцінити через відсутність достовірних даних та ретельного аналізу. Ці фахівці розглядають широкий спектр подій, пов'язаних з кібер-ризиком, та фактичні дані про витрати. Для цього вони визначають кіберзбитки з бази даних операційних ризиків та аналізують їх за допомогою методів статистики та актуарної науки. Вони використовують метод пік-порогового значення з теорії екстремальної цінності для виявлення "кібер-

ризиків повсякденного життя" та "крайніх кібер-ризиків". Показано, що поведінка людини є основним джерелом кібер-ризику, а кібер- ризики сильно відрізняються порівняно з іншими категоріями ризику. Приведені моделі можуть бути використані для отримання послідовних оцінок ризику в залежності від країни, галузі, розміру та інших змінних [24].

Досліджено статтю [25], яка присвячена оцінці економічного впливу Інтернету речей (IoT) та пов'язаних з ним кібер-ризикових векторів і вершин - переосмислення вертикалей IoT. Автори адаптують до IoT як модель Cyber Value at Risk, добре налагоджену модель вимірювання максимально можливих втрат за даний період часу, так і модель MicroMort - широко використовувану модель прогнозування невизначеності через одиниці ризику смертності. Отриманий новий IoT MicroMort для обчислення ризику IoT тестується та підтверджується реальними даними з IoT-сканера BullGuard (понад 310 000 сканувань) та звіту Garner про пристрої, підключені до IoT. Розроблено два розрахунки, поточний стан кібер-ризику IoT та майбутні прогнози кібер-ризику IoT. Таким чином, зазначена наукова робота спрямовує зусилля на інтеграцію оцінок впливу на кібер-ризики та пропонує краще розуміння оцінки економічного впливу на кібер-ризик IoT [25].

У роботі [26] показано, що поширення технологій, вбудованих у підключені та автономні транспортні засоби (CAV), збільшує потенціал кібератак. Системи зв'язку між транспортними засобами та інфраструктурою надають віддалений доступ для атак для зловмисних хакерів для використання вразливості системи. Підвищена сполучуваність у поєднанні з функціями автономного водіння створює значну загрозу величезним соціально- економічним вигодам, обіцяним CAV. Однак відсутність історичної інформації про кібератаки означає, що традиційні методи оцінки ризику роблять неефективними. У цій роботі пропонується проактивна модель класифікації кібер-ризиків CAV, яка долає цю проблему, включаючи відомі вразливості програмного забезпечення, що містяться в Національній базі даних про вразливість США, у етапи побудови моделі та тестування. Цей метод використовує модель Bayesian Network (BN), спираючись на

змінні та причинно-наслідкові зв'язки, що випливають із загальної схеми оцінювання вразливості (CVSS), для представлення ймовірнісної структури та параметризації кібер-ризику CAV. Отримана модель BN підтверджується вибірковим тестом, що демонструє майже 100% точність прогнозу кількісного показника ризику та якісного рівня ризику. Потім модель застосовується до випадку використання GPS-систем CAV з криптографічною автентифікацією та без неї. У випадку використання демонструється, як модель може бути використана для прогнозування ефекту заходів щодо зменшення ризику [26].

У статті [27] зазначається, що кіберзлочинці без особливих перешкод ведуть свою торгівлю. Користувачі домашніх комп'ютерів особливо вразливі до нападу все більш досконалої та глобально розповсюдженої групи хакерів. Епоха смартфонів загострила ситуацію, запропонувавши хакерам ще більше нападників для експлуатації. Це може бути не зовсім збігом випадків, коли кіберзлочинність розмножується паралельно з урядами, що дотримуються порядку денного неолібералізму. Цей порядок денний має сильний потяг до індивідуалізації ризику, тобто, поради громадян, як дбати про себе, а потім залишати їх перед наслідками, якщо вони вирішать не дотримуватися порад. Насправді, громадяни "відповідальні". Оскільки реагування ефективне для деяких ризиків, відповідальність на кібербезпеку сприяє глобальному успіху кібератак. Отже, має бути розроблений випадок для урядів, які беруть активнішу роль, ніж просто надання порад, як це відбувається у багатьох країнах. Автори надають конкретну пропозицією щодо режиму регулювання ризиків, який би більш ефективно зменшив кібер-ризик [27].

У науковій роботі [28] представлено кібер-ризик як критичний бізнес- ризик, що переливається на стратегічний ризик, кредитний ризик та регулятивний ризик на рівні організації, а також ринковий ризик та системний ризик на рівні портфеля. Потім автор аналізує унікальність кібер-ризику, необхідність вимірювання кібер-ризику та його поточні виклики, після чого проводиться огляд вартості кіберзлочинності, категорії втрат кібер-інцидентів та моделі для вимірювання

очікуваних збитків від кібер-інцидентів, включаючи річну тривалість втрат, стандарт відхилення втрат та сприйнятий складений ризик. Потім він охоплює сучасні методи вимірювання кібер-ризиків, наприклад, загальну систему оцінювання вразливості (CVSS), CORAS, стохастичне моделювання, моделювання в Монте-Карло, кібер-значення з ризиком та факторний аналіз інформаційного ризику (FAIR). Квадрант кібер-ризику представлений у цій главі, застосовуючи вимірювання медичного ризику до кібер-контексту. Він класифікує фактори ризику на технологічні, нетехнологічні, притаманні (немодифікуючі) та контрольні (що змінюються) фактори. Наведено також приклади аналізу сценаріїв для оцінки контролю та кількісної оцінки втрат [28].

У роботі [29] пропонується система оцінювання кібер-ризиків, яка враховує найгірший випадок лікаря щодо можливості медичного обладнання вплинути на пацієнта. Підвищена підключеність медичних пристроїв прискорює лікування пацієнтів та забезпечує життєзабезпечення можливостей, але відсутність акценту на безпеці пристроїв призвело до кількох порушень кібербезпеки. Більшість медичних працівників не мають належних знань у галузі інформаційних технологій чи кібербезпеки, але вони несуть відповідальність за оцінку того, які медичні пристрої забезпечують найкращий баланс ризику та ймовірності успіху. Система оцінювання також спирається на анкету безпеки, засновану на моделі STRIDE, яка допомагає створити оцінку ризику для медичного обладнання. Для демонстрації застосування та корисності системи оцінки ризику використовуються три тестові сценарії із застосуванням медичних пристроїв [29].

У статті [30] представлені аналітичні моделі оптимізації витрат на кібербезпеку фірми та кіберстрахування на основі ефективності витрат відповідно до зниження кіберзагроз, вразливості та впливу. На макрорівні стаття показує, як внесок приватного сектору у боротьбу з кіберзлочинністю може зменшити загальні кіберзбитки та створити економічну цінність. На мікрорівні ефективність фірми витрат на безпеку для подолання конкретних кіберзагроз може бути знижена, коли не будуть вжиті інші заходи, що залежать від безпеки. У статті виходить

оптимальний поєднання вкладень в кібербезпеку в «знання та досвід», а не в «вжиття заходів щодо пом'якшення наслідків». У роботі пропонується налаштувати кіберстрахування для фірм із деталізованим покриттям, що залежить від загрози, та часткою надбавки, яка використовується для того, щоб допомогти клієнтам, які знають про ризики, та підштовхнути клієнтів у здійсненні заходів щодо зменшення ризику. Малі та середні підприємства можуть отримати найбільшу вигоду від такого інноваційного страхування в кібер-умовах [30].

У статті [31] розглядають можливість визначити вразливість електричних кіберфізичних систем (CPS) шляхом поширення несправностей під час кібератаки. Спочатку пропонується модель поширення несправностей, головним чином з урахуванням впливу перебоїв на деяких вузлах кібермережі на електричні фізичні системи. По-друге, два графіки, тобто графік розповсюдження та графік атаки, пропонуються для виявлення механізмів розповсюдження фізичних несправностей та аналізу інтенсивності атаки комбінацій різних вузлів зв'язку відповідно. По-третє, набір традиційних вразливих індексів на основі графіків розповсюдження та атаки використовується для ідентифікації як критичних фізичних гілок, так і вузлів зв'язку в CPS. Нарешті, порівняльний аналіз із та без урахування CPS показує, що поширення несправностей серед більш складних та неправильних рішень, які приймає центр управління, викликає більшу вразливість електричної мережі через перерву інформації про передачу в кіберсистемі під дією кібератак [31].

У [32] зазначається, що традиційні рамки для оцінки ризиків не працюють добре для хмарних обчислень. Хоча останні роботи часто зосереджуються на ризиках, з якими стикаються фірми, які приймають або вибирають хмарні сервіси, мало досліджень про те, як хмарні провайдери можуть оцінювати власні послуги. У цій роботі автори використовують поглиблений огляд існуючої літератури, щоб висвітлити слабкі місця традиційних рамок оцінювання ризику для цього завдання. Використовуючи приклади, вони описують нову модель оцінки ризику (CSCCRA) та порівнюють її з трьома усталеними підходами. Для кожного підходу вони враховують його цілі, процес оцінки ризику, рішення, обсяг оцінки та спосіб

концептуалізації ризику. Ця оцінка вказує на необхідність динамічних моделей, спеціально розроблених для оцінки хмарного ризику. Пропозиції авторів щодо майбутніх досліджень спрямовані на вдосконалення виявлення, оцінки та зменшення взаємозалежних хмарних ризиків, властивих визначеному ланцюгу поставок [32].

У дослідженні [33] досліджено поточний стан та майбутній напрямок використання інформаційних систем управління ланцюгами поставок для компаній з багатокомпонентним виробництвом. У статті представлений якісний метод дослідження для аналізу процесів ланцюга поставок та визначення шляхів його інформаційного забезпечення. На основі даних, зібраних від різних підприємств, можна зробити висновок, що для виявлення найбільш ефективних стратегій інформаційного забезпечення ланцюга поставок увага повинна зосереджуватися на виявленні та управлінні джерелами невизначеності, ризиків та кібербезпеки. Для успішної інтеграції бізнес-процесів між постачальниками та замовниками виробники повинні вирішити складну проблему інформаційної безпеки. Таким чином у роботі запропонований новий підхід до виявлення та прогнозування ризику постачання в умовах невизначеності та запропоноване комплексне рішення щодо захисту даних в інформаційних системах управління ланцюгами поставок [33].

Велика кількість досліджень, наукових праць, у яких розглядається та аналізується сутність, зміст і типологія управлінських рішень в системі державного і муніципального управління [34-48].

У роботі [49] описано вплив злочинної діяльності, що ґрунтується на характері злочину, жертві та підставі (чи то короткострокової чи довгострокової / тривалості) впливу кіберзлочинності в Інтернеті. Останнім часом багато країн стикаються з численними кіберзагрозами, зокрема DoS (та DDoS), зловмисне програмне забезпечення, наклеп на веб-сайт, спам та фішинг- атаки на електронну пошту. У зв'язку з розвитком цих кіберзлочинів виявлення та оцінка ризику для безпеки має вирішальне значення для доступу до даних нових технологій, а також

намагання зрозуміти, як технологіями можна зловживати. Тому існує потреба розробити спеціальну модель оцінки ризиків кібербезпеки для вирішення цих кіберзагроз. У цій роботі автори пропонують використовувати модель нечітких висновків (FIS) для отримання результату оцінки ризику на основі чотирьох факторів ризику, які є: вразливістю, загрозою, ймовірністю та впливом для визначення кола ризиків, які можуть загрожувати будь-якій організації та намагатися вирішити такі питання пропонованим організаціям. Автори провели різноманітні аналізи щодо цих факторів і, нарешті, результати оцінювання показують життєздатність запропонованого нами підходу [49].

Робота [50] є першою з серії робіт про заходи ризику та уніфікацію економічної бази, що охоплює міждисциплінарну сферу «кіберноміки». Це також перший навчальний документ, який офіційно запропонував одиниці вимірювання кібер-ризику. У цій роботі використовуються мультидисциплінарні методології для застосування перевірених методів вимірювання ризику у фінансах та медицині для визначення нових одиниць ризику, що є центральними в кіберноміці. Використання встановлених одиниць ризику - MicroMort (MM) для вимірювання медичного ризику та Value-at-Risk (VaR) для вимірювання ринкового ризику - BitMort (BM) та hekla (названий на честь ісландського вулкана) визначаються як одиниці кібер-ризику. Методи та приклади обчислення ризику вводяться в цій роботі для вимірювання економічної ефективності факторів контролю, формулювання «готовності платити» (ціноутворення на ризик) для зниження кібернебезпеки, обмеження кібер-ризику та апетиту до кібер-ризику. Кіберноміка, побудована навколо БМ та Гекла, інтегрує управління кібер-ризиками та економіку для вивчення вимог банку даних з метою вдосконалення рішень щодо аналізу ризиків для: 1) оцінки цифрових активів; 2) вимірювання впливу ризику цифрових активів; 3) оптимізація капіталу для управління залишковим кіберризиком. Створення адекватних, цілісних та статистично надійних точок даних про сутність, портфоліо та глобальний рівень для розвитку банку даних з кіберноміки є важливим для стійкості нашого спільного цифрового майбутнього. У цій роботі пояснюється необхідність створення схем даних, таких як Міжнародна

класифікація цифрових активів (IDAC) та Міжнародна класифікація кібер-інцидентів (ICCI) [50].

Автор у [51] зазначає, що якщо ви будете шукати в Google термін "викупна програма", ви побачите дві речі. Перший - це визначення WannaCry, нападу викупного програмного забезпечення, яке 12 травня 2017 року поширилось по всьому світу та торкнулося сотні цілей, включаючи комунальні послуги, великі корпорації та, головне, покалічило NHS у Великобританії1. Але можна також побачити серію новин, і, незалежно від того, в який день ви вводите "викупницьку програму" на панель пошуку, ви, ймовірно, побачите історії про напади за кілька днів тому, або, в деяких випадках, лише кілька годин тому. Всі підприємства ризикують піддатися кібератакам, які занадто часто є успішними. Це пов’язано з нестачею бюджету чи бюджети витрачаються неправильно? Чи достатньо просто витратити більше грошей, щоб допомогти? Усі підприємства стикаються з бюджетним тиском - це означає, що вони повинні розуміти, як витратити свої бюджети розумно. І саме тут керовані постачальники послуг можуть відігравати вирішальну роль. Автор Тім Браун із SolarWinds пояснює, як забезпечити правильну комбінацію технологій та персоналу [51].

У відповідності з [52] власники критичної інфраструктури та оперативні критики завжди шукають способи мінімізувати кібер-ризик, зберігаючи при цьому витрати на кібербезпеку. Протягом сотень років страхова галузь кількісно оцінює ризик, щоб мінімізувати ризик та отримати максимальний прибуток. Для досягнення цих цілей страховики постійно збирають та аналізують статистичні дані для покращення їх прогнозів, стимулювання інвестицій клієнтів у самозахист та періодично вдосконалюють їх моделі для підвищення точності оцінок ризику. У цій статті представлено основу, яка включає принципи роботи страхової галузі для надання кількісних оцінок кібер-ризику. Автор використовує методи оптимізації, щоб запропонувати рівні інвестицій у кібербезпеку та страхування власників та операторів критичної інфраструктури. Цей аналіз може бути використаний для кількісного формулювання стратегій мінімізації кібер-ризику [52].

Дослідники у [53] зазначають, що кіберфізичні суспільства стають залежними від кібер-сфери у повсякденному житті. Оскільки кібервійни все більше стають частиною майбутніх конфліктів, потрібні нові та нові рішення для допомоги урядам у забезпеченні їх національної інфраструктури. Кібермиротворення - це одне таке рішення: виникає та багатодисциплінарна сфера досліджень, яка стосується технічних, політичних, урядових та суспільних областей думки. У цій статті автори спираються на попередні роботи, розвиваючи кібермиротворчу діяльність щодо спостереження, моніторингу та звітності. Вони застосовують практичний підхід: описуючи сценарій, за якого два кіберфізичні товариства відчувають негативні наслідки кібер-війни та вимагають кібер-експертизи для відновлення послуг, від яких залежать громадяни. Автори досліджують, як може розпочатися операція з підтримання кіберзахисту, і обговорюють проблеми, з якими вона зіткнеться. У статті подано низку пропозицій, включаючи використання віртуального середовища для спільної роботи для отримання багатьох переваг [53].

Кількісне емпіричне онлайн-дослідження [54] вивчало безпечну поведінку в Інтернеті та порівняння студентів у Великобританії та США, вимірюючи сприйняття ризику та інші виміри ризику. По-перше, сприйнятий ризик був найвищим для крадіжок особистих даних, кейлогерів, кібер-знущань та соціальної інженерії. По-друге, відповідно до існуючої теорії, важливими прогнозами сприйнятого ризику були добровільність, безпосередність, катастрофічний потенціал, боязнь, тяжкість наслідків та контролю, а також досвід роботи в Інтернеті та частота використання Інтернету. Більше того, контроль був важливим провісником запобіжної поведінки. Методологічні наслідки підкреслюють необхідність неокупного аналізу, а практичні наслідки підкреслюють повідомлення про ризики для користувачів Інтернету [54].

Велика кількість досліджень, наукових праць, у яких викладено основи методології та організації процесу розробки і реалізації управлінських рішень [55-69].

Технології Smart Grid [70] розробляються для модернізації електромережі за допомогою мережевої метрології та елементів управління, які дозволяють підвищити ефективність та запропонувати нові методи управління системою. Незважаючи на те, що ці технології пропонують великі переваги, вони також впроваджують нові класи ризику, особливо, створюючи нові вектори атак, які можуть бути використані кібератакою. Для оцінки та подолання ризиків у таких кіберфізичних системах, набір інструментів дизайнера системи повинен включати концепції, засновані на кібербезпеці, надійності та конструкції стійкості до відмов, інтегрованих у загальну методологію. У цій роботі обговорюється фрагментарний пейзаж досліджень ризику кібер-атаки на інтелектуальні системи вимірювання, а потім спираємось на концепції з інженерії систем та проектування відмов, щоб організувати та уніфікувати деталі [70].

Кібербезпека є важливим питанням у галузі ядерної інженерії [71], оскільки ядерні об'єкти використовують цифрове обладнання та цифрові системи, які можуть призвести до серйозних небезпек у разі аварії. Регулюючі агенції по всьому світу оголосили вказівки щодо кібербезпеки, пов'язані з ядерними питаннями, включаючи Посібник з регулювання норм NRC в США

Важливо оцінити ризик кібербезпеки відповідно до цих нормативних посібників. У цьому дослідженні автори пропонують модель оцінки ризику кібербезпеки для ядерних приладів та систем управління з використанням байєсівської мережі та дерев подій. Оскільки складно виконати тести на проникнення в системи, модель оцінки може інформувати про дослідження кіберзагроз для систем кібербезпеки ядерних установок шляхом використання попередньої, зворотної інформації та розрахунків зворотного розповсюдження. Крім того, пропонується методологія застосування аналітичних результатів з байєсівської моделі мережі до моделі дерева подій, яка є імовірнісним методом оцінки безпеки. Запропонований метод дозволяє зрозуміти ризики безпеки та кібербезпеки [71.

У дослідницькій роботі [72] автори розробили новий нечіткий логічний контролер інтервалу типу 2 (IT2FLC) для вдосконалення моделі оцінки ризиків для кібербезпеки. Запропонований IT2FIS реалізує цю модель для отримання загального ризику для такої системи кібербезпеки, яка поєднується з трьома підмоделями, як: а) загальна спроможність, яка контролюється можливостями, наміром, б) загальною вірогідністю, що залежить від вразливості, загалом здатності та нарешті в) ризик, який вимірюється загальною вірогідністю, впливом. Комбінуючи ці три підмоделі, ми сформулювали та оптимізували загальну оцінку ризику для кібербезпеки. Цей підхід матиме розширений контроль для прогнозування можливості оцінки ризику кібербезпеки, незважаючи на невизначеність даних та інформації про кібербезпеку через різні ризики, спричинені наслідками злочинної діяльності залежно від видів правопорушення, жертви та походження наслідків кіберзлочинності. Нарешті, обґрунтованість запропонованої моделі обговорюється за допомогою статистичного аналізу, адаптивного нейро-нечіткого висновку (ANFIS) та множинної лінійної регресії (MLR) [72].

Автори статті [73] стверджують, що держави, які використовують кіберпроксі, стикаються із схожими дилемами. По-перше, уряди ризикують прометейською дилемою, коли вони оснащують кіберпроксі інструментами, які можуть бути проти них. По-друге, уряди ризикують дилемою ненавмисного загострення кризи шляхом надання повноважень проксі-сервісам з більш розширеними або менш стриманими політичними програмами, які можуть перевищувати їхні мандати. У роботі досліджується, як держави можуть управляти ризиками, пов'язаними з цими дилемами, та умовами, за яких вони, ймовірно, можуть дати відсіч [73].

Автори у роботі [74] зазначають, що кібербезпека стосується захисту підключених до Інтернету систем, таких як апаратне забезпечення, програмне забезпечення, а також дані (інформація) від кібератак (супротивників). Регулювання кібербезпеки необхідне для захисту інформаційних технологій разом

з комп'ютерними системами з метою примусити різні організації, а також компанії захищати свої системи та інформацію від кібератак. Можливі кілька кібератак, таких як віруси, фішинг, троянські коні, глисти, напади на заборону обслуговування (DoS), незаконний доступ (наприклад, крадіжка інтелектуальної власності або конфіденційної інформації), а також напади на систему контролю. У цій статті автори акцентують увагу на важливості різних стандартів в кіберзахисті та архітектурі кібербезпеки, обговорюють загрози безпеці, атаки та заходи в галузі кібербезпеки. Також обговорюють різні проблеми стандартизації в галузі кібербезпеки, національну стратегію кібербезпеки для забезпечення кіберпростору, а також різні урядові політики щодо захисту кібербезпеки. Нарешті, надають деякі рекомендації, які мають вирішальне значення для кібербезпеки та кіберзахисту [74].

У травні минулого року уряд Великобританії повідомив [75], що дві третини великого бізнесу країни зазнали кібератаки протягом попередніх 12 місяців. Тому не дивно, що кібербезпека є на порядку денному для уряду - підкреслено нещодавніми інвестиціями в розмірі 1,9 млрд. фунтів стерлінгів у п'ятирічну стратегію кібербезпеки, яка була розпочата в лютому 2017 року з офіційним відкриттям Національного центру кібербезпеки. Нещодавно уряд Великобританії повідомив, що дві третини великого бізнесу країни зазнали кібератаки протягом попереднього року. Тож не дивно, що кібербезпека належить до порядку денного уряду. У статті зазначається, що кібербезпеку потрібно використовувати в усіх куточках кожної урядової організації. Від управління фінансами до найменших працівників, кожен повинен відігравати свою роль у забезпеченні безпечної та безпечної урядової інфраструктури. Джо Кім з Solar Winds розглядає деякі кроки, які можуть зробити державні IT- команди, щоб допомогти захистити свої організації від рішучих кібер- злочинців, які шукають вигідну оплату праці [75].

Велика кількість досліджень, наукових праць, у яких особливу увагу приділено прийомам розробки і вибору управлінських рішень в умовах

невизначеності і ризику, аналізу факторів якості та ефективності управлінських рішень в органах влади і управління [76-90].

У статті [91] розглядається стан сучасних оцінок ризику кібербезпеки систем нагляду та контролю даних (SCADA). Автори вибрали та детально дослідили двадцять чотири методи оцінки ризику, розроблені для або застосовуються в контексті системи SCADA, описали суть методів, а потім проаналізували їх з точки зору мети; домен програми; розглянуті етапи управління ризиками; охоплені ключові концепції управління ризиками; вимірювання впливу; джерела імовірнісних даних; оцінка та підтримка інструментів. На основі проведеного аналізу запропоновано інтуїтивну схему класифікації методів оцінки ризиків кібербезпеки для систем SCADA, а також окреслено п'ять наукових проблем, які стоять перед цією областю, і вказано на підходи, які можна використовувати [91].

У [92] зазначається, що промислова система управління (ICS) - це паралельний термін, що відноситься до групи технологій автоматизації процесів, таких як системи нагляду та збору даних (SCADA) та розподілені системи управління (DCS), на які, на жаль, зазнали зростаючої кількості атак в останні роки. Оскільки вони надають життєво важливі послуги критичній інфраструктурі, такі як комунікації, виробництво та енергетика серед інших, ворожі зловмисники, які здійснюють напади, становлять серйозну загрозу для щоденного управління національними державами. ICS мають унікальні вимоги до продуктивності та надійності і часто використовують операційні системи, додатки та процедури, які сучасні IT-фахівці можуть вважати нетрадиційними. Ці вимоги, як правило, відповідають пріоритету доступності та цілісності, з подальшим конфіденційністю та включають управління процесами, які, якщо виконуються неправильно, становлять істотний ризик для здоров'я та безпеки людського життя, шкоди навколишньому середовищу, а також серйозні фінансові такі питання, як втрати виробництва. Недоступність критичної інфраструктури (наприклад, електроенергія, транспорт) може мати економічний вплив далеко за межі систем, що зазнають прямого та фізичного пошкодження. Ці наслідки можуть негативно

вплинути на місцеву, регіональну, національну чи, можливо, глобальну економіку [92].

Система аналізу та оцінки ризиків кібербезпеки (CSRAS) була розроблена як інструмент для аналізу вимог безпеки та технічного контролю безпеки на основі загальної процедури оцінки ризику кібербезпеки з урахуванням характеристик систем ІС [93].

Кібербезпека є актуальною проблемою безпеки в ядерній промисловості, особливо в галузі приладів та контролю [94]. Для систематичного вирішення проблеми кібербезпеки потрібна модель, яка може бути використана для оцінки кібербезпеки. У цій роботі запропоновано модель ризику кібербезпеки, засновану на байєсівській мережі, для комплексного оцінювання кібербезпеки ядерних об'єктів. Запропонована модель дає змогу оцінювати як процедурні, так і технічні аспекти кібербезпеки, які пов'язані з дотриманням норм керівництва та архітектури системи відповідно. Модель аналізу якості діяльності була розроблена для оцінки того, наскільки люди та / або організації відповідають нормативним рекомендаціям, пов'язаним з кібербезпекою.

Модель аналізу архітектури була створена для оцінки вразливості та заходів пом'якшення наслідків щодо їх впливу на кібербезпеку. Дві моделі об'єднані в єдину модель, яку називають моделлю ризику кібербезпеки, щоб кібербезпеку можна було оцінити одночасно з процедурних та технічних точок зору. Модель застосовувалася для оцінки ризику кібербезпеки системи захисту реактора дослідницького реактора та для демонстрації його корисності та доцільності [94].

У критичних для безпеки інфраструктурах, таких як атомна електростанція (АЕС), кібератака може мати серйозні наслідки через ініціювання небезпечних подій або виведення важливих систем безпеки [95]. Завдяки застосуванню цифрових технологій до критичних для безпеки інфраструктури кібер-атаки стали однією з нових небезпечних загроз. Оскільки кібератака проводиться навмисно, слід розглянути численні можливі випадки розвитку системи кібербезпеки, такі як

шляхи, методи та потенційні цільові системи атаки. Тому, перш ніж розробляти стратегію кібербезпеки, поінформовану про ризик, слід проаналізувати важливість кібератак та значних критичних цифрових активів (CDA). У роботі [95] запропоновано метод аналізу важливості кібератак на АЕС, використовуючи метод ймовірнісної оцінки безпеки (PSA). Для розробки структури аналізу важливості для кібератак були визначені можливі кібератаки з режимами відмов, а також була розроблена модель PSA для кібератак. Для практичних досліджень кількісні оцінки сценаріїв кібератаки проводилися за пропонованим методом. Використовуючи кількісну важливість кібератак та виявляючи значні CDA, які потрібно захищати від кібератак, можна розробити ефективну та надійну оборонну стратегію проти кібератак на АЕС [95].

Після аварії Фукусіма-Даїчі в 2011 році ризик, що виникає через багато енергоблоків, тобто ризик через декілька атомних електростанцій (АЕС) на ділянці, став важливим питанням у кількох країнах, таких як Корея, Канада та Китай [96]. Однак багатоядерний ризик тривалий час обговорювався в ядерній спільноті до того, як сталася ядерна аварія Фукусіма-Даїчі. Регулюючі органи у всьому світі та міжнародні організації запропонували вимоги або вказівки щодо зменшення ризику, що складається з різних одиниць. Побоювання, пов'язані з ризиком, пов'язаним з кількома одиницями, можна узагальнити в трьох наступних питаннях:

- наскільки аварія АЕС на ділянці впливає на безпеку інших АЕС на тому ж майданчику?
- який загальний ризик ділянки з багатьма АЕС?
- чи буде ризик одночасних аварій на декількох АЕС на ділянці, наприклад, аварії Дакуї Фукусіма?

Багатоодинична оцінка ризику (MURA) в комплексній структурі - це практичний підхід для отримання відповідей на вищезазначені питання. Незважаючи на те, що до ядерної аварії Фукусіма-Даїчі мало ядерних досліджень, які мають оцінити ризик багато одиниць, все ще існує кілька питань, які мають бути

вирішені, щоб виконати повну оцінку ризику. Ця стаття[96] спрямована на те, щоб надати огляд проблем, пов'язаних із ризиком, що складаються з різних одиниць, та його оцінку. Автор обговорює декілька найважливіших питань у поточній оцінці ризику, щоб отримати корисну інформацію про багатоодиничний ризик із сучасними технологіями оцінювання безпеки (PSA). Також розглядаються якісні відповіді на вищезазначені питання [96].

Відповідні стратегії реагування на нові і постійні кібератаки повинні бути в змозі знизити ризики до прийнятного рівня, не жертвуючи місією для безпеки [97]. Існуючі підходи або оцінюють вплив, не враховуючи негативних побічних ефектів місії, або будуються вручну на основі традиційних оцінок ризику, не залишаючи осторонь технічних труднощів. У цій роботі запропоновано динамічну систему реагування на ризик-менеджмент (DRMRS), що складається з активного та реактивного програмного забезпечення для управління, спрямоване на автоматичне оцінювання сценаріїв загроз, а також передбачення виникнення потенційних атак. Автори застосовують кількісний підхід, орієнтований на ризик, який забезпечує комплексний огляд загроз, враховуючи їх вірогідність успіху, спричинений вплив, вартість можливих реакцій та негативні побічні ефекти відповіді. Відповіді вибираються та пропонуються операторам на основі оцінок фінансових, операційних та загроз. DRMRS застосовується до реального дослідження випадку критичної інфраструктури з кількома сценаріями загрози [97].

Критичні інфраструктури, що мають важливе значення для нашого сучасного життя, такі як електромережі та водяні насоси, контролюються системами нагляду та збору даних (SCADA) [98]. За останні два десятиліття підключення критичної інфраструктури до Інтернету стало надзвичайно важливим завдяки продуктивності та комерційним потребам. Поєднання підключень до Інтернету до систем з малою мірою захисту, а також той факт, що безпека через незрозумілість вже не працює, перенесла тему безпеки SCADA на перший план в останні кілька років. Для вирішення цих викликів у роботі [98] пропонуються методи виявлення кібератаки

на основі розпізнавання тимчасового шаблону. Методи розпізнавання тимчасових шаблонів не тільки шукають аномалії в даних, що передаються компонентами SCADA по мережі, але й шукають аномалії, які можуть виникнути шляхом неправильного використання законних команд, таким чином, що несанкціоновані та неправильні інтервали часу між ними можуть калічити систему. Зокрема, автори пропонують два алгоритми на основі прихованих моделей Маркова (HMM) та штучних нейронних мереж (ANN). Оцінюють алгоритми за реальними та імітованими даними SCADA за допомогою п'яти різних методів вилучення функцій; в кожному методі алгоритми враховують різні аспекти необроблених даних. Результати показують, що методи розпізнавання тимчасових шаблонів, особливо ті, що базуються на вилученні часових особливостей, можуть виявляти кібератаки, в тому числі ті, що передбачають законні функції, які відомі в літературі як важко виявити [98].

Дослідники широко визнають загрозу для систем управління промисловістю (ICS) від кібератак [99]. Оператори ICS прагнуть вирішити ці загрози ефективно та з урахуванням витрат, які не піддають своїх операцій додатковим ризикам шляхом інвазивного тестування. Хоча існуючі стандарти та вказівки пропонують вичерпні поради щодо перегляду безпеки інфраструктури ICC, обмеження ресурсів та часу може призвести до неповних оцінок або небажано довгих графіків виконання контрзаходів. У статті [99] розглядається проблема проведення ефективних оцінок ризику кібербезпеки та здійснення пом'якшення наслідків у великих, встановлених операціях ICS, для яких повний огляд безпеки не може бути здійснений у обмежений термін. Внесок - процес протидії кіберзахисту захищеної системи промислового управління (ICS-CDTP). ICS-CDTP визначає пріоритетні райони, де вплив атак найбільший, і де початкові інвестиції швидко зменшують загальну експозицію організації. ICS-CDTP розроблений як попередник більш широкого цілісного огляду впродовж усієї операції, дотримуючись встановлених підходів до управління безпекою. ICS-CDTP - це нова комбінація діамантової моделі аналізу на вторгнення, життєвого циклу атаки та матриці CARVER, що дозволяє ефективно тиражувати вектори атаки та ймовірні цілі для дієздатного антагоніста. ICS-CDTP

визначає та фокусує увагу на ключових процесах ICS та їх впливі на кіберзагрози з метою підтримки критичних операцій. У статті визначено ICS-CDTP та наводиться приклад його застосування за допомогою фіктивного очищення води та пояснюється його оцінка як частина масштабної серйозної гри [99].

Інфраструктури морських портів покладаються на використання інформаційних систем для співпраці, тоді як важливою частиною співпраці є забезпечення кіберзахисту цих систем [100]. Аналіз графіків атак та оцінка ризику надають інформацію, яку можна використовувати для захисту активів мережі від кібератак. Крім того, графіки атак забезпечують функціональність, яку можна використовувати для виявлення вразливих ситуацій в мережі та їх використання потенційними зловмисниками. Існуючі методи генерування графіків атак неадекватні для задоволення певних вимог, необхідних в динамічному середовищі управління ризиками ланцюгів постачання, оскільки вони не враховують змінні, що допомагають досліджувати конкретні мережеві частини, що задовольняють певним критеріям, таким як точки входу та цілі, довжина поширення а також місцезнаходження та можливості потенційного зловмисника. У статті [100] автори представили метод виявлення шляху кібер- атаки, який використовується як складова системи управління морськими ризиками. Метод використовує обмеження та глибинний пошук, щоб ефективно генерувати графіки атак, які зацікавлені адміністратором [100].

Велика увага приділяється питанням інформаційної безпеки в галузі економіки, викликів оптимізації витрат на управління кібер-ризиками, викликів у кількісному оцінці витрат на безпеку, викликів у визначенні оптимального рівня інвестицій у безпеку та ризики та інвестиції в кібербезпеку [101]. У роботі представлені сучасні моделі оптимізації витрат на кібер-ризики, моделі витрат для прогнозування та моделі витрат на інвестиції, тобто визначають, скільки потрібно витратити на кібер-ризик, включаючи рентабельність інвестицій в безпеку (ROSI), чисту присутність вартості (NPV), та внутрішня норма прибутку (IRR). У роботі приводяться моделі прийняття рішень щодо оптимальних стратегій управління

ризиками, тобто коли буде досягнута точка зменшення рентабельності інвестицій в кібер-ризики [101].

Велика кількість досліджень, наукових праць, у яких розглянуто напрями вдосконалення процесу розробки та прийняття управлінських рішень на основі застосування інформаційно-комунікативних технологій [102-116].

Порушення кібербезпеки негативно впливають на норму прибутку, ринкову капіталізацію та імідж фірми [117]. Глобальні організації вдаються до використання технологічних пристроїв для зменшення частоти порушень кібербезпеки. Щоб мінімізувати вплив фінансових втрат від порушень кібербезпеки, автори [117] радять використовувати продукти кіберстрахування. У цій статті пропонуються моделі, які можуть допомогти фірмам визначитися з корисністю продуктів кіберстрахування, пропонується мережу байєсівської віри (CBBN) для оцінки кіберзахищеності та розрахунку очікуваних втрат. Беручи це за основу і використовуючи концепції теорії колективного моделювання ризиків, автори також розраховують кошти, які може стягувати страховик кібер-ризику для відшкодування кібер-збитків. Крім того, для надання допомоги страховикам з кібер-ризику та ефективного проектування продукції пропонується модель пільгового ціноутворення (UBPP) на основі корисних послуг. UBPP враховує профілі ризику та багатство потенційної страхової фірми перед тим, як запропонувати премію [117].

Було здійснено чимало зусиль та досліджень для підвищення безпеки критичної інфраструктури, зокрема [118]. Як одне із зусиль, було створено численні оперативні центри безпеки (SOC) для захисту від кібератак. На жаль, захистити від кібератак занадто важко, оскільки є занадто багато подій безпеки для аналізу та реагування на них. Зменшення подій у сфері безпеки є дуже важливим для підвищення ефективності реагування на інциденти. У роботі[118] автори вивчали кіберзагрози проти корейських електроенергетичних компаній, аналізуючи вихідні дані. В результаті цього аналізу було виявлено, що 95% усіх кібератак походили від іноземних країн. Якщо IT-система не пов’язана із

закордонним бізнесом, слід подумати про блокування непотрібних зовнішніх діапазонів IP. Автори запропонували модель посиленого контролю безпеки (ESC) з процесом блокування пріоритетності (BP) для критичних інфраструктур для покращення щоденних заходів щодо реагування на інциденти. Ця модель має процес блокування пріоритетності із шістьма факторами, які слід враховувати, вирішуючи, які IT-системи блокувати від зовнішніх діапазонів IP: зовнішнє відношення, реальний вхід, складність блокування, толерантність до зупинки, зовнішнє відношення та вплив зупинки. Враховуючи ці шість факторів, модель ESC може дати можливість встановити пріоритет ступеню блокування впливу (BID) IT-систем і допомогти прийняти рішення щодо блокування від непотрібних зовнішніх діапазонів IP. Ця модель ESC зменшить події в галузі безпеки та покращить умови концентрації на решті незаблокованих та важливих IT-систем [118].

Як уже зазначалося вище, на даний час кібербезпека є серйозною проблемою не тільки для систем автоматизації офісу, але і для систем промислового управління (ICS) [119]. Якщо ICS піддаються кібератаці, можуть статися серйозні аварії, такі як вибухи та витоки шкідливих речовин. Тому, кібербезпека є дуже важливим фактором обговорення безпеки та не повинна розглядатися окремо. Як правило, аналіз ризиків проводиться на етапі проектування та експлуатації установки, щоб уникнути ризику експлуатації систем промислового управління. Однак, оскільки традиційні методи аналізу зосереджені на «обладнанні» та «продуктах» заводу, важко розглянути систему верхнього шару. У статті автори пропонують оцінку ризику для безпеки, щоб можна було пов'язати фізичні процеси та системи промислового управління. Автори запропонували метод аналізу ризиків з використанням теоретичної моделі аварійних систем та процесів (STAMP) [119].

Зростає усвідомлення того, що ідентифікація ризику відіграє важливу роль у дослідженні фактичної та потенційної шкоди пацієнтам [120]. Хоча сучасні методи ідентифікації ризику в охороні здоров'я мають сильні сторони та обмеження, відкритим питанням є те, чи були вони реалізовані оптимально та наскільки добре

вони інтегровані для забезпечення повної картини ризику в складних системах охорони здоров’я. Щоб висвітлити це, у статті [120] розглядаються характеристики методів реактивної та проактивної ідентифікації ризиків, а також їх вплив на практику ідентифікації ризиків. Виявлені різні точки навчання з інших галузей, що мають важливе значення для безпеки, і обговорюється інтеграція декількох методів, щоб забезпечити більш всебічний вигляд у сфері управління ризиками. Як особливий приклад, у цій статті розглядається прогностичний метод, розроблений командою майбутньої авіаційної безпеки (FAST), щоб покращити ідентифікацію існуючих ризиків в авіаційній галузі, шляхом виявлення ризиків, які виникають через майбутні зміни. Метод FAST також демонструє інтеграцію методів ідентифікації ризиків, пропонуючи чотири взаємодоповнюючих підходи для використання в авіаційній галузі. Дослідження забезпечує концептуальні рамки, які можуть бути використані в охороні здоров'я для інтеграції декількох методів для прискорення покращення безпеки пацієнтів за допомогою комплексного охоплення системи [120].

У проблемах з оцінкою ризику безпеки часто залучаються численні експерти та декілька критеріїв, а дані оцінки часто даються у вигляді інтервальних чисел [121]. У роботі, в основному, пропонується новий метод побудови матриці ризиків для оцінки ризиків для безпеки в нафтовій і газовій промисловості. Для кращої оцінки ризиків у цій роботі пропонується визначення номера інтервалу з функцією розподілу та функцією корисності. Частота та наслідок ризику - лише два необхідні показники в матриці ризику, і їх значення потрібні у вигляді чітких значень. Таким чином, в цій роботі будується багатоекспертний та багатокритеріальний інформаційний синтез на основі моделі інтервальних номерів (MEMCIF-IN). По-перше, побудована багатоекспертна та багатокритеріальна модель синтезу для об'єднання окремих інтервальних чисел у колективне інтервальне число та інтеграції декількох критеріїв у комплексний індекс. У моделі синтезу ваги експертів з оцінки розраховуються виходячи з об'єктивних ваг та суб'єктивних ваг одночасно, а інформація про окремі інтервальні числа зберігається без втрати інформації у кінцевому результаті. По-друге, пропонується оператор безперервної

зваженої впорядкованої зваженої сукупності (C-WOWA). В операторі C-WOWA одночасно враховуються ваги позиції, які генеруються функцією корисності, і значення ваг, які генеруються функцією щільності ймовірності. Вагові позиції в операторі C-WOWA можуть виправити вплив на позиції експертів щодо ризику, а значення ваг можуть відображати важливість самих точок в інтервальному числі. Нарешті, матриця ризику будується, щоб показати, який ризик високий, а який низький. Крім того, реалізовано додаток, яке показує практичність та раціональність запропонованого способу [121].

Функціонування систем з багатьма водоймами у реальному часі є життєво важливим питанням у галузі управління водоймищами [122]. Невизначеність, спричинена прогнозуванням притоку, означає, що аналіз ризику необхідний для такої операції в режимі реального часу. Однак різниці у тривалості прогнозних періодів для різних водойм у системі рідко враховуються при аналізі ризиків для багатьох водосховищ. У цій статті [122] представлений двоступеневий метод аналізу ризику затоплення систем, який враховує різницю в тривалості прогнозного періоду проживання. Метою запропонованого методу є оцінка невизначеності прогнозування повеней шляхом поділу горизонту експлуатації на прогнозний час очікування та поза прогнозний період часу. Ризик у межах прогнозованого часу оцінюється шляхом підрахунку частоти відмов серед усіх сценаріїв за допомогою прогнозів на основі сценарію. Ризик, що перевищує прогнозний часовий період, визначається за допомогою маршрутизації заплави пластів з проектними гідрографами повені, які вибираються відповідно до різниці тривалості прогнозних періодів між будь-якими двома водоймами. Запропонований двоступеневий метод аналізу ризику перевіряється за допомогою методу стохастичного моделювання на основі вибірки Монте- Карло. Модель операції боротьби з паводком у режимі реального часу встановлюється шляхом використання запропонованого двоступеневого методу аналізу ризиків як обмеження. Запропонований метод розширює наше розуміння управління ризиками для операцій з контролю затоплення в режимі реального часу в системах з багатьма водоймами [122].

Інтеграція обчислювальних і комунікаційних можливостей з електромережою призвела до численних уразливості в кіберфізичній системі (CPS) [123]. Ця загроза кібербезпеці може суттєво вплинути на фізичну інфраструктуру, економіку та суспільство. У традиційних IT-середовищах вже існує безліч випадків нападу, що демонструє, що несанкціоновані користувачі мають можливість доступу та маніпулювання конфіденційними даними із захищеного мережевого домену. Електромережі також сильно прийняли інформаційні технології (IT) для виконання завдань контролю, моніторингу та обслуговування в реальному часі. У статті [123] представлено сучасні найбільш релевантні дослідження кібербезпеки в енергосистемах. У ній розглядається дослідження, яке демонструє ризики кібербезпеки та розробляє рішення для підвищення безпеки електромережі. Для досягнення цієї мети висвітлено: опитування сучасних технологій інтелектуальної мережі, практики та стандарти енергетики, рішення, що стосуються питань кібербезпеки, огляд існуючих тестових панелей CPS для дослідження кібербезпеки та невирішені проблеми кібербезпеки. Дослідження кібербезпеки енергомережі було проведено в Державному університеті штату Вашингтон (WSU) з тестовою панеллю CPS- обладнання в циклі. Крім того, показано, як запропоновані системи можуть бути розгорнуті для захисту електромережі від кібер-зловмисників [123].

Цілісна оцінка ризиків кібербезпеки є складною багатокомпонентною та багаторівневою проблемою, що включає апаратні, програмні, екологічні та людські фактори [124]. У рамках постійних зусиль з розробки цілісної, прогнозної моделі оцінки ризиків кібербезпеки необхідна характеристика людських факторів, що включає поведінку людини, щоб зрозуміти, як дії користувачів, захисників та зловмисників впливають на ризик кібербезпеки. Робоча група, що розробляли цю нову модель та метод оцінки кібербезпеки, вирішила розрізняти довіру та впевненість, використовуючи «довіру» лише для людських факторів, та «впевненість» для всіх нелюдських факторів (наприклад, апаратного та програмного забезпечення) для того, щоб зменшити плутанину між двома поняттями в цій моделі. Автори розробили початкову основу для того, як включити довіру як фактор / параметр у більш широку характеристику впливу людини

(користувачів, захисників та зловмисників) на ризик кібербезпеки. Довіра до людських факторів складається з двох основних категорій: притаманні їм характеристики, те, що є частиною особистості, і ситуативні характеристики, те, що знаходиться поза людиною. Використання довіри як людського чинника в цілісній оцінці ризику кібербезпеки також залежатиме від розуміння того, як різні ментальні моделі та позиції ризику впливають на рівень довіри, що надається людині, і на упередження, що впливають на здатність надавати довіру [124].

Важливе значення має співвідношення характеристики людини з намірами поведінки в кібербезпеці [125]. Автори представляють всебічне дослідження, яке вивчає, як переваги прийняття ризику, стилі прийняття рішень, демографічні ознаки та особливості особистості впливають на поведінку безпеки на захист пристрою, пароль покоління, активна обізнаність та оновлення. Було проведено опитування 369 студентів, викладачів та співробітників у великому державному університеті та виявили, що індивідуальні відмінності становлять 5% -23% відхилення в намірах поведінки в кібербезпеці. Такі характеристики, як прийняття фінансових ризиків, раціональне прийняття рішень, екстраверсія та гендерна ознака, були визнані важливими унікальними прогнозами гарної поведінки в безпеці. Дослідження виявило як валідацію, так і протиріччя супутньої роботи на додаток до пошуку раніше не повідомлених кореляцій. Показано, як вплив індивідуальних відмінностей на наміри поведінки в безпеці може бути специфічним для навколишнього середовища. Таким чином, деякі рішення щодо безпеки повинні також залежати від навколишнього середовища [125].

Ключовим елементом удосконалення є визнання важливості поведінки людини під час проектування, побудови та використання технології кібербезпеки [126]. У статті автори описують, чому включення розуміння поведінки людини в продукти та процеси кібербезпеки може призвести до більш ефективної технології. Наведено два приклади: перший демонструє, як використання науки про поведінку призводить до явних поліпшень, а другий ілюструє, як поведінкова наука пропонує потенціал для значного підвищення ефективності кібербезпеки. На основі

зворотного зв'язку, зібраного практикуючими на попередніх інтерв'ю, увага акцентується на двох важливих поведінкових аспектах: когнітивне навантаження та упередженість. Далі визначаються перевірені та потенційні результати науки про поведінку, які мають значення для кібербезпеки, пов'язані не лише з когнітивним навантаженням та упередженістю, але й з евристикою та моделями науки про поведінку [126].

Перехід від послідовної комунікації «точка до точки» до мереж традиційних інформаційних технологій (IT) створив нові проблеми в забезпеченні кібербезпеки для систем контролю та збору даних (SCADA) в критичній інфраструктурі [127]. Поточні дослідження ландшафту атаки для критичної інфраструктури зосереджені на атаках, що базуються на IT, або на протоколах. Тим не менш, обмежений фокус на дослідженні на «більшій картині», поєднанні IT-атак та критичних інфраструктурних протокольних атак та мало уваги до кібератак, спрямованих на всю критичну інфраструктурну систему на базі SCADA. Через такі вузькі дослідження виникає повна відсутність уваги при осмисленні повномасштабних кібератак на критичні інфраструктурні системи на базі SCADA. Як результат, нові атаки, що поєднують різні вразливості в інженерних системах та IT-системах, ще не розкриті. У роботі [127] автори зіставили наявні відомі атаки, виявили та об'єднали існуючий діапазон ландшафтів атаки, розширили та «заповнили прогалини» у ландшафті, тим самим представивши повну структуру кібератаки, яка сприймає напади на всю критичну інфраструктуру на базі SCADA. Ця структура визначає чотири типи атак, традиційні атаки на основі IT, атаки, характерні для протоколу, атаки на основі конфігурації та атаки управління процесом, що дозволяє нам описати практичні атаки. Перевага розпізнавання діапазону атак на цілі критичні системи полягає в тому, що це дозволяє захищатись від атак із значно більшою ефективністю та інтелектом [127].

Уразливості програмного забезпечення є однією з головних недоліків системи інформаційних технологій (IT) в аспекті кібербезпеки, і, на сьогодні, консолідовані офіційні дані, наприклад, словник загальної експозиції вразливостей

(CVE) [128]. Ця інформація разом з ідентифікацією систем пріоритету для захисту дозволяє перевіряти структуру мережі та найбільш ймовірні шляхи, на які зловмисник, ймовірно, слідує, щоб досягти розумних ресурсів, основною метою виявлення відповідних дій, що знижують ризик кібер-атаки. Деякі з цих дій можуть бути застосовані без подальшої затримки, деякі з них, натомість, означають високий оперативний вплив на організацію бізнесу, що робить їх використання зручним лише тоді, коли атака дійсно актуальна. Справа з цим питанням особливо складна у контексті критичної інфраструктури, де, навіть якщо патчі є, обмеження місії організації створюють перешкоди для їх прямого застосування. У цьому випадку оператори безпеки змушені мати справу з відомими вразливими місцями, які неможливо виправити, і вони витрачають значні зусилля на проактивний аналіз, розробляючи контрзаходи, які можуть знизити вплив можливої атаки. У цьому документі представлено багатоступеневе рішення для візуальної аналітики кіберзахисту (MAD), спрямоване на те, щоб допомогти операторам безпеки в поліпшенні їхньої мережевої безпеки шляхом аналізу можливих атак та виявлення відповідних контрзаходів. Більше того, під час нападу система візуально представляє оператору безпеки відповідні відомості, що дозволяють краще зрозуміти стан атаки та його ймовірний розвиток, щоб прийняти рішення щодо можливих контрзаходів [128].

У роботі [129] представлені основні положення запропонованого методу ймовірнісного оцінювання ризику ІБ і визначено зміст етапів розв'язання задачі оцінювання. В основу методу покладено подієво-логічний підхід, що отримав назву загального логіко-імовірнісного методу. При розробці пропонованого методу використані основні положення методу і поняття, що стосуються визначення найкоротших шляхів розвитку небезпеки і мінімальних перетинів її запобігання, а також функції небезпеки. Крім того, у роботі розкрито методику ЛВ-моделювання сценаріїв ситуацій ризику ІБ, на прикладі дослідження трьох класів атак, пов'язаних з порушенням конфіденційності, цілісності та доступності інформації в інфокомунікаційній системі, а саме: атак на основі несанкціонованого збору інформації про сегменти системи; атак, спрямованих на генерування і подальше

впровадження нових об'єктів мережевої взаємодії в сегменти системи; атак, спрямованих на виведення з ладу мережевих пристроїв (DoS-атак). Також, у роботі показаний ітераційний процес побудови ДС ІБ, заснований на дослідженні характеристик атак: способів і об'єктів реалізації, шляхом синтезу функціонального та системного ДС. Обґрунтовано концепцію реалізації запропонованого методу в рамках продукційної експертної системи. У другій частині показані особливості побудови бази знань і розроблені алгоритми роботи інтерпретатора експертної системи [129].

В розглянутих джерелах описується суть методів, розглядаються етапи управління ризиками, запропонована схема класифікації методів ризиків кібербезпеки для SCADA систем. Досліджено широкий спектр загроз, які призводять до ризику кібербезпеки, створено базу даних фактичних втрат у випадку реалізації цих загроз, здійснено аналіз втрат з використанням методів статистики та актуарної математики. Розроблені структури для розрахунку кількісних оцінок ризиків кібербезпеки. Розглядаються моделі оцінювання ризиків кібербезпеки з використанням апарату нечіткої логіки, нові метрики ризику, основані на адаптації існуючих методів розрахунку ризиків і невизначеностей, таксономічна класифікація вимог до оцінювання ризиків кібербезпеки, досліджуються модель оцінювання ризику кібербезпеки для пристроїв і систем управління ядерних установок з використанням Байєсовської мережі, дерева подій, ймовірнісного методу оцінювання ризику кібербезпеки.

Дослідження існуючих методів оцінювання ризиків (табл. 1.1) дало можливість встановити, що практично всі досліджені методи дозволяють здійснювати оцінювання ризиків на технічному рівні, в процесі оцінювання пропонуються способи протидії ризикам, а також заходи по запобіганню та виявленню ризиків.

Таблиця 2.1 — Зведені дані методів оцінювання ризиків

	Критерії

Метод	Можливість ідентифікації ризику	Можливість визначення наслідків	Визначення ймовірності	Можливість визначення рівня	Можливість оцінювання ризику	Визначення суми ризиків	Визначення комплексного ризику
Brainstorming	+	–	–	–	–	–	–
Structured or semi-structured interviews	+	–	–	–	–	–	–
Delphi method	+	–	–	–	–	–	–
Checklist	+	–	–	–	–	–	–
PHA	+	–	–	–	–	–	–
HAZOP	+	+	+	+	+	–	–
HACCP	+	+	–	+	+	–	–
Toxicity assessment	+	+	+	+	+	–	–
SWIFT	+	+	+	+	+	–	–
Scenario analysis	+	+	+	+	+	–	–

Продовження таблиці. 2.1

FMEA	+	+	+	+	+	–	–
Fault tree analysis	+	–	+	+	+	–	–
Event tree analysis	+	+	+	+	+	–	–
Cause and consequence analysis	+	+	+	+	+	–	–
Cause-and-effect analysis	+	+	–	–	–	–	–
LOPA	+	+	+	+	–	–	–
Decision tree	–	+	+	+	+	–	–
HRA	+	+	+	+	+	–	–
Bow tie analysis	–	+	+	+	+	–	–
Monte Carlo simulation	–	–	–	+	+	–	–
Consequence/probability matrix	+	+	+	+	+	–	–
Cost/benefit analysis	+	+	+	+	+	–	–
MCDA	+	–	+	–	+	–	–

2.2 Модель загроз інформаційних систем об’єктів критичної інфраструктури до кібератак

На сьогоднішній день інформаційна безпека держави визначається, в тому числі, рівнем інформаційної безпеки існуючих складних людино- машинних систем управління об’єктами технічних, технологічних, організаційних і економічних комплексів країни – автоматизованих систем управління технологічними процесами (АСУ ТП) [6], [7].

І якщо, спочатку зазначені системи були у вигляді окремого комп’ютера із власними операційними системами і мережами, то розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж дає можливість забезпечувати управління виробничою діяльністю в режимі реального часу, здійснювати дистанційний моніторинг систем управління технологічним процесом, підвищити безпеку підприємства і персоналу, зменшити витрати на експлуатацію.

Однак, ціною цих переваг являється підвищена уразливість до нового типу загроз інформаційної безпеки АСУ ТП – злому і порушення режимів функціонування ключових об'єктів, які відповідають за управління та забезпечення безпеки об’єктів критичної інфраструктури, до яких можна віднести: атомні і гідроелектростанції, нафто - і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня тощо. І від інформаційної безпеки систем управління подібними об’єктами залежить не тільки прибуток компаній, але й національна безпека.

Забезпечення інформаційної безпеки, яка включає в себе в якості основних складових духовно-світоглядну, архетипічну, соціально-моральну, психічну, інтелектуальну і психофізіологічну безпеку, являє собою актуальну військово-політичну, наукову і соціально-економічну проблему [8]. На думку деяких фахівців [9], [10], наукове вирішення даної проблеми повинно базуватися на дослідженні відповідних інформаційних відносин активних компонентів вказаних систем, якими є обслуговуючий персонал, з відповідними активними компонентами конфронтуючих систем і між собою. Інформаційні відносини активних об’єктів в різних інформаційних середовищах (природних, штучних, гібридних) повинні включати відносини інформаційного відокремлення (ізоляції та захисту) і взаємодії (суперництво та співробітництво).

Крім того, деякі автори [11] висловлюють думку, що на даний час все більше зростає роль людського фактору на інформаційну безпеку АСУ ТП при недостатній кількості методів і засобів його оцінки та захисту. Засоби і методи, які наразі

розробляються (наприклад, метод інженерної психології) дають змогу зменшити рівень помилкової інформації, але не досліджують проблему у цілому, в тому числі не проводять оцінку і захист, як від випадкових, так і від умисних деструктивних дій обслуговуючого персоналу.

При цьому, людський фактор являється одночасно і необхідним елементом людино-машинних систем управління і джерелом загроз інформаційній безпеці таких систем, рис. 2.1.

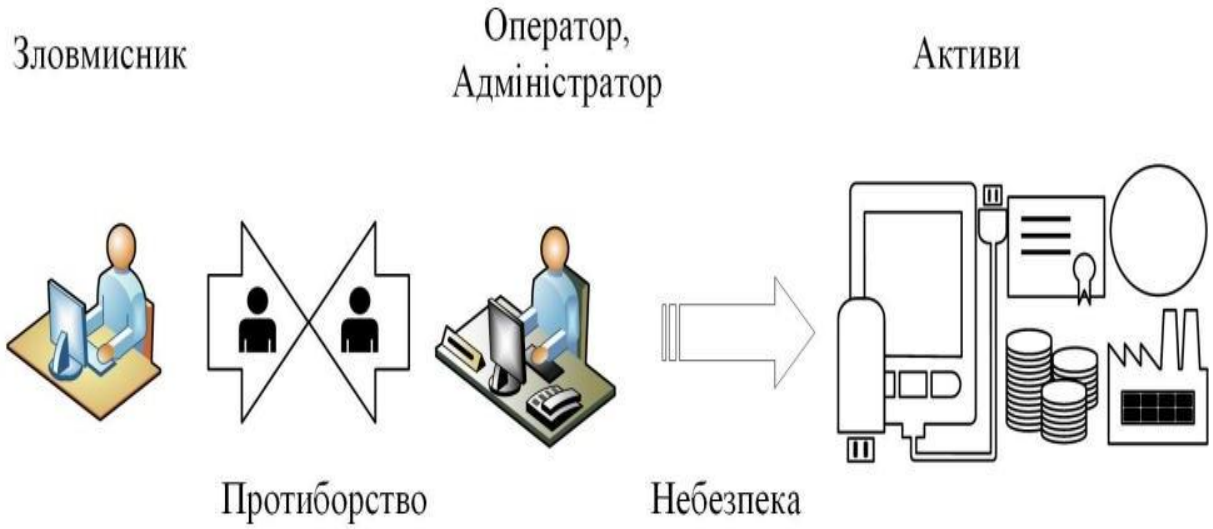


Рисунок 2.1 — Об’єктивне протиріччя

Таким чином, основними об’єктами інформаційно-психологічного впливу в АСУ ТП являється обслуговуючий персонал і особа, яка приймає рішення щодо управління процесами в тій чи іншій предметній області [11].

В складних людино-машинних системах управління персоналу доводиться приймати ті чи інші рішення. При цьому, на адекватність прийнятих рішень персоналом в таких системах можуть впливати такі фактори [10]: зовнішні та внутрішні дестабілізуючі впливи, нестійкість рішення при великій кількості альтернатив, тривалість часового інтервалу для прийняття рішення.

Враховуючи викладене, можна зазначити, що важливою задачею являється прийняття адекватних рішень обслуговуючим персоналом в різних інформаційних середовищах і відносинах. Для цього актуальним є отримання моделі імовірних

деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки.

Кількість альтернатив і тривалість часового інтервалу для прийняття рішення буде залежати від технологічних особливостей конкретної системи і вплив даних факторів може призвести до ненавмисних помилкових дій персоналу. В той же час, дія зовнішніх та/або внутрішніх дестабілізуючих впливів може призвести до навмисних деструктивних дій персоналу. Загальна схема дії таких чинників приведена на рис. 2.2. Розглянемо більш детально, що собою являє кожний з наведених чинників

Виділяють п’ять відповідних груп засобів, які можуть бути застосовані для інформаційно-психологічного впливу на персонал людино-машинних систем управління [9]:

- засоби масової інформації, агітаційно-пропагандистські засоби;
- психотронні засоби;
- електронні засоби: радіоелектронні, оптикоелектронні, електронно-обчислювальні засоби і засоби комп’ютерних інформаційних технологій;
- лінгвістичні засоби;
- психотропні засоби.

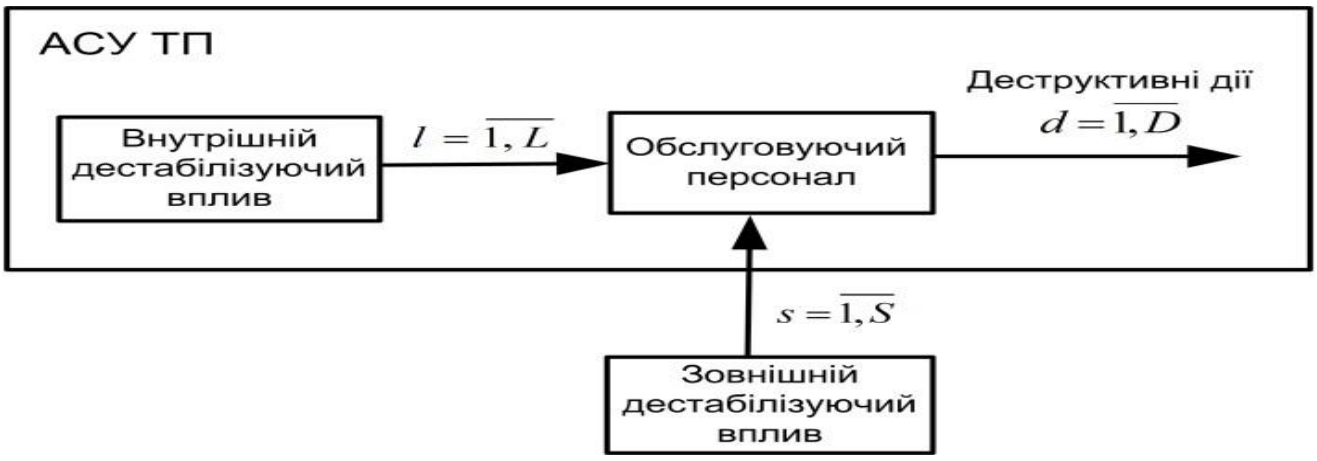


Рисунок 2.2 — Загальна схема дії чинників в АСУ ТП

Таким чином, стан інформаційної безпеки персоналу АСУ ТП визначається двома основними чинниками: інформаційно-психологічною задоволеністю людських потреб персоналу і дестабілізуючими (навмисними або випадковими) інформаційно-психологічними та інформаційно-технічними впливами.

Загрози можуть бути реалізовані різними типами деструктивних дій. Взаємозв'язок між загрозами і можливими деструктивними діями приведений на рис. 2.3 [12].

Як бачимо з рис. 2.3, загрози інформації можна класифікувати за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності доступності інформації і відповідальності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;

- несанкціоновані зміни або викрадення інформації;

- відмова в обслуговуванні або профілактика авторизованого доступу;

- відмова у відповідальності.

Таким чином, конфіденційність буде забезпечуватись, якщо дотримуються встановлені правила доступу до системи, цілісність - якщо дотримуються встановлені правила модифікації інформації або її видалення, доступність - якщо зберігається можливість доступу до системи або модифікації інформації відповідно до встановлених правил упродовж будь- якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

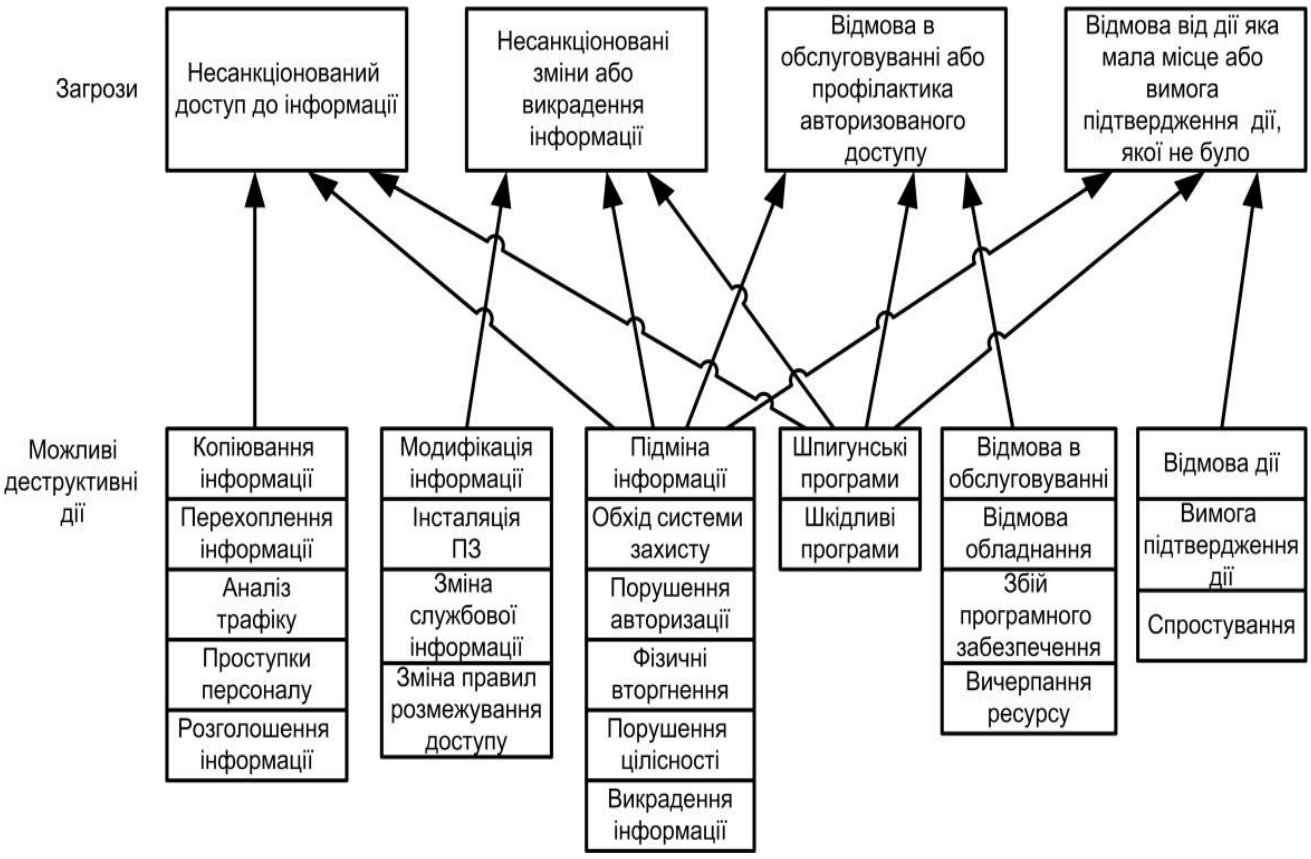


Рисунок 2.3 — Взаємозв’язок між загрозами і деструктивними діями

Загрози для автоматизованих систем управління технологічними процесами можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природних (стихійні лиха, кліматичні умови тощо). Однак, ми розглядаємо загрози, які можуть виходити від імовірних навмисних деструктивних дій обслуговуючого персоналу при умові наявності деструктивних впливів.

Очевидно, що обслуговуючий персонал складається з індивідів, кожний з яких здатний здійснювати хороші або погані вчинки, бачити себе зі сторони спостерігача, усвідомлювати відповідні відчуття за здійсненні вчинки тощо.

Найпростішу модель, яка описує поведінку такого індивіда, його готовність до дій, можливо представити у вигляді імплікації [8]:

Загрози інформації класифікують за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності доступності інформації і відповідальності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;

- несанкціонована модифікація або викрадення інформації;

- відмова в обслуговуванні;

- відмова у відповідальності.

Загрози для об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природні (стихійні лиха, кліматичні умови тощо). Приведемо більш детальний опис груп, що входять в категорію навмисних загроз [35]:

Зловмисники. Найчастіше хакери зламують мережі для гостроти відчуттів в дусі змагань або для хвастощів серед колег. Раніше віддалений злом вимагав неабияких комп'ютерних знань та навичок, а тепер зловмисники можуть завантажити сценарії атаки і протоколи Інтернету. Таким чином, у той час як інструменти атаки стали більш складними, вони також стали більш легкими для використання.

Оператори ботнету. Ботнет - комп'ютерна мережа, що складається з деякої кількості хостів, з запущеними ботами (автономним програмним забезпеченням). Найчастіше бот у складі ботнета є програмою, що потай встановлюється на пристрій жертви і дозволяє зловмиснику виконувати якісь дії з використанням ресурсів зараженого комп'ютера. Зазвичай ботнети використовуються для

нелегальної або злочинної діяльності: розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні.

Злочинні групи. Злочинні групи прагнуть атакувати системи для отримання грошової вигоди з допомогою спаму, фішингу, шпигунських програм для вчинення крадіжки та шахрайства в Інтернеті.

Іноземні спецслужби. Іноземні спецслужби використовують кіберзасоби, як частину їх шпигунської діяльності, спрямованої на збір інформації або для проведення операцій в рамках інформаційних впливів на супротивника.

Інсайдери. Незадоволені інсайдери є основним джерелом комп'ютерної злочинності. Інсайдерам не потрібно мати багато спеціальних знань про кібератаки, тому що можливості якими вони володіють, перебуваючи усередині системи, часто дозволяють їм отримати необмежений доступ до системи, а також здійснити її пошкодження або крадіжку даних. Також інсайдерські загрози становлять сторонні постачальники обладнання та програм, а також співробітники, які ненавмисно впроваджують шкідливі програми в системі. Інсайдерами можуть бути працівники, підрядники, партнери по бізнесу.

Фішери. Фішинг - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролів. Дана загроза реалізується шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів. У листі міститься пряме посилання на сайт, зовні відрізнити від справжнього, або на сайт з переадресацією. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленої сторінці свої логін і пароль.

Сніфінг. Сніфінг - поширений вид атаки, коли всі пакети, отримані мережевою картою, пересилаються на обробку спеціальною програмою, званому сніфером. У результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою

небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

Спамери. Спам - розсилка реклами або інших видів повідомлень особам, які не висловлювали бажання їх отримувати.

Автори шпигунських і шкідливих програм. Особи або організації, які зі злим умислом проводять атаки на користувачів шляхом написання і поширення шпигунського і шкідливого програмного забезпечення.

Терористи. Терористи ставлять перед собою мету знищити, вивести з експлуатації критично важливі об'єкти інфраструктури, створити загрозу національній безпеці, викликати масові жертви, послабити економіку країни, завдати шкоди суспільній моралі. Терористи можуть атакувати одну мету, щоб відвернути увагу та ресурси від інших цілей.

Промислові шпигуни. Метою шпигунства може стати компрометація інформації або її крадіжка з подальшим деструктивним використанням, до повної зупинки і банкрутства промислового об'єкта.

Загрози інформації класифікують за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки через уразливості. Уразливістю є недолік або слабке місце інформаційної системи, системи безпеки, процедур внутрішнього контролю, які можуть бути використані для порушення цілісності або доступності системи та її коректної роботи. Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

Класифікація уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами показана на рис. 2.4.

Розглянемо більш докладно уразливості автоматизованих систем управління [35].

1. Уразливості політик і процедур. До цієї категорії можна віднести:

- невідповідність або відсутність політики безпеки;
- невідповідність або відсутність процедур безпеки (повинні бути розроблені конкретні процедури безпеки і навчений відповідний персонал);
- відсутність підвищення кваліфікації персоналу у сфері безпеки;
- невідповідність архітектури безпеки;
- невідповідність або відсутність керівництва по впровадженню обладнання;
- відсутність відповідальності за документальне адміністрування політик і процедур безпеки;
- відсутність або недолік аудитів в області безпеки;
- відсутність конкретного плану аварійного відновлення системи у випадку збою або аварії (план повинен бути готовий, апробований та доступний у разі виникнення апаратного або програмного збою, щоб уникнути простою і втрати виробництва);
- відсутність змін конфігурації управління (повинно здійснюватися управління модифікаціями апаратних засобів, програмованого обладнання, програмного забезпечення, щоб гарантовано захистити систему від невідповідних або неправомірних модифікацій до, під час, і після впровадження системи).

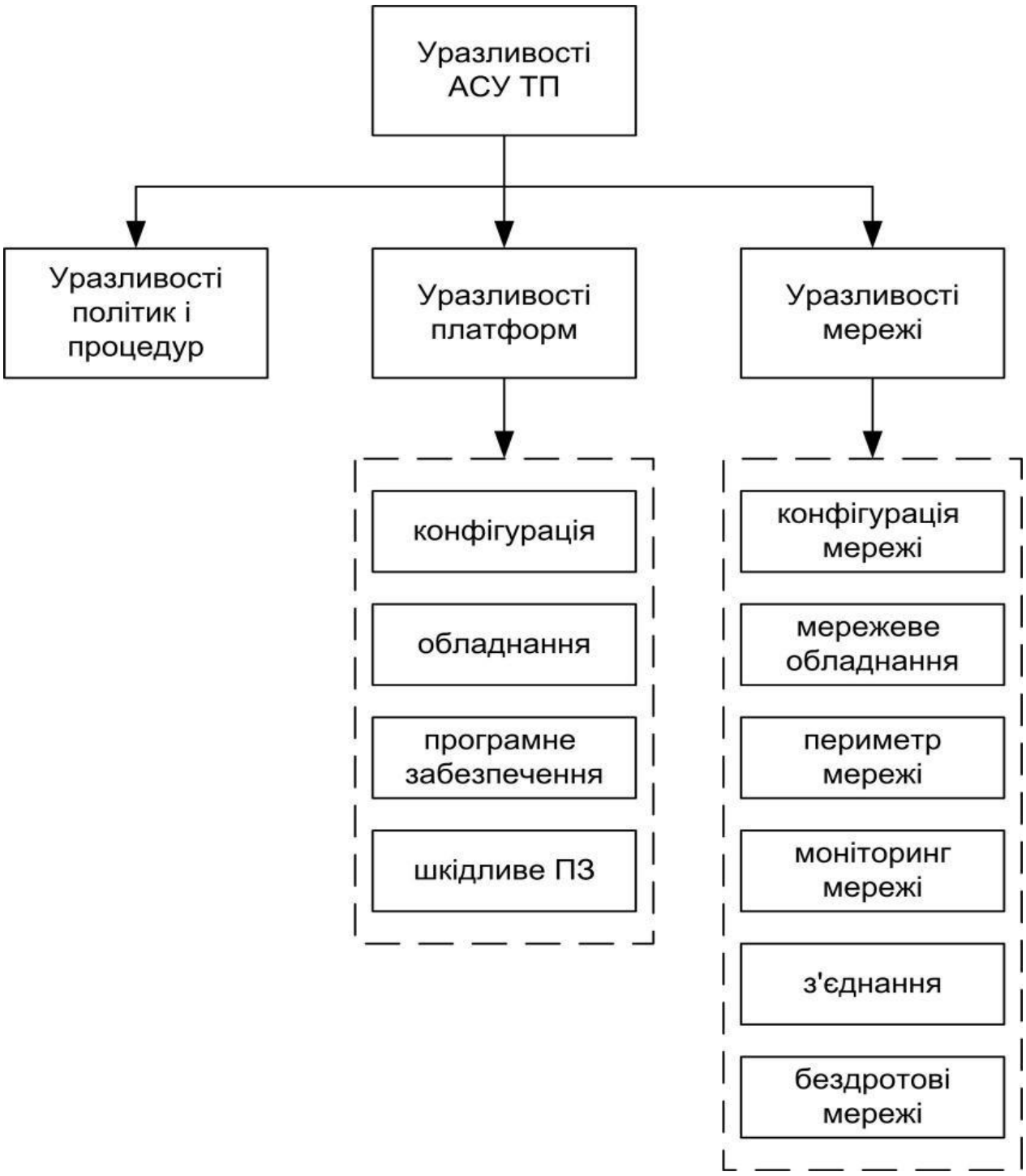


Рисунок 2.4 — Класифікація уразливостей інформаційної безпеки АСУ ТП

Аналіз показує, що уразливості політик і процедур в промислових автоматизованих системах управління виникають через відсутність або неповну, неадекватну документацію в галузі безпеки, у тому числі політик і керівництва (процедур), адміністрування аудиту, відновлення.

Розглянемо уразливості платформ. До даної категорії можна віднести:

1. Конфігурація:

- програмне забезпечення не оновлюється для виявлення вразливостей (через складність програмного забезпечення АСУ зміни повинні пройти комплексне тестування, що займає певний час і забезпечує уразливість до загроз);

- операційна система та програми безпеки впроваджуються і оновлюються без ретельних випробувань (повинні бути розроблені документовані процедури для тестування нових програм безпеки);

- параметри конфігурації використовуються за замовчуванням (це часто призводить до небезпечного відкриття портів інших служб і виконання небажаних програм);

- не зберігаються критичні конфігурації системи (для підтримки доступності системи і запобігання втрати даних повинні бути розроблені документовані процедури для відновлення параметрів конфігурації у разі випадкової або зловмисної зміни в конфігурації);

- зберігання незахищених конфіденційних даних (наприклад, паролі) на портативних пристроях (ці пристрої будуть втрачені або вкрадені і безпека системи може бути порушена);

- відсутність адекватної політики паролів (коли паролі повинні бути використані, наскільки стійкими вони повинні бути і як вони повинні зберігатися);

- відсутність пароля (паролі повинні бути реалізовані для запобігання несанкціонованого доступу - для входу в систему (якщо в системі є облікові записи користувачів), при включенні живлення (якщо в системі немає облікових записів користувачів), при виході та режиму заставки);

- розкриття паролів (прикладами можуть бути спільне використання паролів для різних облікових записів користувачів, повідомлення паролів стороннім, передача паролів в незашифрованому вигляді через незахищені підключення);

- підбір пароля (погано підібраний пароль може бути легко розгаданий зловмисником або комп'ютерною програмою для отримання несанкціонованого доступу);

- неадекватність контролю доступу (неправильно налаштований контроль доступу може дозволити оператору дії адміністратора або заборонити оператору коригувальні дії в аварійній ситуації).

2. Обладнання:

- невідповідне тестування змін системи безпеки;

- недостатній рівень фізичного захисту критично важливих систем;

- несанкціонований фізичний доступ сторонніх осіб до обладнання;

- незахищений віддалений доступ до компонентів АСУ;

- подвійні мережеві карти для з'єднання мереж (при підключенні до різних мереж можливий несанкціонований доступ з однієї мережі в іншу);

- відсутність документування активів (відсутність точного списку активів в системі може залишити несанкціоновані точки доступу);

- радіочастотний і електромагнітний імпульс (наслідки впливу можуть бути від тимчасового порушення управління до пошкодження плат);

- відсутність резервного електроживлення;

- втрата контролю навколишнього середовища системи (втрата контролю навколишнього середовища процесорів може привести до перегріву і пошкодження або роботі з помилками);

- відсутність резервування критично-важливих компонентів.

3. Програмне забезпечення:

- переповнення буфера (може викликати аварійне завершення або зависання програми, що веде до відмови обслуговування. Окремі види переповнення, наприклад переповнення в стековому кадрі, дозволяють зловмиснику завантажити та виконати довільний машинний код від імені програми і з правами облікового запису, від якої вона виконується);

- не включені або ідентифікуються як відключені можливості безпеки, які були встановлені з програмним продуктом;

- відмова в обслуговуванні;

- неправильна обробка невизначених, погано визначених, або "неприпустимих" умов (деякі реалізації систем уразливі для пакетів, які спотворені або містять "неприпустимі" значення полів);

- використання незахищених галузевих протоколів передачі даних;

- передача повідомлень в незахищеному вигляді;

- запуск надлишкових сервісів, тобто тих служб, які не використовуються для вирішення поставлених завдань;

- використання пропрієтарного програмного забезпечення, яке було предметом обговорення на конференціях і в періодичних друкованих виданнях;

- недостатня перевірка справжності та контролю доступу для конфігурування та програмування;

- не встановлено програмне забезпечення виявлення/запобігання несанкціонованого проникнення;

- не підтримується протоколювання роботи всіх служб і сервісів;

- не реєструються інциденти.

4. Шкідливе програмне забезпечення:

- не встановлено захист від шкідливого програмного забезпечення;
- захист від шкідливого програмного забезпечення не актуальна, тобто не оновлюється або оновлюється рідко;
- захист від шкідливого програмного забезпечення впроваджена без проведення ретельних випробувань.

Як бачимо, уразливості платформ в АСУ ТП можуть виникати через недоліки, помилки, або неякісне обслуговування своїх платформ, у тому числі обладнання (апаратні засоби, операційні системи і додатки, відсутність контролю фізичного доступу.

Розглянемо уразливості мережі. До даної категорії можна віднести:

1. Конфігурація мережі:

- невідповідність архітектури мережевої безпеки;
- відсутність контролю потоку даних;
- неякісно налаштовані параметри безпеки обладнання;
- відсутність резервування конфігурації мережевого пристрою;
- передача паролів в незахищеному вигляді;
- недостатньо часта зміна паролів доступу до мережевих пристроїв;
- неадекватність контролю доступу до мережевих пристроїв.

3.2. Мережеве обладнання:

- недостатній рівень фізичного захисту мережевого обладнання;
- несанкціонований доступ до портів мережевого обладнання;
- відсутність надлишковості для критично важливих сегментів мережі.

3. Периметр мережі:

- не визначений периметр безпеки;

- відсутня або неправильно налаштовано міжмережевий екран;

- мережі управління використовуються для трафіку інших типів;

- управління мережевими сервісами мережі АСУ реалізується в мережі ІТ (мережа АСУ стає залежною від мережі ІТ, у якої немає необхідного пріоритету надійності і доступності).

4. Моніторинг мережі:

- неадекватні журнали міжмережевого екрану (кількість контрольованих параметрів не достатньо для проведення аналізу інцидентів);

- відсутність регулярного моніторингу безпеки в мережі.

5. З'єднання:

- не ідентифікуються критичні шляхи контролю та управління;

- використання стандартних протоколів зв'язку;

- відсутня або недостатня аутентифікація користувачів, данихабо пристроїв;

- відсутність перевірки цілісності з'єднань.

6. Бездротові мережі:

- невідповідність аутентифікації між бездротовими клієнтами і точками доступу;

- невідповідний захист даних між бездротовими клієнтами і точками доступу.

Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування

мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

З метою забезпечення інформаційної безпеки розглянемо деякі з існуючих методів своєчасного виявлення загроз автоматизованих систем (АС) [36]:

а) обмеження доступу;

б) контроль доступу до обладнання;

в) обмеження і контроль доступу до інформації;

г) надання привілеїв на доступ;

д) ідентифікація і установлення справжності об’єкта (суб’єкта);

е) захист інформації від витоку за рахунок побічного електромагнітного випромінювання і наведень.

Розглянемо кожний із приведених методів більш детально [36].

а) Обмеження доступу полягає у створенні деякої фізичної замкнутої перепони навколо об’єкта захисту із організацією контролює мого доступу осіб, пов’язаних з об’єктом захисту по своїх функціональних обов’язках.

Обмеження доступу до автоматизованої системи полягає у наступному:

- виділення спеціальної території для розміщення АС;

- обладнання по периметру виділеної зони спеціальних огороджень з охоронною сигналізацією;

- спорудження спеціальних приміщень або споруджень;

- виділення спеціальних приміщень в спорудженні;

- створення контрольно-пропускного режиму на території, в спорудженнях, в приміщеннях.

Задача засобів обмеження доступу – виключити випадковий і/або навмисний доступ сторонніх осіб на територію розміщення АС і безпосередньо до обладнання.

б) З метою контролю доступу до внутрішнього монтажу, ліній зв'язку і технологічних органів управління використовується обладнання контролю розкриття. Це значить, що внутрішній монтаж обладнання і технологічні органи, пульти управління закриті кришками, дверцятами або кожухами, на які встановлені датчики. Датчики спрацьовують при розкритті обладнання і видають електричні сигнали, які поступають на пристрій контролю.

в) Розмежування доступу до інформації в АС полягає в розділенні інформації, яка в ній циркулює на частини і організації доступу до неї посадових осіб у відповідності з їх функціональними обов'язками і повноваженнями.

Задача розмежування доступу до інформації – скорочення кількості посадових осіб, які не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед допущеного до неї персоналу.

При цьому, розділення інформації може здійснюватися по ступеню важливості, секретності, по функціональному призначенню, по документах тощо.

Зважаючи на те, що доступ здійснюється з різних технічних засобів, починати розмежування можна шляхом розмежування доступу до технічних засобів, розмістивши їх в окремих приміщеннях. Всі підготовчі функції технічного обслуговування обладнання, її ремонту, профілактики, перезавантаження програмного забезпечення тощо повинні бути технічно і організаційно відокремлені від основних задач системи.

г) Надання привілеїв на доступ до інформації полягає у тому, що із числа допущених до неї посадових осіб виділяється група, якій надається доступ тільки при одночасному пред'явленні повноважень усіх членів групи.

Задача методу – ускладнити навмисний перехват інформації порушником.

Даний метод ускладнює процедуру доступу до інформації, але перевагою є висока ефективність захисту.

д) Ідентифікація – це присвоєння будь якому об’єкту або суб’єкту унікального образа, імені або числа.

Встановлення справжності (аутентифікація) полягає в перевірці, чи являється об’єкт (суб’єкт), який перевіряється, насправді тим, за кого себе видає.

Кінцевою метою ідентифікації і встановлення справжності об’єкта в АС – допуск його до інформації з обмеженим доступом у випадку позитивного результату перевірки, або відмову в допуску у випадку негативного результату перевірки.

е) З метою захисту інформації з обмеженим доступом від витоку за рахунок побічного електромагнітного випромінювання і наведень проводяться виміри рівня небезпечних сигналів. Заміри виконуються в декількох точках на різних відстанях від джерела за допомогою спеціальної апаратури. Якщо рівень сигналу на границі встановленої зони перевищив допустимі значення, застосовують заходи захисту.

Заходи захисту можуть носити різноманітний характер в залежності від складності, вартості і часу їх реалізації, які визначаються при створенні конкретної АС.

Такими заходами можуть бути:

- удосконалення апаратури з метою зменшення рівня сигналів;

- встановлення спеціальних фільтрів;

- застосування генераторів шуму;

- використання спеціальних екранів;

- інші заходи.

В автоматизованих системах (АС) інформаційна безпека традиційно зосереджена на досягненні трьох цілей, конфіденційності, цілісності, доступності. Стратегія безпеки традиційної інформаційної технології направлена в першу чергу на конфіденційність з необхідними засобами управління доступом для досягнення заданої мети. При цьому цілісність займає другу сходинку по важливості задачі.

Стосовно інформаційних систем об'єктів критичної інфраструктури загальний пріоритет цих цілей часто відрізняється. Безпека в цих системах, перш за все, стосується підтримки доступності усіх компонентів системи. При цьому, цілісність являється часто другою по важливості задачею. Конфіденційність, як правило, для автоматизованих системах управління об'єктів критичної інфраструктури має найменше значення.

В переважній більшості випадках пріоритети повністю інвертовані. В той же час, в залежності від обставин у цілісності системи може бути самий високий пріоритет. Певні вимоги до функціонування, які висувають окремі компоненти або система в цілому, мають різні пріоритети для цілей (тобто, цілісність чи проблеми доступності можуть переважити конфіденційність, або навпаки).

Задачі забезпечення основних виробничих функцій автоматизованих системах управління об'єктів критичної інфраструктури іноді суперечать задачі забезпечення їх інформаційної безпеки і тому не можуть бути застосовані в АСУ ОКІ, а іноді навіть можуть бути небезпечними.

До основних особливостей ключових систем критичної інфраструктури, які суттєво впливають на зміст вимог по забезпеченню безпеки інформації, відносяться наступні [35]:

- основною інформацією, що захищається на об'єктах критичної інфраструктури держави є технологічна (забезпечує управління технологічними або чутливо важливими процесами) інформація програмно-технічна (програми системного і прикладного характеру, що забезпечують функціонування об'єктів), командна (керуюча) і вимірювальна, яка не належить до інформації з обмеженим доступом

(якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту згідно з чинними вимогами і нормами з технічного захисту інформації);

- переважна більшість ключових систем забезпечують керування безперервними технологічними процесами, що зумовлює значно більш жорсткі вимоги до часу і порядку виконання автоматизованих функцій, неможливість відключення на період проведення контрольних заходів в інтересах забезпечення безпеки інформації і оцінки їх реальної захищеності від негативних інформаційних впливів;

- різноманітність об’єктів, наявність в них різних, територіально і просторово розподілених елементів з поєднанням різноманітних інформаційних технологій;

- надзвичайна небезпека наслідків виведення з ладу і (або) порушення функціонування об’єктів критичної інфраструктури;

- широке застосування операційних систем реального часу, необхідність адаптації програмних та програмно-апаратних засобів захисту до цих операційних систем;

- компоненти системи об’єктів критичної інфраструктури працюють в режимі реального часу с жорстко заданими часовими параметрами и не потребують високої пропускної спроможності;

- для об’єктів критичної інфраструктури, наряду з інформаційною безпекою, пріоритетним є безпека обслуговуючого персоналу, збереження обладнання, запобігання виробничих втрат;

- на об’єктах критичної інфраструктури може бути дуже складний взаємозв’язок інформаційного захисту з фізичними процесами і наслідками в промисловому секторі. Тому, всі функції безпеки повинні бути протестовані на предмет відсутності загрози штатному функціонуванню систем;

- в системах об’єктів критичної інфраструктури дуже критичний час реакції системи на дію оператора. Доступ до системи жорстко контролюється, але не повинен перешкоджати або втручатися в процес взаємодії оператора и системи;
- системи об’єктів критичної інфраструктури створюються для забезпечення промислових процесів і, зазвичай, не вистачає ресурсів для підтримки програм по забезпеченню безпеки.

2.3 Структурна модель взаємодії елементів інформаційної системи об’єктів критичної інфраструктури

Проведений аналіз існуючих систем захисту інформації [1, 2], дає змогу визначити основні складові частини системи кіберзахисту інформаційних систем об’єктів критичної інфраструктури:

- нормативно-правова;
- організаційна;
- технічна;
- підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Так, одними із актуальних питань є наявність нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури, приведення національної нормативно-правової бази з питань забезпечення кібербезпеки об’єктів критичної інфраструктури у відповідність з положеннями міжнародних документів; виконання узгодженості понятійного апарату, що використовується в існуючих національних законодавчих та нормативно-правових документах; доопрацювання (при необхідності - розробка)

нормативних документів, вимог, методологій до оцінки загроз об’єктам, що є критичними для життєдіяльності держави, загальної методології оцінки ризиків для критично важливих об’єктів та критичної інфраструктури у цілому.

Крім того, слід зазначити, що керівники та/або власники об’єктів критичної інфраструктури повинні усвідомлювати можливість і ймовірність здійснення кібератак та наслідки, у випадку їх реалізації. Запровадження заходів з питань забезпечення кібербезпеки потребують залучення додаткових ресурсів, на що керівники цих об’єктів не завжди згодні, а механізм, який би вимагав від даних керівників запровадження необхідних заходів, відсутній. Тому, без запровадження згаданого механізму усі стандарти, інструкції тощо з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури будуть носити рекомендаційний характер, оскільки та інформація, яка циркулює, наприклад, в автоматизованих системах управління технологічними процесами, не відноситься ні до одного виду інформації, що підлягає захисту згідно із чинним законодавством.

Інформаційні системи об’єктів критичної інфраструктури зазвичай являються об’єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об’єкти захисту від кіберзагроз.

Кіберзагрози для інформаційних систем об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних, ненавмисних, природних. Основними з них є [3]: зловмисники, оператори ботнету, злочинні групи, іноземні спецслужби, інсайдери, фішери, сніфери, спамери, автори шпигунського і шкідливого програмного забезпечення, терористи, промислові шпигуни тощо.

На рис. 2.5 приведена структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури. Розглянемо, яким чином впливає

кожна із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Із приведеної структурної моделі взаємодії можна бачити, що джерела кіберзагроз для інформаційних систем об’єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини (інсайдер). При цьому, кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково повинні входити:

- захист периметра мережі;
- забезпечення безпеки міжмережевих взаємодій;
- моніторинг і аудит безпеки;
- виявлення і запобігання діям атак;
- резервне копіювання і відновлення даних;
- аналіз захищеності і керування політикою безпеки;
- контроль цілісності даних;
- захист від шкідливого програмного забезпечення;
- фільтрація контенту і запобігання витоку конфіденційної інформації;
- установка оновлень програмного забезпечення;

- адміністрування безпеки.

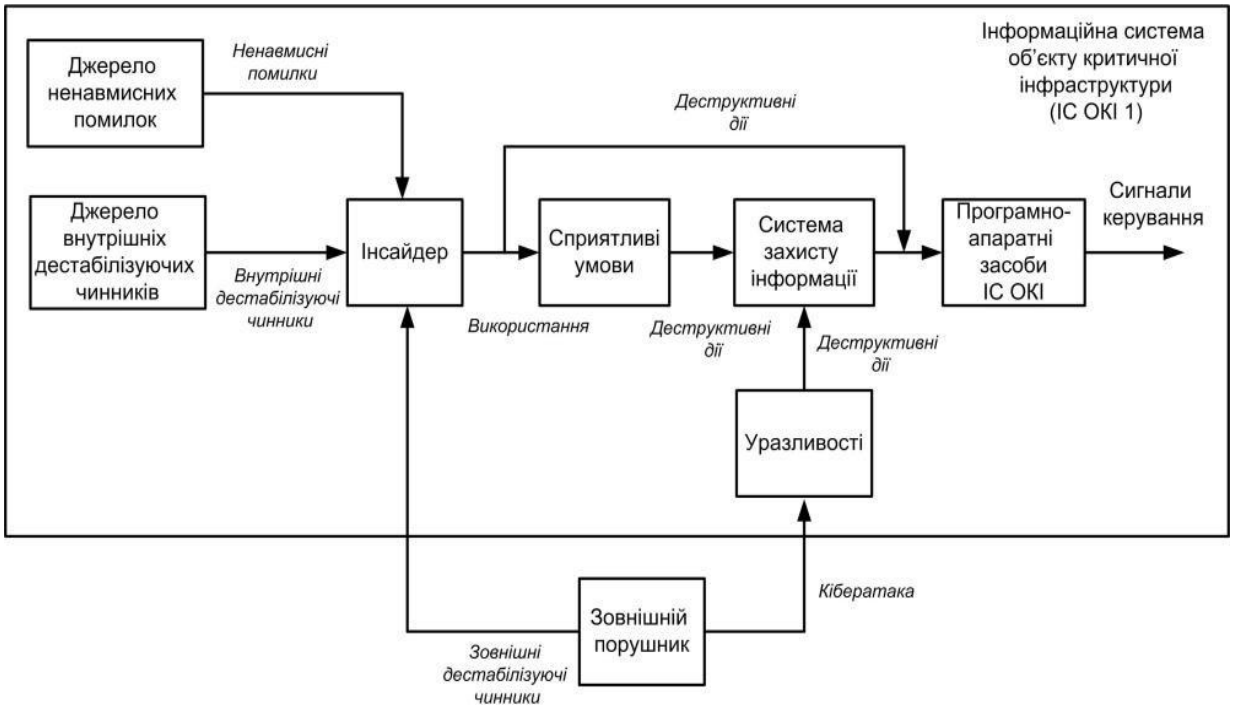


Рисунок 2.5 — Структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури

За результатами проведеного аналізу загроз та уразливостей [4], можливо зазначити, що захист таких систем повинен розглядатися по наступних напрямках:

- захист інформаційних і фізичних компонентів інформаційної системи об’єктів критичної інфраструктури;
- технічний захист інформації інформаційних систем об'єктів критичної інфраструктури;
- захист процесів, процедур і програм обробки інформації інформаційних систем об’єктів критичної інфраструктури;
- захист каналів зв'язку інформаційних систем об’єктів критичної інфраструктури;
- придушення побічних електромагнітних випромінювань;
- керування та контроль системою захисту.

Однак, основна відмінність інсайдера від зовнішнього порушника полягає у тому, що інсайдер має легітимний доступ до системи. В той час, як зовнішній порушник прикладає зусилля, щоб подолати систему захисту, прагнучи отримати доступ до інформації, інсайдер отримує цю інформацію абсолютно безперешкодно в межах своєї компетенції або незаконно розширюючи свої права і можливості. Тому, будь-який захист системи від зовнішнього порушника виявляється неефективним проти інсайдера. При цьому, зовнішній порушник може здійснювати кібератаки на програмно-апаратну складову інформаційної системи, використовуючи уразливості системи захисту інформації інформаційної системи об'єкту критичної інфраструктури, або чинити інформаційно-психологічний вплив на інсайдера (зовнішні дестабілізуючі чинники).

Окрім зовнішніх дестабілізуючих чинників до можливих деструктивних дії інсайдера можуть спонукати внутрішні дестабілізуючі чинники - людські потреби, через захищеність яких може розкриватися забезпечення кібербезпеки інформаційної системи об'єкта критичної інфраструктури, а також власні ненавмисні помилки.

Внутрішніми дестабілізуючими чинниками можуть бути [5]:

- фізіологічні (природні): їжа, одежа, житло, відпочинок, комфорт, екологія тощо;
- потреби в безпеці: комфорт, постійність умов життя тощо;
- пізнавальні: активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;
- наукові: освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;
- соціальні: соціальні зв'язки, спілкування, увага до себе, спільна діяльність тощо;
- престижні: самоповага, повага зі сторони інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;

- духовні: щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

У залежності від того, які чинники спонукають інсайдера на деструктивні дії, останніх поділяють на типи. Ці типи розділяються у залежності від мети, мотивації і послідовності дій інсайдерів.

Необхідно відмітити, що якщо інсайдер отримує доступ до активів інформаційної системи об’єкта критичної інфраструктури незаконно розширюючи свої права та можливості, то для цього може бути необхідна наявність сприятливих умов. У випадку отримання інсайдером доступу до активів інформаційної системи об’єкта критичної інфраструктури у межах своєї компетенції необхідності у сприятливих умовах немає. Крім цього, при цьому обходиться система захисту інформації.

Тому, проведений аналіз показує, що з метою мінімізації ймовірності здійснення інсайдером деструктивних дій необхідно:

- вчасно виявляти та вживати певних заходів для зменшення впливу внутрішніх дестабілізуючих чинників;
- покращувати відбір співробітників на етапі прийняття на роботу та вживати відповідних заходів щодо підвищення їх фахового рівня для недопущення або мінімізації ненавмисних помилок.Таким чином, із урахуванням викладеного можна зазначити, що на стан забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури впливають такі фактори:
- наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури;
- наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;
- наявність уразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

- наявність чи відсутність сприятливих умов для реалізації кіберзагроз;
- привабливість активів, на які власне і спрямовуються кібератаки;
- наслідки від можливої реалізації кіберзагроз;
- рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Також, одним із таких показників, на нашу думку може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, силові відомства, дипломатичні установи тощо.

Корисним для оцінки та аналізу стану кібербезпеки може бути поєднання кількості кібератак за певний інтервал часу з урахуванням їх спрямованості. Це дасть змогу визначити вектор зацікавленості зловмисника та їх мету – кібердиверсія, кіберрозвідка, кібершпигунство тощо по відношенню до кожного напрямку.

Перелік показників, однозначно, може бути розширений з урахуванням досвіду та аналізу статистичних даних щодо приведених вище факторів.

2.4 Визначення ймовірності реалізації загроз кібербезпеки об’єктів критичної інфраструктури

Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів [14-17].

Причинами виникнення загроз інформації являються дестабілізуючі фактори – явища чи події, які можуть з'являтися на будь-якому етапі життєвого циклу

системи. Наслідком виникнення дестабілізуючих факторів може бути ризик інформаційної безпеки – ймовірність того, що певна загроза використає уразливість системи, в результаті чого буде нанесено шкоду компонентам системи [18]. Отже, порушення інформаційної безпеки - це виникнення і реалізація загроз.

Разом з тим, слід відмітити, що загроза, яка не має відповідної уразливості, може не призводити до ризику. І навпаки, наявність уразливості не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею.

Взаємозв’язок між загрозами, уразливостями і ризиком приведений на рис.2.6[19].

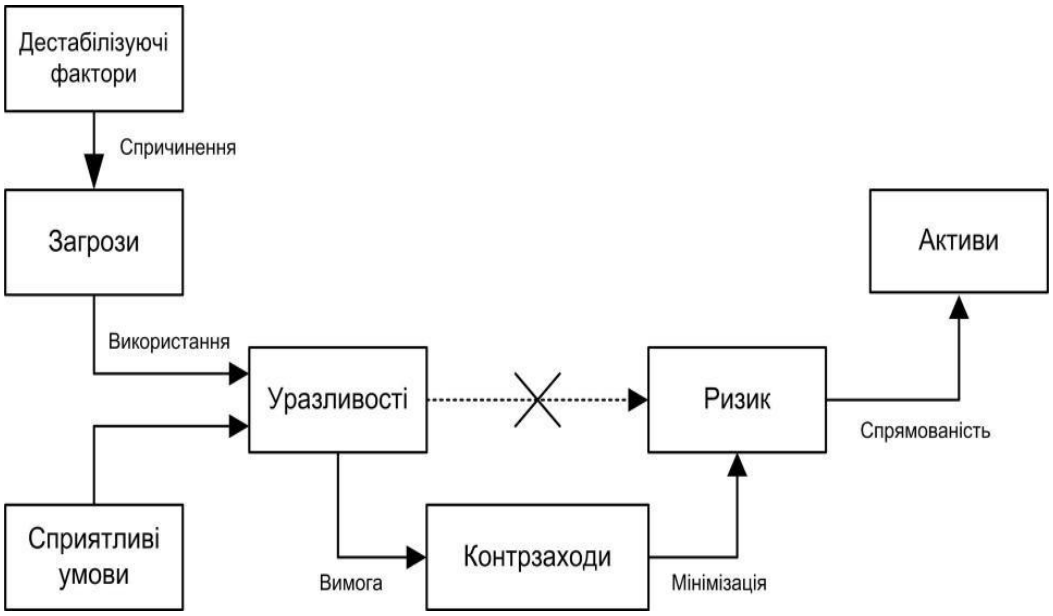


Рисунок 2.6 — Взаємозв’язок між загрозами, уразливостями і ризиком

Уразливість, яка не має відповідної загрози, може не вимагати впровадження засобу контролю, але повинна усвідомлюватися і піддаватися постійному моніторингу.

Виходячи із зазначеного, можна зауважити, що ймовірність реалізації загрози буде залежати від наявності сприятливих умов для використання уразливостей, пов’язаних з цими загрозами.

Життєвий цикл процесу аналізу ймовірності реалізації загроз представлений на рис. 2.7.

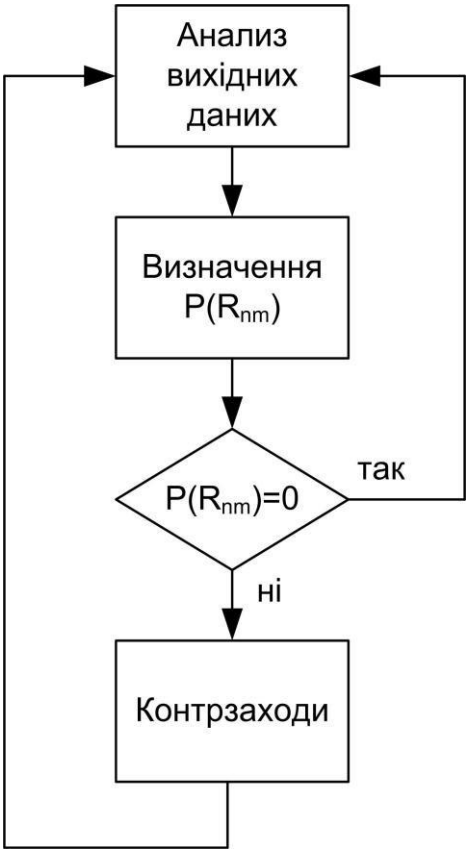


Рисунок 2.7 — Життєвий цикл процесу аналізу ймовірності реалізації загроз

2.5 Оцінювання небезпеки кібератак в інформаційних системах об'єктів критичної інфраструктури

Аналіз статистичних даних показує [20-23], що за останні 5 років найбільшу кількість уразливостей для атак виявлено в системах SCADA і людино-машинних інтерфейсах (ЛМІ), рис. 2.8. Крім того, порушення інформаційної безпеки на об'єктах деяких критичних інфраструктур можуть мати значні фізичні впливи.

Основними категоріями впливу є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій ІС ОКІ. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;

- економічні впливи - наслідки другого порядку від фізичних впливів, що є похідними від аварій ІС ОКІ. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;

- соціальні впливи - наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

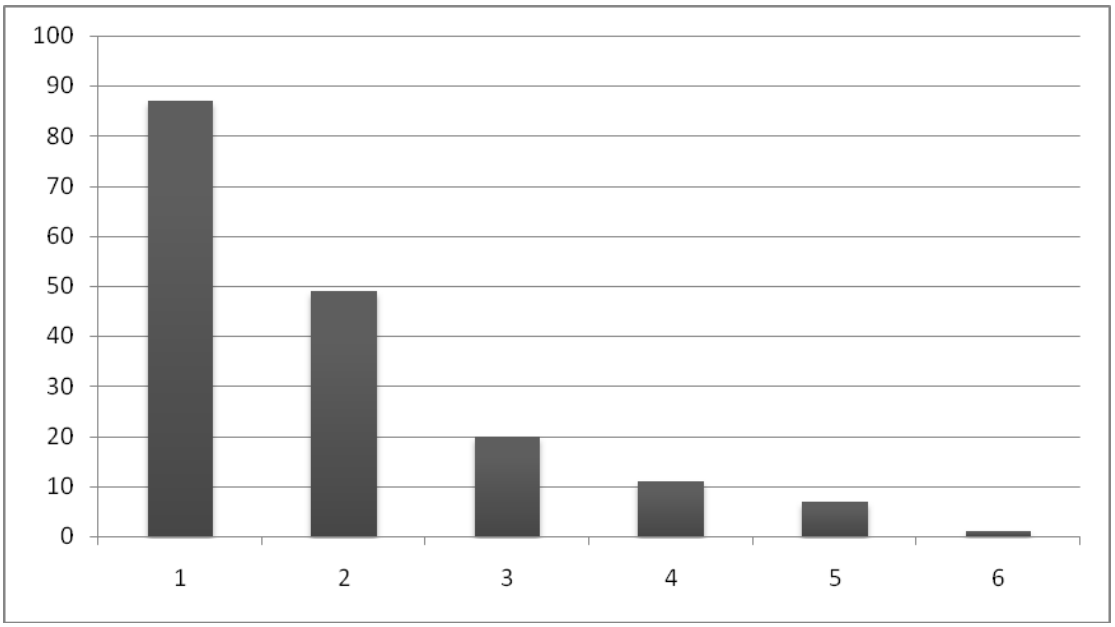


Рисунок 2.8 — Кількість уразливостей в компонентах АСУ ТП

Враховуючи приведені вище категорії впливу порушення інформаційної безпеки ІС ОКІ можливо навести перелік наслідків цих впливів [23]:

- порушення національної безпеки;
- сприяння вчиненню акту тероризму;
- втрата або скорочення виробництва;
- каліцтва або загибель людей;
- пошкодження обладнання;
- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;

- екологічні збитки;
- кримінальні або цивільно-правові зобов'язання;
- втрата приватної або конфіденційної інформації;
- втрата іміджу бренду або довіри клієнтів.

Слід зазначити, що елементи приведеного переліку не є незалежними.Очевидно, що один з наслідків може призвести до іншого.Атаки спрямовані на те, щоб заподіяти шкоду активам. Актив - деяка сутність, цінна для особистості, організації або держави [22]. Тому програми безпеки спрямовані на захист активів від збитків.

Активи ІС ОКІ можуть бути класифіковані за видами наступним чином[25]: фізичні, логічні, людські.Розглянемо більш детально кожний з видів активів.

Фізичні активи включають в себе будь-які фізичні компоненти або групи компонентів, які належать організації. В ІС ОКІ вони включають: системи управління, фізичні компоненти мережі передачі інформації або будь-які інші фізичні об'єкти, які певним чином залучені до процесів управління та аналізу виробничих процесів.

Логічні активи можуть включати в себе інтелектуальну власність, алгоритми, спеціальні знання, або інші інформаційні елементи, які містять в собі здатність функціонування організації або інноваційної діяльності. Крім того, ці види активів можуть містити суспільну репутацію, довіру покупця, або інші заходи, які, у разі їх пошкодження, безпосередньо впливають на виробничий процес. Логічні активи можуть бути представлені у формі особистої пам'яті, документів, інформації, що міститься на фізичному або електронному носіях інформації та включати в себе результати тестів, нормативних даних, або будь-яку іншу інформацію, яка розглядається як конфіденційна або приватна. Втрата логічних активів часто викликає значну шкоду організації і на тривалий час.

Активи ІС ОКІ є особливою формою логічних активів. Вони містять логіку автоматизації, яка приймає участь у виконанні виробничих процесів. Ці процеси надзвичайно залежать від повторного або безперервного виконання чітко визначених подій. І тому, нанесення шкоди цим активам, наприклад видалення або несанкціонована модифікація, може призвести до втрати цілісності або доступності безпосередньо до самого процесу.

Л юдські містять людей, знання, а також теоретичні і практичні навички, якими вони володіють, і які пов'язані з їх виробничою діяльністю. Вони можуть включати в себе необхідні сертифікати або важливі навички, необхідні для дій під час надзвичайних ситуацій.

Оцінка збитків активам може бути виражена або кількісно або якісно [25]. Кількісна оцінка активу дає точну відповідь щодо фінансових витрат, які пов'язані з цим активом. Це може бути вартість заміни, вартість втраченого продажу або інші заходи грошово-кредитної політики.

Якісна оцінка активів, як правило, виражається більше на абстрактному рівні, як наприклад показники у відсотках або у відносних значеннях. Багато активів можуть бути проаналізовані тільки з точки зору якісних збитків.

Збитки в ІС ОКІ можуть бути класифіковані як прямі і непрямі. Прямі збитки є витратами, які пов'язані з заміною активів. Збитки можуть мати місце за причиною фізичного пошкодження активу, в результаті втрати цілісності або доступності, переривання точної послідовності або зміни характеру процесу. Логічні ж активи мають порівняно низькі прямі збитки по відношенню до їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів з коротким часом відновлення можуть мати низькі прямі збитки для організації, навіть у випадку довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані з процесом простою, переробки або інші виробничі витрати через втрату активів.

Для фізичних активів непрямі збитки, як правило, включають наслідки, які виникають через втрату компонентів. Непрямі збитки від пошкодження обладнання можуть призвести до ремонту, реінжинірингу або інших зусиль для відновлення контролю над промисловим процесом. Для логічних активів непрямі збитки часто є дуже великими. Вони включають в себе втрату довіри громадськості, втрату ліцензії на діяльність, втрату конкурентних переваг від випуску інтелектуальної власності, як наприклад конфіденційний процес, нові технології тощо.

Шляхом здійснення упорядкування приведених вище даних за видами активів і способом вираження їх оцінки, можна співвіднести види збитків для кожного типу активів. Результуючі дані приведені у табл. 2.2.

Таблиця 2.2 — Види збитків для кожного типу активів

Вид активу	Прямі збитки	Непрямі збитки	Оцінка збитків, кількісна/якісна
Фізичні	Можуть бути досить високими через заміну вартості активу	Наслідки в результаті втрати або пошкодження активу (в залежності від вартості активу)	Якісна або кількісна (спочатку якісна при високому рівні ризиків, а далі кількісна для більшої точності)

Логічні	Зазвичай досить низькі, часто порівняно дешеві і можуть бути досить легко відновлені	Досить часто великі	В основному якісна, але в деяких випадках може бути кількісною
Людські	Як правило, низькі і середні (в залежності від ступеня пошкодження)	Як правило низькі або великі (в залежності від ступеня травми)	Безпосередній якісний вплив на виробництво, а потім кількісний вплив для відновлення

Загрози можуть бути реалізовані різними типами атак. Тому контрзаходи, які впроваджуються для захисту інформації повинні враховувати різні типи загроз і можливих атак. Взаємозв’язок між загрозами і можливими атаками приведений на рис. 2.3 [26].

На відміну від традиційних систем ІТ, в АСУ ТП існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [22]. Тому, порушення інформаційної безпеки в АСУ ТП може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека атаки в АСУ ТП буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної атаки.

2.6 Метод визначення актуальності загрози кібербезпеки об’єктів критичної інфраструктури

Кожна загроза безпеці інформації, якщо вона є актуальною для систем управління ОКІ, після ідентифікації підлягає нейтралізації і блокуванні, тобто, в

системах управління ОКІ із заданими структурно функціональними характеристиками і особливостями функціонування існує ймовірність реалізації загрози порушником з відповідним потенціалом і реалізація цієї загрози призведе до неприпустимих негативних наслідків - збитку, втрат, шкоди.

При всій важливості питання щодо визначення актуальних загроз безпеці інформації на ОКІ, на сьогоднішній день в нашій державі зазначене питання залишається недостатньо вивченим та дослідженим і наполегливо потребує розвитку.

Кожна загроза характеризується ймовірністю її реалізації і нанесеними нею збитками [27-30]. Таким чином, показник актуальності загрози ОКІ буде пропорційний ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

В класифікації загроз можливо виділити два найбільш важливих їх типу:

- намір завдати шкоди, який проявляється у вигляді анонсованого мотиву діяльності суб'єкта;
- можливість нанесення шкоди - існування достатніх для цього умов і факторів.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питання про наявність у загрозливого суб'єкта сил і засобів, достатніх для здійснення наміру.

Можливість нанесення шкоди полягає в існуванні достатніх для цього умов і факторів. Особливість загроз даного типу полягає в тому, що оцінка потенціалу сукупності факторів, які можуть послужити перетворенню цих можливостей і умов для нанесення шкоди, може бути здійснена тільки суб'єктами загроз.

Метою визначення актуальності загроз безпеці інформації є встановлення того, чи існує можливість порушення конфіденційності, цілісності або доступності інформації, що міститься в ОКІ, і чи призведе порушення хоча б одного з вказаних властивостей безпеки інформації до неприйнятних збитків.

У процесі визначення загроз безпеці інформації на всіх стадіях (етапах) життєвого циклу інформаційних систем необхідно регулярно проводити ідентифікацію джерел загроз, оцінювати їх можливості і визначати на цій основі загрози безпеці інформації. Дані про порушників і їх можливості з реалізації загроз безпеці інформації, отримані при ідентифікації джерел загроз, включаються до моделі загроз безпеці інформації.

З метою проведення дослідження та аналізу взаємодії джерел загроз, власне самих загроз, сприятливих умов реалізації цих загроз, уразливостей, активів, як об’єктів впливу зловмисників, а також системи захисту інформації, яка запобігає даному впливу, розглянемо узагальнену модель процесу захисту інформації, рис. 2.9.

Таким чином, для ідентифікації загроз безпеці інформації в ОКІ необхідно визначити:

- джерела загроз: можливості (тип, вид, потенціал) порушників;
- вразливості, які можуть використовуватися при реалізації загроз безпеці інформації;
- сприятливі умови для реалізації загроз безпеці інформації;
- активи: об'єкти впливу ОКІ, на які спрямована загроза безпеці інформації;
- коефіцієнт небезпеки загроз: результат і наслідки від реалізації загроз безпеці інформації.

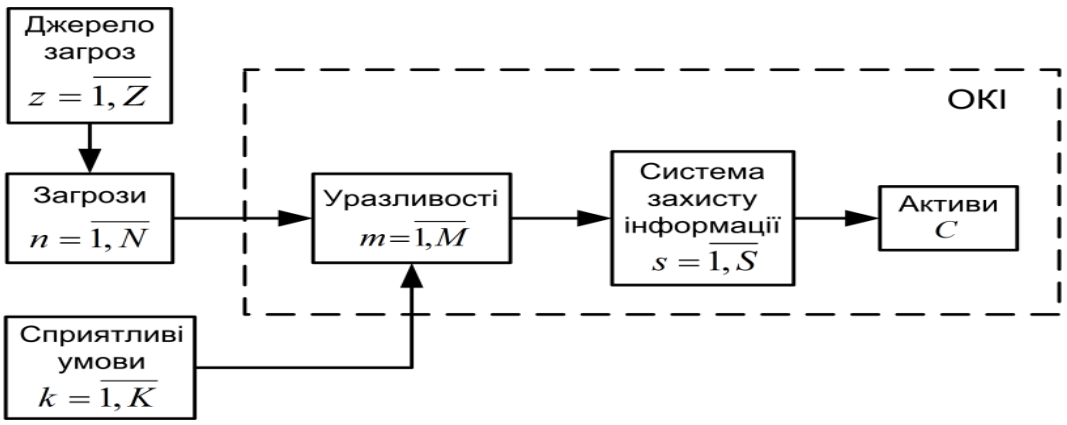


Рисунок 2.9 — Узагальнена модель процесу захисту інформації ОКІ

Структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури показує, рис. 2.5, що кожну загрозу кібербезпеці інформаційної системи, яка циркулює в інформаційній системі об’єкту критичної інфраструктури.

Загроза безпеці інформації, яка циркулює на ОКІ, буде вважатися актуальною, якщо для вказаного ОКІ з заданими структурно-функціональними характеристиками і особливостями функціонування існує ймовірність реалізації розглянутої загрози порушником з відповідним потенціалом і її реалізація призведе до неприйнятних збитків від порушення конфіденційності, цілісності або доступності інформації.

Це викликано тим, що в автоматизованих системах ОКІ існує досить тісний взаємозв’язок автоматизованих систем з фізичними процесами і виконавчими пристроями [30]. Тому, порушення безпеки інформації в даних системах може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека загрози в автоматизованих системах ОКІ із множини загроз буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем ОКІ, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної загрози [31].

За відсутності таких статистичних даних актуальність загрози визначається на основі оцінки можливості реалізації загрози безпеці інформації, яка, в свою чергу, визначається на основі оцінки рівня захищеності автоматизованої системи ОКІ та потенціалу порушника, необхідного для реалізації даної загрози.

Коефіцієнт небезпеки загрози можливо визначити на основі оцінки ступеня наслідків від порушення конфіденційності, цілісності або доступності інформації в автоматизованих системах ОКІ.

Актуальність загроз безпеці інформації визначається щодо загроз, для яких експертним методом обумовлено наступне:

- можливості (потенціал) порушника достатні для реалізації загрози безпеці інформації;
- в автоматизованій системі ОКІ є потенційні уразливості, які можуть бути використані при реалізації певної загрози безпеці інформації;
- структурно-функціональні характеристики та особливості функціонування автоматизованої системи ОКІ не виключають можливості застосування способів, необхідних для реалізації певної загрози, тобто існує сценарій реалізації загрози;
- реалізація загрози безпеці інформації призведе до порушення конфіденційності, цілісності або доступності інформації, в результаті якого можливе виникнення неприйнятних негативних наслідків, заподіяння значної шкоди.

Джерелами інформації щодо вихідних даних про загрози безпеці інформації та їх характеристики можуть бути базові та типові моделі загроз безпеці інформації, визначені нормативними документами для різних класів і типів автоматизованих систем [32-33].

Визначимо оцінку ймовірності (можливості) реалізації загрози безпеці інформації. Під ймовірністю реалізації загрози безпеці інформації будемо розуміти показник, визначений експертним шляхом, що характеризує значення ймовірності реалізації певної (n-ої) загрози безпеці інформації в автоматизованій системі ОКІ із заданими структурно-функціональними характеристиками і особливостями функціонування.

У випадку відсутності необхідних даних для оцінки ймовірності реалізації загрози безпеці інформації або наявності сумнівів в об'єктивності експертних

оцінок при визначенні градацій ймовірності реалізації загроз безпеці інформації, актуальність n-ої загрози безпеці інформації визначається на основі оцінки можливості її реалізації.

Можливість реалізації *n*-ої загрози безпеці інформації можливо оцінити виходячи із рівня захищеності автоматизованої системи і потенціалу порушника, необхідного для реалізації цієї загрози безпеці інформації в автоматизованій системі ОКІ із заданими структурно функціональними характеристиками і особливостями функціонування. Отже, можливість реалізації *n*-ої загрози можливо описати наступним чином:

Однак, в ході експлуатації автоматизованих систем ОКІ можлива поява нових уразливостей систем, підвищення потенціалу порушника, зміна структурно-функціональних характеристик, важливості оброблюваної інформації, особливостей функціонування зазначених систем та інших умов, що призводять до виникнення нових загроз безпеці інформації, які можуть суттєво знизити рівень проектної захищеності даних систем. У цьому випадку для підтримки рівня захищеності автоматизованих систем ОКІ в ході експлуатації повинен проводитися регулярний аналіз зміни загроз безпеці інформації, а актуальні загрози безпеці інформації повинні підлягати періодичній переоцінці.

Таким чином, рівень захищеності автоматизованої системи ОКІ можливо визначити на основі аналізу наступної інформації:

- чи з'явилися додаткові загрози безпеці інформації в ході експлуатації;
- чи можуть бути вжиті заходи захисту інформації щодо додаткових загроз безпеці інформації, що з’явились в ході експлуатації;
- з якою оперативністю можна нейтралізувати додаткові загрози безпеці інформації, які з’явилися в ході експлуатації.

Потенціал порушника для реалізації певної загрози безпеці інформації можливо визначити на основі даних, наведених у базових і типових моделях загроз безпеці інформації, які визначаються нормативними документами для інформаційних систем різних класів і типів.

Визначимо оцінку ступеня можливого збитку від реалізації загрози безпеці інформації. Для оцінки ступеня можливого збитку загрози безпеці інформації визначаються можливий результат реалізації загрози безпеці інформації в автоматизованій системі ОКІ, вид збитку, до якого може призвести реалізація загрози безпеці інформації, ступінь наслідків від реалізації загрози безпеці інформації для кожного виду збитку.

В результаті реалізації загрози безпеці інформації можливі прямий або непрямий впливи на конфіденційність, цілісність, доступність інформації, що циркулює в автоматизованій системі управління ОКІ [34].

Прямий вплив на конфіденційність, цілісність, доступність інформації можливий в результаті реалізації прямої загрози безпеці інформації. У цьому випадку об'єктами впливу загрози є безпосередньо інформація та/або інші об'єкти захисту, які забезпечують отримання, обробку, зберігання, передачу, знищення інформації в автоматизованих системах ОКІ, в результаті доступу до яких або впливу на які можливий вплив на конфіденційність, цілісність або доступність інформації.

Непрямий вплив на конфіденційність, цілісність, доступність інформації розглядається в результаті реалізації непрямих загроз безпеці інформації. Реалізація непрямих загроз безпеці інформації не приводить безпосередньо до впливу на конфіденційність, цілісність, доступність інформації, але створює умови для реалізації одної або декількох прямих загроз безпеці інформації, що дозволяють реалізувати такий вплив. У цьому випадку в якості результату реалізації непрямої загрози необхідно розглядати результати реалізації всіх прямих

загроз безпеці інформації, які можливо реалізувати в разі реалізації даної непрямої загрози.

При визначенні ступеня можливого збитку необхідно виходити з того, що в залежності від цілей і завдань, що вирішуються автоматизованою системою ОКІ, видів оброблюваної інформації, вплив на конфіденційність, цілісність або доступність кожного виду інформації, що міститься в системі, може призвести до різних видів збитку. При цьому для різних власників інформації будуть характерні різні види збитку.

Як зазначається в [30], основними категоріями впливу в автоматизованих системах управління ОКІ є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій автоматизованих систем управління технологічними процесами. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;

- економічні впливи - наслідки другого порядку від фізичних впливів, що є похідними від аварій автоматизованих систем управління технологічними процесами. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;

- соціальні впливи - наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу в автоматизованих системах управління ОКІ можливо навести перелік наслідків цих впливів [30]:

- порушення національної безпеки;

- сприяння вчиненню акту тероризму;

- втрата або скорочення виробництва;

- травми або смерть людей;

- пошкодження обладнання;

- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;

- екологічні збитки;

- кримінальні або цивільно-правові зобов'язання;

- втрата приватної або конфіденційної інформації;

- втрата іміджу бренду або довіри клієнтів.

Зазначені наслідки можуть доповнюватися іншими видами залежно від цілей і завдань, що вирішуються автоматизованою системою ОКІ, а також виду інформації, яка в ній обробляється.

Таким чином, ступінь негативних наслідків від порушення конфіденційності, цілісності або доступності інформації визначається для кожного виду збитку, залежить від цілей і завдань, які виконуються автоматизованою системою ОКІ, і може мати різні значення для різних власників інформації і операторів, і визначається експертним методом.

У випадку, якщо в автоматизованій системі ОКІ обробляється два і більше види інформації, ступінь можливого збитку необхідно визначати окремо для кожного виду інформації, яка циркулює у системі. Підсумкова ступінь можливого збитку буде визначатися найвищим значенням ступеня можливого збитку,

визначеним для конфіденційності, цілісності, доступності кожного виду інформації.

З урахуванням викладеного, схематичне відображення методу визначення актуальності загрози кібербезпеки інформаційної системи об’єкту критичної інфраструктури, представлена у загальному вигляді на рис.2.10.

У випадку виявлення загрози безпеці інформації визначаємо її актуальність.Визначення актуальності загрози ґрунтується на аналізі вхідних даних, а саме:

- наявності чи відсутності сприятливих умов для реалізації даної загрози;
- наявності чи відсутності необхідної статистики щодо фактів реалізації даної загрози;
- наявності чи відсутності у потенційних порушників мотивації для реалізації даної загрози;
- можлива частота реалізації даної загрози;
- рівень захищеності автоматизованої системи ОКІ щодо реалізації даної загрози;
- потенціал порушника, необхідний для реалізації даної загрози.
- Рисунок 2.10 — Схематичне відображення методу визначення актуальності загрози

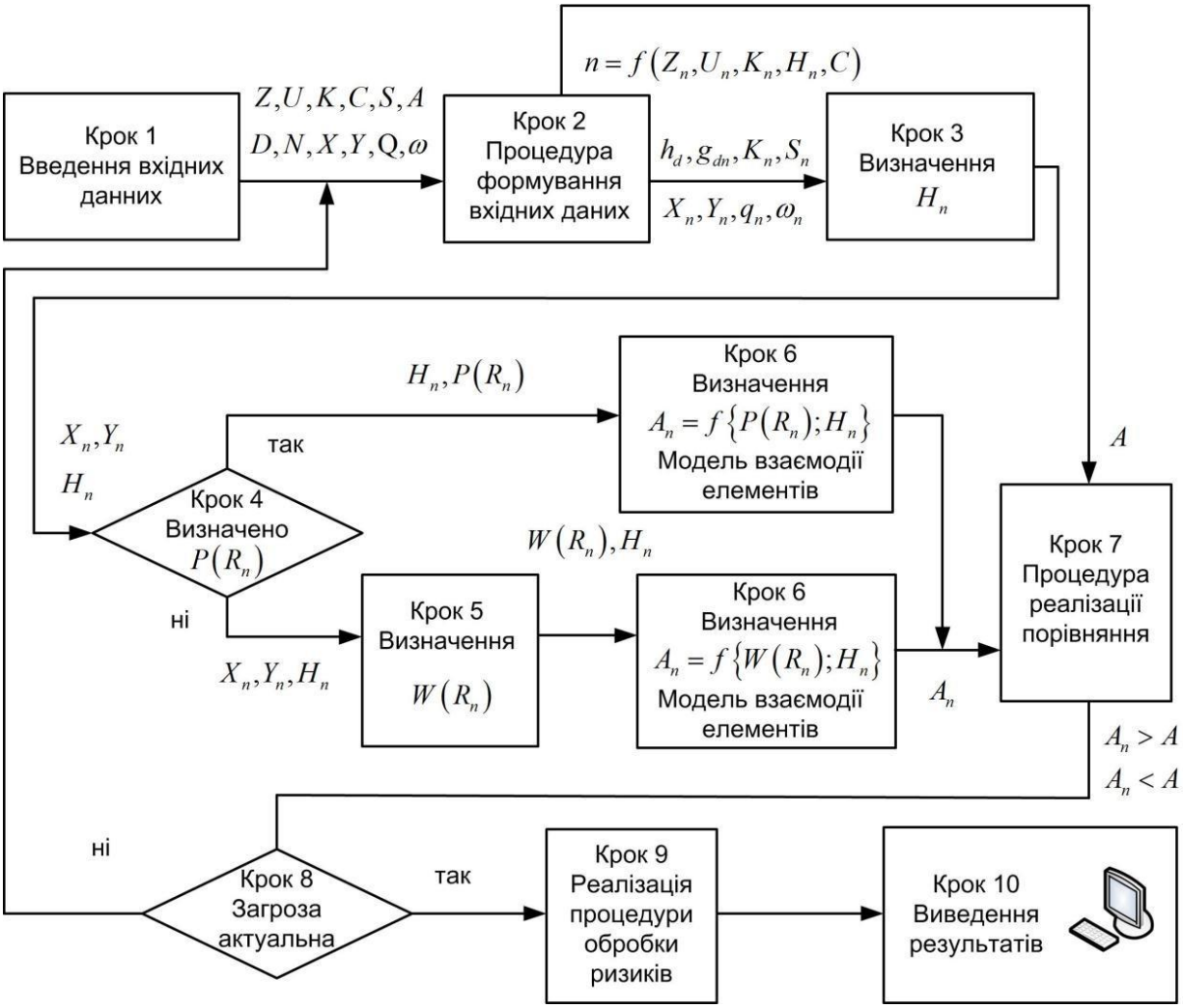


Рисунок 2.10 — Схематичне відображення методу визначення актуальності загрози

Разом з тим, визначається ступінь можливих наслідків у випадку реалізації виявленої загрози.У подальшому, в залежності від наявних вихідних даних, здійснюється або оцінка ймовірності реалізації виявленої загрози, або оцінка можливості її реалізації.

За результатами проведеної оцінки приймаються рішення щодо вжиття відповідних заходів, спрямованих на ефективне та своєчасне блокування (нейтралізацію) загроз безпеки інформації, в результаті реалізації яких можливі неприйнятні негативні наслідки.

2.7 Висновки до другого розділу

Виконано аналіз факторів, що впливають на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури. Результати проведеного аналізу можливо використати при розробці пропозицій та заходів щодо кіберзахисту інформаційних систем об’єктів критичної інфраструктури. Приведена модель імовірних деструктивних дій обслуговуючого персоналу АСУ ТП при умові наявності зовнішніх та/або внутрішніх дестабілізуючих впливів. Проведено аналіз джерел загроз та уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, досліджено взаємозв’язки між загрозами, уразливостями і ризиком для автоматизованих систем управління технологічними процесами. Приведено життєвий цикл аналізу ймовірності реалізації загроз інформаційної безпеки автоматизованих систем управління технологічними процесами та сформульовано вихідні дані, які необхідні для цього аналізу.

3 РОЗРОБКА МЕТРИКИ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Враховуючи важливість підтримки безпеки та стійкості критичної інфраструктури в умовах все більш складних кіберзагроз, наступним кроком є глибше заглибитися в розробку метрики, яка може бути використана для вимірювання рівня кіберстійкості в критичній інфраструктурі. Цей показник відіграє центральну роль у допомозі зацікавленим сторонам, від компаній до урядів та некомерційних організацій, у вимірюванні того, наскільки вони захищали свою інфраструктуру та як вони можуть відновитися в надзвичайних ситуаціях, викликаних все більш складними кібератаками. Крім того, цей показник має вирішальне значення для оцінки ефективності стратегій та тактики, що використовуються для захисту критичної інфраструктури, а також для визначення необхідних заходів щодо вдосконалення.

3.1 Сутність метрики кіберстійкості критичної інфраструктури

Показник вимірювання кіберстійкості критичної інфраструктури повинен точно відображати її складність та вразливість до кіберзагроз, що розвиваються. Враховуючи життєво важливу роль критичної інфраструктури у підтримці соціальної та економічної стабільності, ця метрика повинна забезпечити глибоке розуміння того, як зацікавлені сторони, включаючи компанії, уряди та некомерційні організації, можуть захистити свою інфраструктуру та якою мірою вони можуть відновитися в надзвичайних ситуаціях. Цей показник стає вирішальним наріжним каменем у забезпеченні того, щоб критична інфраструктура продовжувала працювати ефективно та безпечно, а також в оцінці ефективності стратегій та тактик, що використовуються для захисту критичної інфраструктури. Крім того, цей показник служить об'єктивним та надійним інструментом оцінки для визначення необхідних заходів щодо вдосконалення.

3.1.2. Ключові компоненти метрики кіберстійкості критичної інфраструктури

Існує кілька ключових компонентів оцінки критичної інфраструктури:

Оцінка ризиків та оцінка вразливості: Цей показник повинен включати комплексну оцінку ризиків для виявлення потенційних вразливостей у критичній інфраструктурі. Це передбачає оцінку потенційних кіберзагроз, з якими може зіткнутися інфраструктура, як часто вони можуть виникати та їх потенційний вплив. У цьому контексті може бути необхідним надання показників вразливості та рівнів ризику, щоб допомогти організаціям визначити пріоритети дій та розподілити ресурси. Крім того, ця оцінка також повинна враховувати такі фактори, як існуюча політика безпеки, впроваджені засоби контролю безпеки та рівень готовності організації протистояти кіберзагрозам.

Можливості реагування та відновлення: Цей показник повинен відображати ступінь, в якій критична інфраструктура може реагувати на кібератаки та відновлюватися після них. Це включає оцінку готовності до кіберінцидентів, включаючи навчання персоналу, плани надзвичайних ситуацій, а також інструменти та системи, що підтримують відновлення. Здатність швидко та ефективно реагувати на атаки та ефективно відновлюватися є ключовим елементом підвищення кіберстійкості. Крім того, цей показник також повинен враховувати такі фактори, як час відгуку, ефективність дій реагування та ефективність процесу відновлення.

Використання передових технологій: Використання передових технологій, таких як штучний інтелект, аналітика даних та системи раннього виявлення, слід вимірювати за допомогою цього показника. Впровадження цих технологій може значно покращити можливості виявлення та реагування на все більш складні кіберзагрози. Тому оцінка використання інноваційних технологій є ключовим компонентом показника кіберстійкості. Крім того, цей показник повинен

враховувати ступінь, в якій ці технології були інтегровані в систему безпеки організації, та їх ефективність у виявленні та реагуванні на кіберзагрози.

Співпраця та обмін інформацією: Рівень співпраці з іншими зацікавленими сторонами, як у державному, так і в приватному секторах, повинен бути значним фактором оцінки в цьому показнику. Здатність ділитися інформацією та співпрацювати у колективному захисті критичної інфраструктури є вирішальним елементом забезпечення оптимальної кіберстійкості. Крім того, цей показник також повинен враховувати ступінь, в якій організації побудували та підтримували ефективні відносини співпраці з іншими зацікавленими сторонами.

Вимірювання впливу та час відновлення: Цей показник повинен включати вимірювання впливу кібератак на критичну інфраструктуру, включаючи те, як швидко інфраструктура може відновитися та відновити роботу після атаки [87,88]. Це вимірювання дає уявлення про те, наскільки атаки впливають на операції та скільки часу потрібно для повного відновлення. Крім того, цей показник також повинен враховувати такі фактори, як фінансовий вплив атак, вплив на репутацію організації та вплив на клієнтів або користувачів критичної інфраструктури.

3.1.3. Процес розробки метрик

Процес розробки цієї метрики є систематичним і постійним кроком, який включає кілька важливих етапів:

Аналіз тенденцій та моделей кіберзагроз: Зосередьтеся на аналізі тенденцій та закономірностей кіберзагроз без необхідності збирати конкретні дані. Визначте загальні характеристики попередніх атак, часто цільову інфраструктуру та відповідні показники ефективності. Розуміючи ці тенденції, можна розробити стратегічні ідеї для підвищення безпеки без подальшого збору даних.

Впровадження показників безпеки: Зосередьтеся на впровадженні показників безпеки, використовуючи всю раніше ідентифіковану інформацію. Це передбачає застосування формул або рівнянь, призначених для вимірювання безпеки на основі

виявлених тенденцій та закономірностей кіберзагроз. Крім того, впровадження метрики має враховувати такі фактори, як відповідність метрики організаційним цілям, зручність використання метрики та здатність метрики надавати значну інформацію.

Контекстний аналіз та метрична оцінка: На цьому етапі основна увага приділяється контекстному аналізу та метричній оцінці. Це передбачає вивчення реальних ситуацій, не покладаючись на тестування. Процес може включати оцінки на основі наративу, пов'язані з ефективністю метрики у зображенні потенційних кіберзагроз, з якими стикаються організації. Метрична оцінка також повинна враховувати надійність, узгодженість та актуальність метрики для екологічної динаміки безпеки.

Розширений розвиток: Цей етап передбачає перегляд та вдосконалення метрики на основі результатів тестування та відгуків користувачів. Це може включати коригування формул або рівнянь, додавання або віднімання метричних компонентів або зміни в процесах збору даних. Мета полягає в тому, щоб забезпечити, щоб метрика залишалася актуальною та ефективною при вимірюванні кіберстійкості критичної інфраструктури.

3.1.4. Застосування метрики

Показник кіберстійкості в критичній інфраструктурі має кілька важливих застосувань:

Оцінка поточних рівнів стійкості: Організації можуть використовувати цей показник для оцінки поточного рівня кіберстійкості та визначення областей, де потрібні вдосконалення. Це допомагає організаціям визначити пріоритети для заходів щодо вдосконалення та планувати ефективні стратегії підвищення кіберстійкості.

Порівняння зі стандартами та правилами: Цей показник дозволяє організаціям порівнювати свій рівень стійкості з галузевими стандартами або

чинними правилами. Це допомагає організаціям забезпечити дотримання існуючих керівних принципів та правил та визначити сфери, де їм може знадобитися внести покращення.

Планування та розподіл ресурсів: Цей показник допомагає організаціям планувати ефективні зусилля з розподілу ресурсів для підвищення кіберстійкості. За допомогою даних, згенерованих метрикою, організації можуть визначити пріоритети використання своїх ресурсів та планувати ефективні стратегії підвищення кіберстійкості.

Звітність та підзвітність: Цей показник можна використовувати для надання звітів про стан кіберстійкості зацікавленим сторонам та регулюючим органам. Це вирішальний крок у підтримці прозорості та підзвітності щодо безпеки критичної інфраструктури.

Порівняння з іншими організаціями: Цей показник дозволяє порівнювати з іншими організаціями в тому ж секторі або аналогічному секторі. Завдяки цьому порівнянні організації можуть визначити найкращі практики та побачити, як вони порівнюються з іншими організаціями.

Розробка метрики кіберстійкості в критичній інфраструктурі є вирішальним кроком у захисті все більш взаємопов'язаної критичної інфраструктури від складних кіберзагроз. Цей показник дає чітке уявлення про те, наскільки добре критична інфраструктура захищена і може відновитися в надзвичайних ситуаціях. Таким чином, цей показник є не лише інструментом вимірювання, але й життєво важливим інструментом забезпечення безперервності діяльності критичної інфраструктури, що має вирішальне значення для добробуту та стійкості нашого суспільства та сучасної економіки. Зіткнувшись з розвитком кіберзагроз, розробка цієї метрики є активним кроком у забезпеченні стійкості критичної інфраструктури, що має вирішальне значення для нашого добробуту та стійкості.

3.2. Зміцнення стійкості в критичній інфраструктурі

Щоб зрозуміти тонкощі стійкості критичної інфраструктури та чому вона має вирішальне значення у все більш взаємопов'язаному та складному світі, нам потрібно глибше заглибитися в цю концепцію. У контексті критичної інфраструктури стійкість відноситься до здатності системи витримувати і функціонувати відповідно до її основних цілей. Наприклад, при розгляді рішень для резервного копіювання основною метою є підтримка надійності системи в умовах потенційних втрат даних, які можуть стати значною катастрофою, якщо не обробляти належним чином. Ось чому стійкість стає ключовим у захисті роботи критичної інфраструктури, часто під високим тиском.

3.2.1. Стійкість проти надійності: відмінності та взаємозв'язок

Важливо розрізняти "стійкість" та "надійність", оскільки ці терміни часто використовуються як взаємозамінні. У контексті критичної інфраструктури стійкість, по суті, є ключовим елементом досягнення високого рівня надійності. Тому, хоча стійкість - це процес, який дозволяє інфраструктурі продовжувати працювати навіть у складних умовах, надійність є бажаним результатом цього процесу. Ми можемо розглядати стійкість як основу, яка забезпечує надійність. Багато в чому стійкість має вирішальне значення для досягнення бажаної надійності критичних інфраструктурних систем.

Хоча вони концептуально відрізняються, стійкість і надійність також відрізняються кількісно. У цьому контексті стійкість може бути визначена як функція первинних заходів надійності. Наприклад, стійкість (R) може бути наближена як

R=(1−M□T□T□R/M□T□B□F)

де MTTR означає середній час відновлення, а MTBF означає середній час між невдачами. Рівняння передбачає, що скорочення часу відновлення та підвищення операційної стабільності сприяють більшій загальній стійкості. Хоча в цьому дослідженні не включено жодних емпіричних доказів для перевірки цієї формули, рівняння пропонує основу для подальшого моделювання та польових випробувань. Подальші дослідження можуть аналізувати історичні записи про інциденти з метою калібрування та впровадження цього заходу для різних видів інфраструктури.

3.2.2. Вирішення різноманітних проблем

Критична інфраструктура стикається з різними проблемами, які можуть вплинути на її діяльність. Фізичні загрози, такі як стихійні лиха, терористичні атаки та все більш складні кіберзагрози, є конкретними прикладами цих проблем. В операційній реальності рішення щодо стійкості часто зосереджуються на групах потенційних факторів, які можуть порушити інфраструктуру. Глибоко розуміючи ці фактори, ми можемо розробити більш ефективні та надійні стратегії стійкості для вирішення цих різноманітних проблем.

3.2.3. Механізми відмовостійкості: серце стійкості критичної інфраструктури

У контексті критичної інфраструктури механізми відмовостійкості є ключовим елементом, який забезпечує надійну та безперервну роботу. Ці механізми складаються з двох основних шарів. По-перше, існує рівень бізнес-логіки, відповідальний за підтримку нормальної роботи системи, гарантуючи, що всі операції протікають за планом. Потім є мета-шар, який обробляє помилки та процес відновлення у разі збоїв. Ця концепція забезпечує гнучкість у впровадженні відмовостійкості в існуючій або розвивається інфраструктурі. Більше того, важливо зосередитися не тільки на стійкості фізичної інфраструктури, але й на стійкості агентів або модулів моніторингу, які часто не беруться до уваги при плануванні стійкості. Деякі підходи навіть підкреслюють те, що називається "сірим

провалом", а не "важкою невдачею". Це означає, що основна увага приділяється стійкості до конкретних збоїв у обслуговуванні, а не просто зосереджується на потенційних збоях.

3.2.4. Категорії рішень стійкості для критичної інфраструктури

Якщо ми класифікуємо рішення щодо стійкості для критичної інфраструктури, ми можемо класифікувати їх на три основні категорії, як показано на рисунку 3.1:

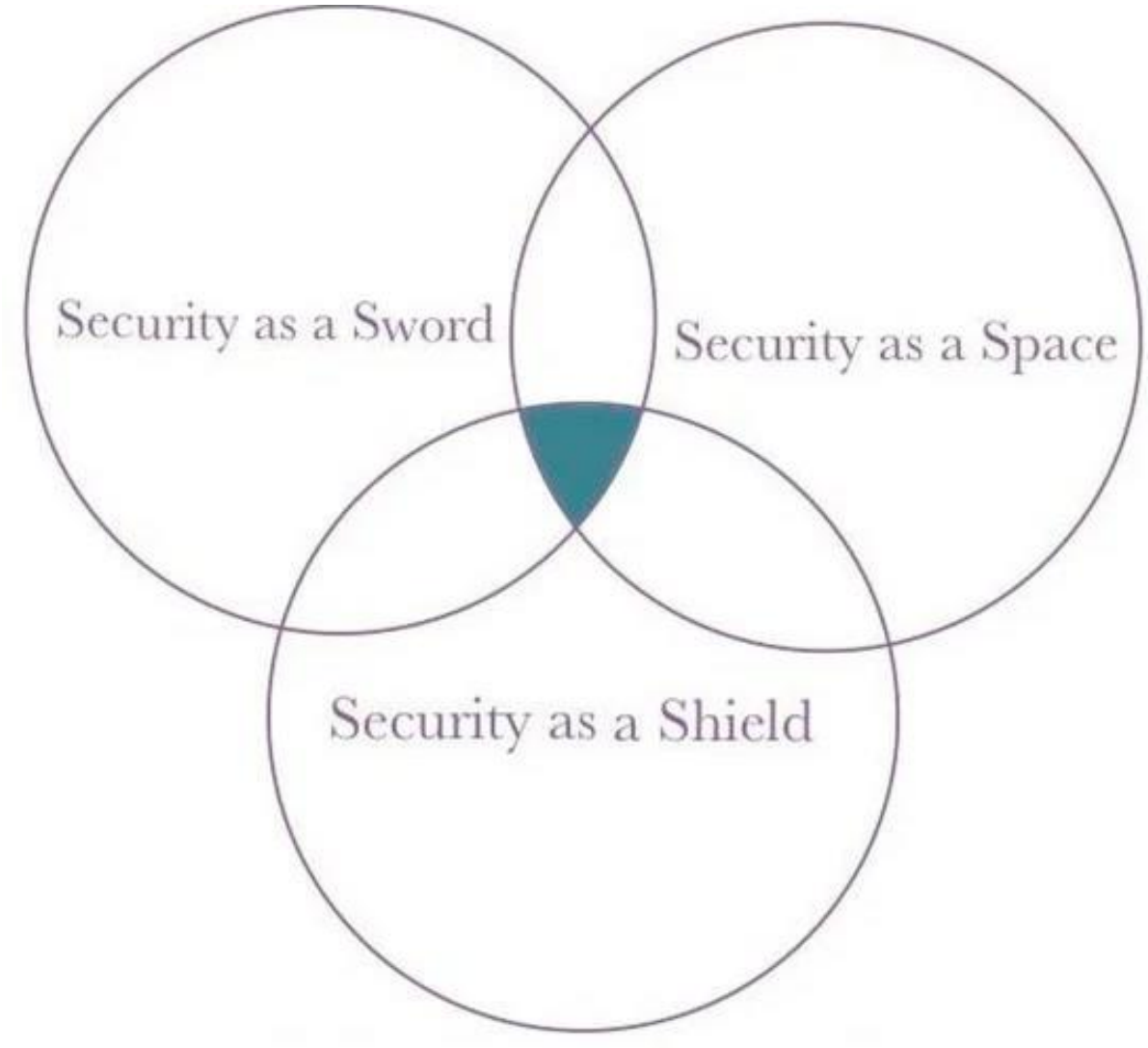


Рисунок 3.1 — Класифікація підходів до кібербезпеки.

Кіберпростір як щит: Ця категорія включає різні важливі аспекти, такі як ситуаційна обізнаність, забезпечення безпеки та принципи стійкості. Основна увага цієї категорії приділяється захисту систем та даних від різних загроз та атак. Ситуаційна обізнаність передбачає розуміння та знання середовища операційної системи та того, як зміни в навколишньому середовищі можуть вплинути на роботу системи. Забезпечення безпеки включає в себе ряд кроків, вжитих для забезпечення захисту системи від різних загроз та атак. Принципи стійкості відносяться до фундаментальних принципів, що керують проектуванням та експлуатацією систем для забезпечення їх стійкості до загроз.

Кіберпростір як простір: Друга категорія включає такі аспекти, як управління ризиками, стійкість інфраструктури та готовність інфраструктури. Основна увага цієї категорії полягає в тому, щоб критична інфраструктура могла ефективно та результативно працювати в різних умовах. Управління ризиками включає в себе виявлення, оцінку та визначення пріоритетів ризиків, а потім розподіл ресурсів для мінімізації, моніторингу та контролю впливу ризику. Стійкість інфраструктури відноситься до здатності інфраструктури протистояти та відновлюватися після різних загроз та викликів. Готовність інфраструктури передбачає превентивні кроки для підготовки інфраструктури до потенційних загроз та атак.

Кіберпростір як меч: Третя категорія включає такі аспекти, як активна оборона, обізнаність про критичну інфраструктуру, політика захисту інфраструктури та відновлення критичних інцидентів. Основна увага цієї категорії полягає в тому, щоб вжити активних заходів для виявлення, запобігання та реагування на атаки на системи. Активний захист передбачає проактивні дії, вжиті для виявлення, запобігання та реагування на атаки на системи. Поінформованість про критичну інфраструктуру передбачає розуміння важливості критичної інфраструктури та того, як вразливості цієї інфраструктури можуть вплинути на національну безпеку та економіку. Політика захисту інфраструктури включає політику та процедури, призначені для захисту інфраструктури від фізичних та

кіберзагроз. Відновлення критичних інцидентів включає в себе кроки, вжиті після інциденту, щоб відновити нормальну роботу системи якомога швидше.

Модель, відома як "InfraGuard Cybersecurity Framework", формується цими трьома основними категоріями рішень щодо стійкості критичної інфраструктури Таблиця 3.1. Ця модель забезпечує чітке та всебічне уявлення про загальну структуру структури. Переглянувши цю модель, ми можемо зрозуміти, як кожна частина фреймворку взаємодіє та працює разом, щоб сформувати надійну та ефективну систему безпеки. На рисунку 3.2 показана ця модель. Важливо пам'ятати, що критична інфраструктура є основою нашого повсякденного життя, як економічно, так і з точки зору національної безпеки. Завдяки глибокому розумінню концепцій стійкості в контексті критичної інфраструктури ми можемо краще підготуватися до різних потенційних загроз. Зі збільшенням взаємозв'язку світу та зростаючою складністю кібератак ефективні стратегії стійкості стають все більш важливими для підтримки операційної безперервності та соціальної безпеки. Постійно розробляючи та впроваджуючи відповідні рішення щодо стійкості, ми можемо підвищити стійкість нашої критичної інфраструктури та захистити наше майбутнє. Крім того, розуміння концепції стійкості також допомагає нам оцінити роль критичної інфраструктури у підтримці стабільності нашого соціального та економічного життя, що в кінцевому підсумку впливає на якість нашого життя. Тому підготовка критичної інфраструктури є спільною відповідальністю для всіх нас. Оскільки ми рухаємося до все більш складного майбутнього, стійкість критичної інфраструктури є міцною основою, яка допоможе нам впевнено та впевнено протистояти викликам.

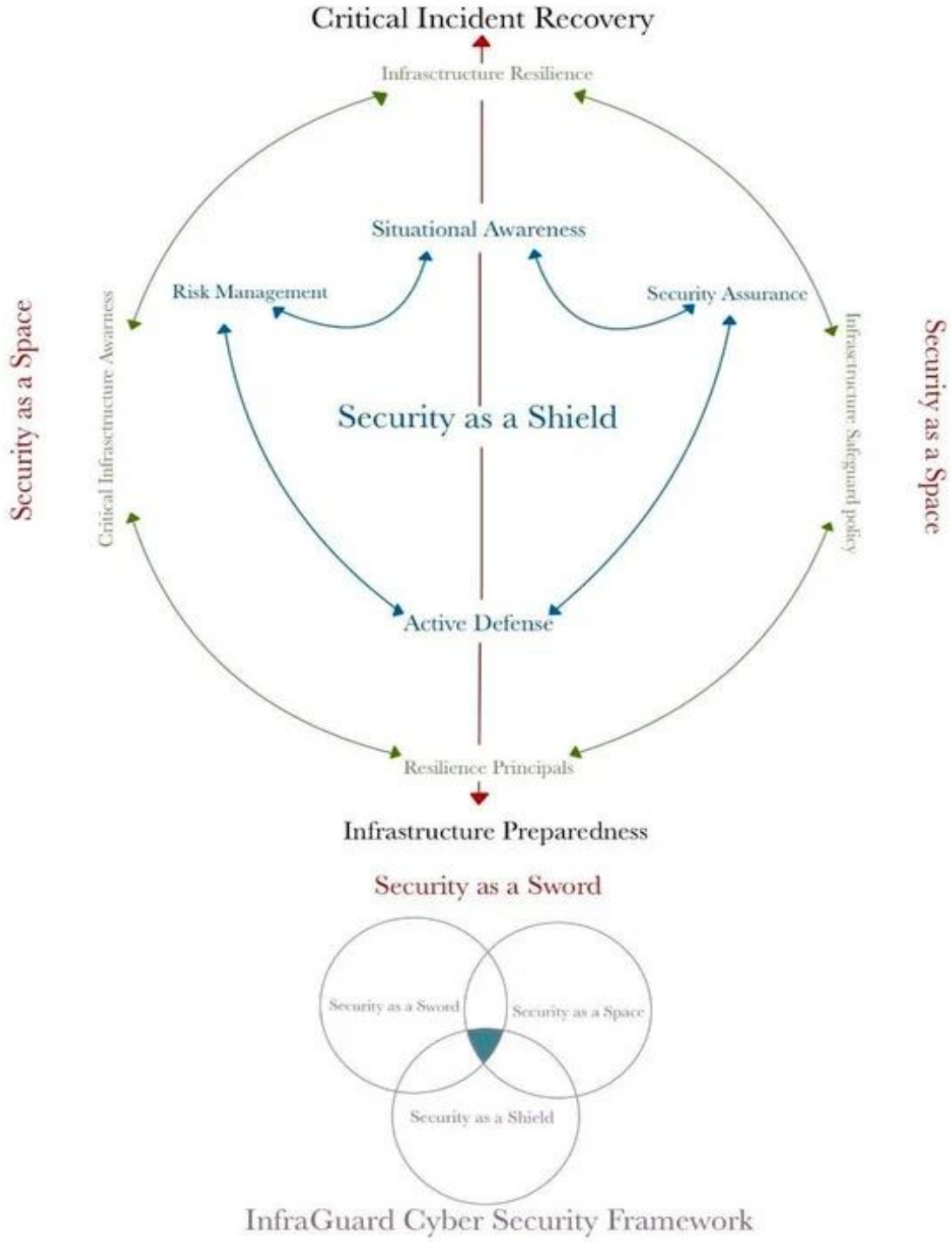


Рисунок 3.2 — Система кібербезпеки InfraGuard

Таблиця 3.1— Домени та компоненти в рамках кібербезпеки для критичної інфраструктури.

Домен	**Компонент**	**Індикатор**	**Опис**
Кіберпростір як щит	Ситуаційна обізнаність	Можливості виявлення та моніторингу загроз	Організація може проактивно спостерігати за оперативними змінами та виявляти потенційні кіберзагрози.
	Гарантія безпеки	Оцінки ризиків та контроль безпеки	Включає рутинні оцінки та дотримання суворих стандартів для забезпечення захисту системи.
	Активний захист	Швидке реагування на загрози	Передбачає використання інструментів та стратегій для виявлення та запобігання атакам до того, як відбудеться пошкодження системи.
	Управління ризиками	Ідентифікація та пом'якшення ризиків	Систематичний процес оцінки загроз та визначення пріоритетів заходів щодо пом'якшення наслідків.
Кіберпростір як простір	Стійкість інфраструктури	Надійність системи та можливості відновлення	Інфраструктура може підтримувати роботу та відновлюватися під час або після кіберінцидентів.

	Поінформованість про критичну інфраструктуру	Організаційна обізнаність про життєво важливі системи	Глибоке розуміння національного значення інфраструктури та пов'язаних з нею ризиків.
	Принципи стійкості	Стійкий дизайн та операційна філософія	Основоположні принципи побудови систем, які можуть витримувати збої.
	Політика захисту інфраструктури	Захисна політика та процедури	Офіційні документи та процедури захисту фізичної та цифрової інфраструктури від загроз.
Кіберпростір як меч	Готовність інфраструктури	Попереджувальна готовність та навчання	Наявність планів реагування на інциденти, навчання персоналу та моделювання сценаріїв.
	Відновлення критичних інцидентів	Швидкість відновлення та заходи безперервності	Можливість швидко та ефективно відновлювати функції системи після збоїв.

3.3. Важливість моделей оцінки процесів у вимірюванні стійкості

Щоб глибше зрозуміти концепцію стійкості в контексті критичної інфраструктури, необхідно вивчити моделі оцінки процесів. Моделі оцінки процесів формують життєво важливу основу для детального розуміння та вимірювання стійкості, і це стає ключовим елементом у зусиллях щодо підвищення стійкості критичної інфраструктури. Ця модель складається з двох основних вимірів. Перший вимір - це тип процесу. Цей вимір відноситься до різних типів процесів, пов'язаних з критичною інфраструктурою. Ці процеси деталізовані та

згруповані за змістовними категоріями. Наприклад, це включає процеси кібербезпеки, процеси аварійного відновлення або процеси моніторингу та реагування.

Візуальна модель "InfraGuard Cybersecurity Framework" нещодавно синтезована авторами для кількісного визначення та визначення кіберстійкості для критичних інфраструктурних контекстів. Модель пропонує двовимірну методологію через перетин рівнів зрілості можливостей (рівень від 0 до рівня 5) та функціональних доменів, класифікованих як Кіберпростір як Щит, Кіберпростір як Простір та Кіберпростір як Меч. Ці метафоричні простори називаються індивідуально для інкапсуляції окремих шарів організаційного захисту через пасивний захист та надійність системи для активного управління інцидентами. Хоча складові компоненти (наприклад, ситуаційне зондування, надійність інфраструктури, відновлення інцидентів тощо) широко визнані в літературі з кібербезпеки, номенклатура, конфігурація та представлення діагональної матриці є новими для цього дослідження.

Ця структура бере концептуальні підказки з кількох визнаних моделей та стандартів. Ці вертикальні рівні зрілості базуються на концепціях у моделях зрілості можливостей, таких як ISO/IEC 15504 (зараз серія ISO/IEC 33000) та модель оцінки процесів COBIT, які окреслюють рівні складності та інституціоналізації процесу. Горизонтальна класифікація елементів відображає теми в рамках кібербезпеки NIST (ідентифікація, захист, виявлення, реагування, відновлення), перебудовані під новою таксономією. Крім того, модель заохочує філософію варіантів використання, таких як AI-CRM, STPA-Sec та DHS's Cyber Resilience Review, які підкреслюють використання складених, динамічних систем захисту. Об'єднавши ці фони в одну послідовну та просту для розуміння модель, ця структура є простим інструментом для оцінки, спілкування та керівництва вдосконаленням стратегії кіберстійкості.

Другим виміром у цій моделі є рівень компетентності. У цьому вимірі атрибути процесу згруповані за кількома рівнями компетентності. Ці атрибути є вимірюваними характеристиками, які допомагають нам класифікувати, наскільки ефективним і компетентним є процес у виконанні своїх завдань. Ці атрибути можуть включати здатність процесу виявляти загрози, реагувати на інциденти або планувати відновлення.

3.3.1. Рівні компетентності процесу в системі кіберстійкості InfraGuard

"InfraGuard Cyber Resilience Framework" - це важливий інструмент, який допомагає класифікувати процеси безпеки на шість рівнів на основі їх прогресу та ефективності. Як на графіку позначаються показники стійкості, можна побачити на ілюстрації на Рисунку 3.3.

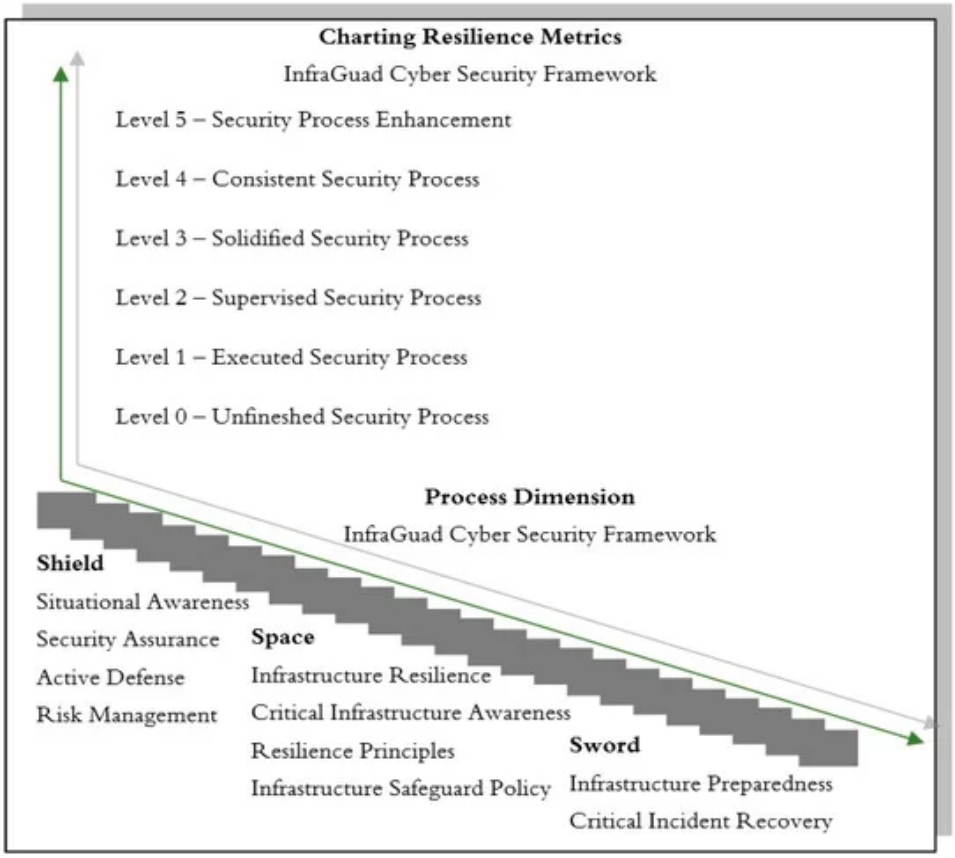


Рисунок 3.3 — Графік показників стійкості

Рівень 5 - Покращення процесу безпеки: Це найвищий рівень у структурі, де процеси безпеки були повністю оптимізовані. На цьому етапі процеси безпеки не тільки проходять гладко, але й постійно вдосконалюються та вдосконалюються на основі зворотного зв'язку та навчання на попередньому досвіді. Організації на цьому рівні досягли найвищого рівня зрілості в процесах безпеки, і кожен аспект оптимізований для повної ефективності. Організації на цьому рівні є лідерами в практиці кібербезпеки.

Рівень 4 — Послідовний процес безпеки: на цьому рівні процеси безпеки працюють послідовно та передбачувано. Процеси дають послідовні результати та відповідають встановленим стандартам якості. Послідовність тут є ключовою, а це означає, що організації можуть покладатися на процеси безпеки для досягнення передбачуваних результатів без особливих варіацій або невизначеності. Організації на цьому рівні досягли дуже високого рівня стійкості у підтримці кібербезпеки.

Рівень 3 — закріплений процес безпеки: на цьому рівні процеси безпеки стали надійними та усталеними. Процеси виявилися ефективними на практиці і стали невід'ємною частиною повсякденних операцій. Це вказує на те, що організації успішно побудували міцну основу для своєї безпеки, і ці процеси вважаються зрілими практиками в їх діяльності. Організації на цьому рівні досягли високого рівня стійкості в підтримці своєї критичної інфраструктури.

Рівень 2 - Контрольований процес безпеки: На цьому рівні процеси безпеки ретельно контролюються, щоб гарантувати, що всі дії відбуваються відповідно до запланованих та встановлених стандартів. Нагляд тут є вирішальним компонентом, і організації гарантують, що процеси безпеки розгортаються, як очікувалося, хоча все ще може бути місце для вдосконалення. Організації на цьому рівні прагнуть підвищити свою стійкість і планують необхідні кроки для досягнення вищого рівня.

Рівень 1 — Виконаний процес безпеки: На цьому рівні виконуються процеси безпеки. Основні заходи безпеки були впроваджені, і процеси працюють відповідно до базового плану. Це початковий крок, який вказує на те, що організація вжила основних заходів для захисту своєї інфраструктури. Поки робота все ще залишається, був зроблений перший крок до стійкості.

Рівень 0 — Незакінчений процес безпеки: це найнижчий рівень у системі, де процеси безпеки незавершені. Деякі аспекти процесів, можливо, не були реалізовані або можуть не функціонувати належним чином. Це вказує на те, що для досягнення гідного рівня стійкості потрібна значна робота.

3.3.2.Соціальний вимір у вимірах стійкості

Не тільки процеси та технології впливають на стійкість критичної інфраструктури. Соціальні фактори також відіграють вирішальну роль у тому, як люди взаємодіють та співпрацюють перед обличчям загроз. Рівень розуміння та обізнаності в суспільстві щодо загроз кібербезпеки значно впливає на здатність сприяти підтримці безпеки критичної інфраструктури. Чим вищий цей рівень розуміння та обізнаності, тим краще суспільство може брати участь у забезпеченні безпеки. Це розуміння включає знання про потенційні загрози та дії, які слід вжити в надзвичайних ситуаціях. Координація та співпраця між різними зацікавленими сторонами також стають вирішальними елементами стійкості. Здатність працювати разом та ефективно обмінюватися інформацією може покращити реагування на загрози та допомогти забезпечити безперервність критичних інфраструктурних операцій.

3.3.3. Інтеграція процесу та соціальних вимірів у вимірювання стійкості

Об'єднавши процес та соціальні виміри в вимірювання стійкості, ми можемо зрозуміти, як складна критична інфраструктура стикається з проблемами. Комплексне вимірювання передбачає оцінку організаційних процесів та розуміння громадськості, а також рівнів готовності та координації серед різних зацікавлених

сторін. Таким чином, ми можемо отримати більш глибоке уявлення про рівень стійкості критичної інфраструктури та визначити області, де потрібні вдосконалення.

3.3.4. Важливість багатовимірного підходу

Висновок, який можна зробити, полягає в тому, що вимірювання стійкості критичної інфраструктури є вирішальним кроком у забезпеченні кібербезпеки. В епоху все більш складних загроз не існує єдиного рішення, яке може гарантувати стійкість. Натомість багатовимірний підхід, який включає глибоке розуміння організаційних процесів, рівня компетентності у виконанні завдань безпеки, а також ролі та готовності суспільства, є ключем до досягнення більш високого рівня стійкості. Всі сторони, що беруть участь у критичній інфраструктурі, будь то уряд, приватні організації чи громадськість, повинні сприяти цим зусиллям для забезпечення безперебійної безперервності роботи. Зосереджуючись на всебічному вимірюванні та розумінні, ми можемо побудувати безпечніше майбутнє, яке є більш стійким до загроз кібербезпеки, що розвиваються. Завдяки спільним зусиллям та співпраці ми можемо підтримувати стійкість критичної інфраструктури, що, в свою чергу, допоможе захистити соціальну та економічну стабільність, від якої ми сильно залежимо. Роблячи це, ми можемо рухатися вперед у вирішенні майбутніх викликів, які є невидимими, але обов'язково з'являться.

3.4. Спектр стійкості

3.4.1. Концептуальна структура спектру стійкості

В епоху, що характеризується постійними змінами та невизначеністю в кіберсвіті, розуміння спектру стійкості є вирішальним зобов'язанням для захисту критичної інфраструктури та процесів. Це передбачає оцінку здатності процесу досягати бізнес-цілей, як поточних, так і очікуваних у майбутньому. Розмір можливостей є ключовим параметром при вимірюванні рівня стійкості процесів

або інфраструктури. Ця модель розглядає набір атрибутів процесу, згрупованих за різними рівнями можливостей, дотримуючись рекомендацій, наданих ISO/IEC 15504-2:2003 та COBIT 5. Ми класифікуємо індикатори можливостей для кожного аспекту: Кіберпростір як щит, Кіберпростір як простір та Кіберпростір як меч.

Крім того, спектр стійкості представлений на Рисунку 3.4, забезпечуючи візуальне зображення значення спектру у підвищенні стійкості критичних систем.

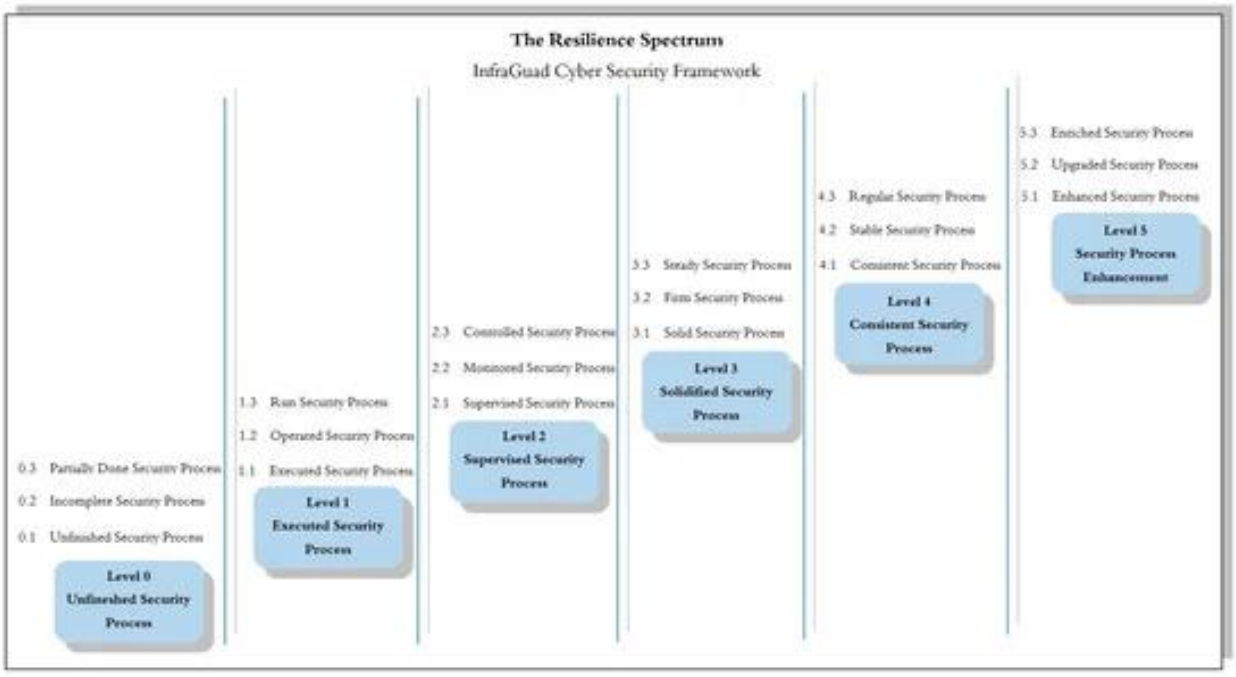


Рисунок 3.4 — Спектр стійкості.

Кіберпростір як щит:

Ситуаційна обізнаність: Ситуаційна обізнаність має вирішальне значення для підвищення стійкості до кіберзагроз. Організації та інфраструктура повинні активно контролювати та виявляти зміни у своєму операційному середовищі, які можуть вплинути на безпеку. Це включає моніторинг мережевого трафіку, аналіз підозрілих дій та розуміння поточних тенденцій кібератак.

Забезпечення безпеки: Забезпечення безпеки включає в себе дії, вжиті для забезпечення безпеки систем від загроз та атак. Це включає періодичні оцінки

ризиків безпеки, впровадження заходів щодо зменшення ризиків та забезпечення суворого дотримання стандартів безпеки.

Активний захист: здатність проводити активний захист має вирішальне значення. Організації повинні мати стратегії та інструменти, які дозволяють їм виявляти атаки якомога раніше, швидко реагувати і навіть вживати активних заходів для блокування або перешкоджанню атакам, перш ніж вони пошкодять систему.

Управління ризиками: Ефективне управління ризиками є життєво важливим компонентом кіберзахисту. Це передбачає виявлення, оцінку та управління ризиками, пов'язаними з кібератаками. Управління ризиками може допомогти організаціям визначити пріоритети зменшення ризиків та розподілити відповідні ресурси.

Кіберпростір як простір:

Стійкість інфраструктури: здатність інфраструктури витримувати та відновлюватися після різних загроз є ключем до створення безпечного простору в кіберконтексті. Це передбачає планування та реалізацію стратегій підтримки працездатності інфраструктури навіть у складних ситуаціях.

Поінформованість про критичну інфраструктуру: Усвідомлення важливості критичної інфраструктури є першим кроком до її захисту та зменшення ризиків. Організації повинні розуміти вразливості критичної інфраструктури та те, як її вразливості можуть вплинути на національну безпеку та економіку.

Принципи стійкості: Принципи стійкості повинні керуватися проектуванням та експлуатацією інфраструктури. Це включає фундаментальні принципи, які керують проектуванням, впровадженням та обслуговуванням інфраструктури, щоб залишатися стійкою до загроз.

Політика захисту інфраструктури: Політика та процедури, призначені для захисту інфраструктури від фізичних та кіберзагроз, є ключовими кроками у створенні безпечного простору в кіберконтексті.

Кіберпростір як меч:

Готовність інфраструктури: Готовність інфраструктури включає в себе превентивні заходи для підготовки інфраструктури до потенційних загроз та атак. Це включає планування, навчання персоналу та тестування сценаріїв безпеки.

Відновлення критичних інцидентів: Вжиття заходів після кіберінциденту для якнайшвидшого відновлення нормальної роботи системи має вирішальне значення. Це передбачає відновлення системи, відновлення даних та заходи, щоб уникнути подібних інцидентів у майбутньому.

У кіберсвіті, що постійно змінюється, глибоке розуміння спектру стійкості є ключем до захисту інфраструктури та забезпечення безперервності бізнесу. Організації повинні постійно адаптуватися та впроваджувати інновації, щоб протистояти викликам, що розвиваються. Завдяки більш глибокому розумінню кожного аспекту спектру стійкості організації можуть визначити області, які потребують вдосконалення та подальших інвестицій, гарантуючи, що вони можуть підтримувати свою стійкість у динамічному кіберсвіті. Оскільки кібератаки збільшуються, а ризики продовжують розвиватися, розуміння спектру стійкості є цінним посібником для забезпечення безпеки критичної інфраструктури та високопродуктивних процесів.

3.4.2. Кількісна модель оцінки для компонентів стійкості

Щоб запропонована структура застосовувалася на практиці, для кожного елемента системи кібербезпеки InfraGuard вводиться кількісна система підрахунку балів. Система дозволяє організаціям вимірювати свою зрілість кіберстійкості в різних функціональних сферах структурованим і вимірюваним способом. Перетворюючи якісні оцінки на чисельні оцінки, зацікавлені сторони можуть легше

зрозуміти існуючі прогалини, контролювати вдосконалення з часом та підтримувати прийняття рішень за допомогою доказових показників. Кожному елементу моделі, від ситуаційної обізнаності до відновлення інцидентів, присвоюється набір певних показників, які відображають її операційну зрілість. Він оцінюється за шкалою від 0 до 5, що вказує на збільшення рівнів зрілості, від неіснуючих або спеціальних процесів до повністю інтегрованих, автоматизованих та оптимізованих можливостей. Рейтинг базується на певних критеріях, таких як моніторинг покриття, доступність системи, дотримання політики та час відновлення, розроблений таким чином, щоб бути реалістичним та кількісним. Структура дозволяє технічним командам, не кажучи вже про керівництво, узгодити свою вимірювальну діяльність з глобальними стандартами, такими як ISO/IEC 15504, NIST CSF та COBIT. Значення оцінки, призначені для кожного компонента в Таблиці 3.2, призначені для відображення вимірюваних показників на основі наявних операційних даних. Ці значення можуть бути отримані за допомогою таких методів, як аудит системних журналів, відстеження часу безвідмовної роботи/часу простою, навчальні записи та структуровані експертні оцінки, залежно від можливостей внутрішнього моніторингу організації. Отримані оцінки на рівні компонентів сприяють загальній оцінці стійкості, як показано в Таблиці 3.3, яка об'єднує ці бали в загальну класифікацію рівня стійкості.

Таблиця 3.2 — Кількісні показники та оцінка для кожного компонента структури.

Компонент	**Індикатор**	**Критерії Вимірювання**	**Опис**

Ситуаційна обізнаність	% систем з моніторингом у реальному часі Середній час виявлення(MTTD)	На основі покриття моніторингу та середнього часу для виявлення аномалій	0: Немає системи моніторингу 1: Тільки ручне спостереження 2: Частковий моніторинг системи 3: Повна система періодично контролюється 4: Моніторинг у реальному часі 5: У режимі реального часу + автоматизоване виявлення аномалій з попередженням
Гарантія безпеки	Кількість впроваджених засобів контролю безпеки Статус сертифікації	Зверніться до впроваджених рамок (наприклад, ISO 27001) та задокументованих засобів контролю	0: Немає контролю чи сертифікатів 1: Тільки базовий брандмауер/AV 2: Реалізовано часткове управління 3: Формальна внутрішня політика з контролем 4: Сертифікація триває 5: Повна сертифікація (наприклад, ISO 27001) та сучасний контроль
Активний захист	Середній час для виявлення/відповіді(MTTD/MTTR) Кількість помилкових спрацювань	На основі чуйності системи та точності виявлення	0: Немає можливості відповіді 1: Затримка ручної відповіді (>72 год) 2: Ручний моніторинг, реактивна реакція 3: Напівавтоматичні сповіщення та пом'якшення наслідків 4: Повний план реагування на інциденти з автоматизацією 5: Автоматизоване виявлення та активний захист з <2% помилкових спрацьовувань

Управління ризиками	Частота оцінки ризиків % пом`якшених предметів високого ризику	На основі процесу управління ризиками та подальших дій	0: Немає оцінки ризику 1: Тільки Ad hoc оцінки 2: Щорічні оцінки ризиків 3: Квартальні оцінки 4: Задокументоване відстеження пом'якшення наслідків 5: Безперервний аналіз ризиків з виконанням зменшення ризику >90%
Стійкість інфраструктури	Час безвідмовної роботи системи(% доступності) Максимальний час простою на рік	На основі безперервності обслуговування та відмовостійкості	0: Нестабільна система, часті збої 1: Час простою >48 год/рік 2: Час простою 24–48 год/рік 3: Час простою 8–24 год/рік 4: Час простою <8 год/рік 5: Налаштування високої доступності з часом простою <1 год/рік
Поінформованість про критичну інфраструктуру	% критичних активів, виявлених та класифікованих Наявність інвентарізації критичних активів	На основі документації та визначення пріоритетів	0: Немає класифікації активів 1: Лише початковий список активів 2: Неповна інвентаризація 3: Повна класифікація, але застаріла 4: Актуальний список критичних систем 5: Інвентаризація, інтегрована з інструментами моделювання ризиків та загроз

Принципи стійкості	Впровадження систем резервування, резервного копіювання та відмовостійкості	На основі архітектурного дизайну та покриття надмірності	0: Немає механізмів стійкості 1: Тільки ручне резервне копіювання 2: Періодичні резервні копії та ізольовані плани відновлення 3: Надликові системи в основній інфраструктурі 4: Можливість часткового аварійного відмовостійкості 5: Повна резервність та автоматизоване відмовостійкість між системами
Політика захисту інфраструктури	Кількість політик, пов`язаних з безпекою Частота оновлення політики	На основі всебічності та актуальності офіційних політичних документів	0: Жодної офіційної політики 1: Єдина загальна політика 2: Кілька, але застарілих політик 3: Актуальна, рольова політика 4: Політика переглядається щорічно 5: Інтегрований, переглядається роз на два роки та узгоджений з національними/міжнародними стандартами
Готовність інфраструктури	Частота кібертренування % підготовленого персоналу	На основі програм готовності та регулярного тестування	0: Немає тренувань або тренувань 1: Базове навчання для деяких співробітників 2: Щорічне навчання для IT-команди 3: Щорічні навчання між відділами 4: Піврічні симуляції 5: Повна організація, що бере участь у щоквартальних симуляціях з підготовленим персоналом >90%

Відновлення критичних інцидентів	Середній час відновлення(MTTR) % послуг, відновлених в рамках SLA	На основі ефективності відновлення та відповідності SLA	0: Відновлення не визначено 1: MTTR >72 год 2: MTTR 48–72 год 3: MTTR 24–48 год 4: MTTR 4–24 год 5: MTTR <4 год, 100% відповідність SLA

Таблиця 3.3 — Загальний бал стійкості.

Оцінка	**Інтерпретація**
0–20	Низька Стійкість
21–35	Розвиток стійкості
36–45	Сильна стійкість
46–50	Оптимізована та адаптивна стійкість

Ця кількісна модель є не лише інструментом бенчмаркінгу, але й дорожньою картою для поступового вдосконалення кібербезпеки для критичних інфраструктур. Визначаючи слабкі області та визначаючи вимірювані цілі, організації можуть визначити пріоритети дій на основі їх терміновості та наявних ресурсів. Крім того, ця система підрахунку балів може підтримувати внутрішній аудит, огляди політики та прийняття інвестиційних рішень, а також міжорганізаційні порівняння та звітність перед регулюючими органами. Нарешті, таблиця пропонує короткий, адаптивний шаблон для перекладу складних понять стійкості в конкретні дії.

3.5. Результати

3.5.1. Показники продуктивності

Показники ефективності, як показано на Рисунку 3.5, використовуються для оцінки того, чи були досягнуті атрибути процесу.

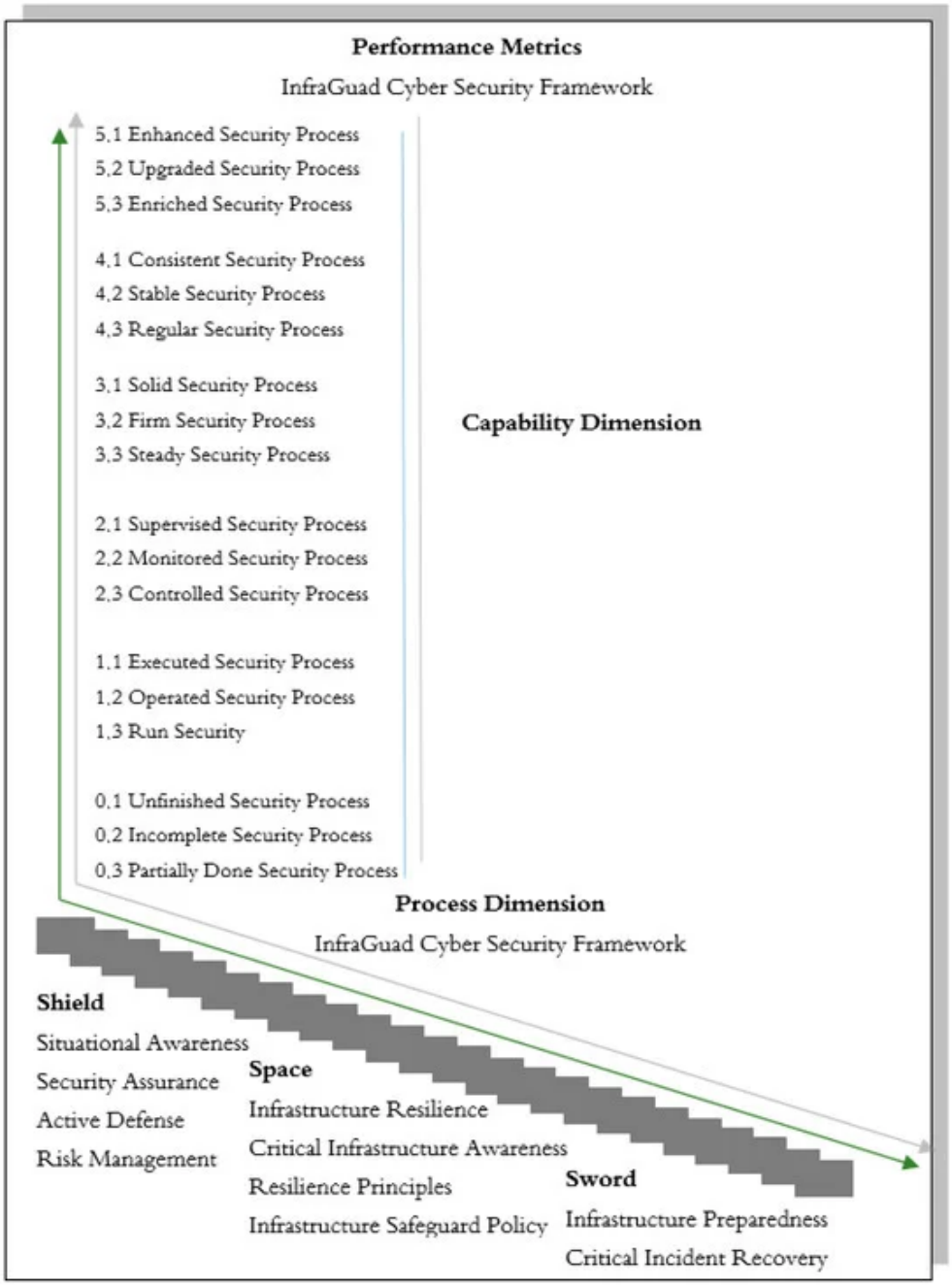


Рисунок 3.5 — Показники ефективності.

Щоб виміряти здатність організації або інфраструктури протистояти кіберзагрозам відповідно до трьох основних аспектів, Кіберпростір як щит, Кіберпростір як простір та Кіберпростір як меч, нижче наведено показники оцінки, які можна використовувати для забезпечення більш глибокого розуміння того, як організація або інфраструктура оцінює свою готовність протистояти кіберзагрозам:

Рівень 5 - Покращення процесу безпеки: На рівні 5 організації досягли своєї пікової готовності до все більш складних кіберзагроз. "Розширений процес безпеки", як центральний елемент на рівні 5, відображає високий рівень впровадження новітніх технологій. Організації на цьому рівні не тільки не відстають від останніх розробок, але й активно впроваджують інновації. На додаток до впровадження новітніх технологій, вони також впроваджують заходи постійного вдосконалення, включаючи комплексні оновлення технологій, політики та практики безпеки. Процеси безпеки на рівні 5 - це ідеальне поєднання передових технологій та безперервної оптимізації. "Оновлений процес безпеки" підкреслює, що процеси безпеки були значно покращені з точки зору їх ефективності, ефективності та надійності. Організації 5-го рівня успішно створили процеси безпеки, які працюють з високим рівнем надійності, послідовно та ефективно реагуючи на загрози. Вони впровадили технологічні оновлення та всебічно вдосконалили свою політику безпеки. Крім того, "Збагачений процес безпеки" акцентує увагу на глибокому розумінні кіберзагроз. Організації 5-го рівня не тільки покладаються на високотехнологічні технології, але й поглиблюють своє розуміння різних загроз. Вони залучають різних зацікавлених сторін і застосовують цілісний підхід до боротьби з кібератаками. Їхні процеси безпеки не тільки пом'якшують ризики, але й надають цінну інформацію для прийняття виконавчих рішень. Організації на рівні 5 служать прикладами інновацій, адаптації та лідерства у протиді кіберзагрозам.

Рівень 4 - Послідовні процеси безпеки: Рівень 4 підкреслює узгодженість та надійність у виконанні процесів безпеки. "Послідовний процес безпеки" вказує на

те, що організації можуть регулярно здійснювати заходи безпеки та обимати стабільні результати. Вони можуть послідовно реагувати на загрози та прогнозувати їх результати. Організації 4-го рівня досягли чудової дисципліни та узгодження у виконанні процесів безпеки. Вони регулярно виконують дії безпеки, створюючи дуже високий рівень готовності. "Стабільний процес безпеки" вказує на те, що процеси безпеки працюють стабільно та послідовно. Вони успішно підтримували надійність своїх процесів безпеки в умовах змін в операційному середовищі. Організації 4-го рівня досягли стадії, коли їхні процеси безпеки залишаються ефективними навіть перед обличчям кіберзагроз, що швидко розвиваються. "Регулярний процес безпеки" відображає дисципліну організації у виконанні процесів безпеки відповідно до існуючої політики та керівних принципів. Вони забезпечили ретельне дотримання кожного кроку відповідно до встановлених процедур. Крім того, рівень 4 - це етап, на якому організації успішно досягли балансу між гнучкістю та дисципліною у виконанні процесів безпеки. Вони можуть адаптуватися до нових загроз і реагувати з високою послідовністю. Організації 4-го рівня є прикладами дисципліни, послідовності та надійності у протидінні кіберзагрозам.

Рівень 3 - Затверділі процеси безпеки: Рівень 3 - це етап, коли організації успішно закріпили свої процеси безпеки як невід'ємну частину своїх повсякденних операцій. "Процес надійної безпеки" вказує на те, що процеси безпеки стали надійними та усталеними. Ці процеси виявилися ефективними у захисті даних, систем та організаційних операцій. Вони успішно створили сильну та проактивну культуру безпеки по всій організації. Організації на рівні 3 мають дуже високий рівень готовності протистояти кіберзагрозам. "Фірм процес безпеки" вказує на те, що процеси безпеки функціонують безпечно та забезпечують надійний захист від кібератак. Організації на рівні 3 можуть протистояти атакам з упевненістю, що їхні процеси безпеки збережуть цілісність, конфіденційність та доступність їхньої інформації. Вони побудували міцну основу для підтримки кібербезпеки у всій

організації. "Стійкий процес безпеки" - це етап, коли процеси безпеки працюють стабільно і можуть ефективно справлятися зі загрозами. Вони досягли балансу між реагуванням на кіберзагрози та повсякденними операціями. Організації на рівні 3 є зразками для наслідування в інтеграції безпеки в кожен аспект своєї діяльності, що призводить до сильної стійкості до кіберзагроз.

Рівень 2 - Контрольовані процеси безпеки: На рівні 2 жорсткий нагляд займає центр уваги. "Процес безпеки під наглядом" вказує на те, що організації гарантують, що вся діяльність відбувається відповідно до встановлених планів та стандартів. При суворому нагляді організації можуть забезпечити дисципліну у виконанні процесів безпеки. Цей нагляд включає в себе моніторинг діяльності та забезпечення відповідності дій встановленим планам та стандартам. Організації 2-го рівня мають надійну систему нагляду, яка забезпечує узгодженість у виконанні процесів безпеки. "Моніторований процес безпеки" зазначає, що процеси безпеки регулярно контролюються для виявлення аномалій або порушень політики, які можуть виникнути. Цей активний нагляд дозволяє організаціям швидко виявляти проблеми та реагувати відповідним чином. Організації 2-го рівня досягли високого рівня нагляду, що дозволяє їм ефективно виявляти та вирішувати потенційні ризики. "Процес контролю безпеки" підкреслює вжиття заходів безпеки з жорстким контролем відповідно до існуючих керівних принципів. У цьому контексті контроль має вирішальне значення для забезпечення того, щоб процеси безпеки йшли так, як очікувалося. Організації 2-го рівня досягли високого рівня нагляду та жорсткого контролю при виконанні своїх процесів безпеки.

Рівень 1 - Виконані процеси безпеки: На рівні 1 організації впровадили основні заходи безпеки та виконали їх відповідно до основних політик. Цей процес являє собою початкові кроки у створенні фундаменту для більш високого рівня безпеки. Вони почали свій шлях до більш високого рівня безпеки. "Виконаний процес безпеки" вказує на те, що організації 1-го рівня ефективно впровадили основні заходи безпеки. Вони виконують процеси безпеки відповідно до основних

політик та встановлених керівних принципів. Хоча вони все ще знаходяться на ранніх стадіях шляху до вищої готовності протистояти кіберзагрозам, ці початкові кроки демонструють їхню прихильність захисту своїх активів та даних. "Процес безпеки, що працює" відображає, що організації 1-го рівня виконують процеси безпеки відповідно до основних політик, хоча вони ще не досягли високого рівня узгодженості. Це початковий етап побудови міцної основи для виконання процесів безпеки. Вони почали свою подорож, щоб підвищити свою безпеку, але потрібно більше часу та зусиль, щоб досягти більш високих рівнів. "Запускати процес безпеки" показує, що процеси безпеки виконуються, хоча і все ще на ранніх стадіях розробки та впровадження. Організації на рівні 1 зробили перші кроки на своєму шляху до більш високих рівнів безпеки. Вони ініціювали зусилля для підвищення своєї безпеки, але все ще потребують подальшого розвитку та більш глибокого розуміння кіберзагроз.

Рівень 0 - Незавершений процес безпеки: На рівні 0 організації усвідомлюють, що їхні процеси безпеки незавершені і вимагають подальшого планування та дій для впровадження. Цей процес все ще знаходиться на ранніх стадіях проектування і потребує більш глибокого розуміння кіберзагроз, з якими стикаються. Організації на рівні 0 усвідомлюють, що їм потрібно почати свій шлях до кіберзагроз і спланувати кроки, які вони зроблять. "Незакінчений процес безпеки" відображає, що організації на рівні 0 визначили, що необхідні подальші зусилля для підвищення їх безпеки. Їхні процеси безпеки все ще знаходяться на ранніх стадіях проектування і не були повністю реалізовані. Це заклик до вдосконалення та розвитку процесів безпеки. "Неповний процес безпеки" вказує на те, що деякі аспекти процесів безпеки, можливо, не були реалізовані або можуть не функціонувати належним чином. Організаціям потрібно більше зусиль для усунення цих слабких сторін та забезпечення більш повного виконання їхніх процесів безпеки. "Частково зроблений процес безпеки" свідчить про те, що деякі заходи безпеки, можливо, були вжиті, але ці процеси все ще далекі від очікуваної

ефективності. Організації на рівні 0 ініціювали зусилля щодо підвищення своєї безпеки, але все ще потребують подальшого розвитку та більш глибокого розуміння кіберзагроз.

Рівень готовності протистояти кіберзагрозам є невід'ємною складовою підтримки безпеки та безперервності організаційних операцій, інфраструктури та інформаційних систем у нинішню цифрову епоху. Ця готовність охоплює кілька важливих аспектів, які формують основу оборони та стійкості до все більш складних кібератак. Одним з основних аспектів готовності до кіберзагроз є впровадження технологій. Організації на передньому краї готовності можуть прийняти новітні технології в контексті кібербезпеки. Вони впроваджують передові рішення та інструменти безпеки, які допомагають їм виявляти, пом'якшувати та ефективно реагувати на загрози. Впровадження новітніх технологій також включає постійне оновлення та моніторинг нових розробок у технології безпеки. Організації, які можуть слідувати тенденціям технологій безпеки, мають перевагу у стиканні з постійно розвиваються кіберзагрозами. На додаток до впровадження технологій, послідовність у виконанні процесів безпеки є ключовим фактором готовності. Послідовність передбачає рутинне та передбачуване виконання заходів безпеки. Організації з послідовними процесами безпеки виконують їх з високим рівнем замовлення, отримуючи стабільні результати. Послідовність також включає підтримку надійності процесів безпеки в умовах змін в операційному середовищі. Висока послідовність у виконанні процесів безпеки створює високий рівень довіри до захисту активів та даних.

Нагляд є ще одним важливим аспектом готовності до кіберзагроз. Організації, які впроваджують суворий нагляд, гарантують, що вся діяльність відбувається відповідно до встановлених планів та стандартів. Завдяки суворому нагляду організації можуть гарантувати, що процеси безпеки виконуються з дисципліною та відповідно до існуючих керівних принципів. Цей нагляд включає моніторинг заходів безпеки для виявлення аномалій або порушень політики, які

можуть статися. Організації, які можуть швидко виявляти проблеми та реагувати відповідним чином, мають перевагу у зіткненні з кіберзагрозами. Цілісність процесів безпеки є ключовою основою готовності до кіберзагроз. Організації, які забезпечують цілісність процесів безпеки, суворо виконують процедури та політику, запобігаючи порушенням або маніпуляціям, які можуть спробувати зловмисники. Цілісність також включає глибоке розуміння кіберзагроз та дотримання сильних принципів безпеки. Організації з безкомпромісними процесами безпеки мають сильніший захист від кібератак.

Адаптація та інновації також є важливими елементами готовності до кіберзагроз. Організації, які можуть швидко адаптуватися до нових загроз та впроваджувати інноваційні рішення безпеки, мають перевагу у стиканні все більш складними атаками. Здатність реагувати на кіберзагрози гнучко та креативно дозволяє організаціям залишатися попереду в боротьбі з кіберзловмисниками. На додаток до технічних аспектів, культура безпеки також відіграє вирішальну роль у готовності. Організації, які створюють сильну культуру безпеки, заохочують усіх членів команди надавати пріоритет безпеці в кожній дії та рішенні, яке вони приймають. Культура безпеки формує проактивне ставлення до кіберзагроз і перетворює безпеку на спільну відповідальність. Завдяки сильній культурі безпеки організації можуть створити більш ефективний захист від кібератак. Періодичні оцінки готовності є важливим інструментом, який допомагає організаціям визначити свій рівень готовності до протистояння кіберзагрозам. Розуміючи, наскільки вони просунулися в кожному аспекті готовності, організації можуть планувати та впроваджувати постійні вдосконалення. Періодичні оцінки також дозволяють організаціям відстежувати свій прогрес у підвищенні рівня готовності до кібербезпеки. Поєднання впровадження технологій, узгодженості, нагляду, цілісності процесів безпеки, адаптації, інновацій та культури безпеки формує комплексну основу для протистояння кіберзагрозам. Організації, які добре поєднують ці елементи, мають сильний захист від постійно розвиваються

кіберзагроз. Сильна готовність до кібербезпеки не тільки захищає організаційні дані та операції, але й захищає сучасне суспільство та економіку від згубного впливу кібератак.

На Рисунку 3.6 шестиступенева модель зрілості, показана вище, - це та, яка використовувалася при кількісній оцінці процесів кіберстійкості в критичних інфраструктурних умовах. Позиція кожного рівня визначає іншу операційну позицію, від рівня 0 (незавершено), де не було формалізовано жодних процесів безпеки, до рівня 5 (підвищення), де процеси безпеки проактивно реактивні та постійно оптимізуються. Ці етапи були названі Репортивними, Реактивними, Профілактичними, Детективними, Чуйними та Адаптивними, після прогресу від базової звітності та реакції до активного захисту, виявлення та довгострокової стійкості. Цей перехід зрілості дозволяє організаціям визначити, де вони знаходяться сьогодні, і збалансувати пріоритетний розвиток у певних сферах у всіх функціях безпеки як основу для моделі підрахунку балів, описаної в наступному розділі.

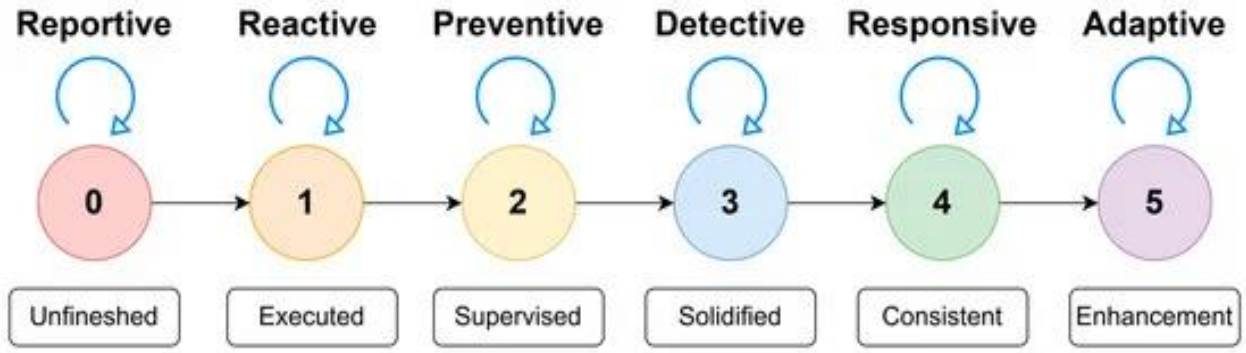


Рисунок 3.6 — Рівні зрілості в розробці процесу кіберстійкості.

3.5.2. Оцінка стійкості

Оцінки безпеки є вирішальним кроком у вимірюванні готовності організації протистояти кіберзагрозам. Цей процес оцінки використовує стандартну шкалу оцінювання для вимірювання того, наскільки організація досягла своїх цілей безпеки. Нижче наведено більш глибоке пояснення шкали оцінювання та її реалізації:

D (Не відповідає): Якщо елемент безпеки або досягнення отримує оцінку "D", це вказує на те, що елемент ще не досяг своєї мети. Оцінка "D" вказує на те, що досягнення цього елемента знаходиться в діапазоні від 0% до 20%. Це тривожний момент, оскільки він означає значні слабкі сторони цього елемента. Організації повинні негайно виявляти та усувати ці недоліки, щоб досягти належного рівня безпеки.

A (Наближення): Коли елемент або досягнення оцінюється як "A", це вказує на те, що елемент наближається до своєї мети, але все ще знаходиться в діапазоні від 20% до 50%. Це показує прогрес, але все ще потрібна робота, щоб досягти бажаного рівня безпеки. Організації повинні внести подальші вдосконалення для досягнення належного рівня безпеки.

M (Помірно відповідає): Оцінка "M" вказує на те, що елемент або досягнення були помірно виконані, з досягненнями в діапазоні від 50% до 75%. Це позитивний знак того, що організація досягла значного прогресу в досягненні кращої безпеки. Однак є місце для подальшого вдосконалення для досягнення оптимального рівня безпеки.

W (Добре досягнуто): Оцінка "W" означає, що елемент або досягнення були добре досягнуті, з досягненнями в діапазоні від 75% до 90%. Це похвальний рівень міцності безпеки, але все ще дозволяє внести незначні покращення. Організації повинні контролювати цей елемент, щоб підтримувати хороший рівень безпеки.

E (Перевищує Очікування): Коли елемент або досягнення отримує оцінку "E", це означає, що елемент не тільки досяг, але й перевершив очікування, досягнувши дуже високого рівня безпеки в діапазоні від 90% до 100%. Це видатне досягнення, яке демонструє здатність організації підтримувати безпеку на найвищому рівні. Важливо продовжувати контролювати та підтримувати цей дуже високий рівень безпеки.

Крім того, оцінка стійкості представлена в Таблиці 3.4, що забезпечує візуальне зображення оцінки стійкості та ступеня, в якій організація досягла своїх цілей безпеки.

Таблиця 3.4 — Градування стійкості.

Оцінка стійкості		
Скорочення	**Опис**	**% Досягнуто**
Д	Не Зустрівся	Досягнення 0–20%
А	Наближається	>20–50% досягнення
М	Помірно Зустрівся	>50–75% досягнення
В	Добре Досягнутий	>75–90% досягнення
Е	Перевершує Очікування	>90–100% досягнення

Важливість оцінки міцності безпеки полягає в тому, що це безперервний процес. Організації повинні періодично переоцінювати, щоб контролювати зміни в середовищі кібербезпеки та гарантувати, що всі елементи безпеки залишаються адекватними. У цьому процесі не повинно бути значних недоліків, пов'язаних з оціненими атрибутами. Послідовність має вирішальне значення для визначення призначених оцінок, як описано в Таблиці 3.4 щодо оцінок з точки зору досягнутих відсотків. Оцінювачі використовують цю шкалу для визначення рівня досягнутих можливостей. Послідовно застосовуючи ці критерії, кожна оцінка може ґрунтуватися на структурованому рівні формальності. Це дозволяє не тільки

проводити порівняння по всій організації, але й у різних компаніях. Таким чином, цей процес оцінки стає вирішальним інструментом для забезпечення безпеки та ефективності організацій.

3.5.3. Дослідницькі сценарії для застосування Framework

Щоб проілюструвати використання системи кібербезпеки InfraGuard на реальній практиці, представлені три сценарії дослідницьких випадків, по одному для кожного дискретного сектору критичної інфраструктури. Вигадані сценарії імітують високоефективні кібератаки та показують використання структури для оцінки організаційної стійкості. Хоча сценарії не реалістичні, вони сформульовані на основі широко розрекламованих методів атаки та операційних вразливостей, які спостерігаються в реальних інфраструктурних середовищах. Всі рахунки підкреслюють атрибути інциденту, технічні вразливості, відповідні виміри стійкості та нормальні рівні зрілості. І в Таблиці 3.5 резюме всіх сценаріїв.

Таблиця 3.5 — Резюме програми на основі сценаріїв.

Сценарій	Сектор	Головний інцидент	Технічні примітки	Ключові компоненти	Рівень стійкості
Зрив електричної мережі	Енергія (електромережа)	Цільова кібератака SCADA	Modbus TCP/IP, без шифрування, плоска мережа, ручне відновлення	Ситуаційна обізнаність, управління ризиками, активний захист	Дуже низький (Рівень 1)
Розумна лікарня-вимагач	Охорона здоров'я	Вимагацьке програмне забезпечення та медичне порушення Інтернету речей	Слабка сегментація, відсутність ІЧ-координації, застарілі резервні копії	Готовність, Стійкість, Відновлення Інцидентів	Розвиток (Рівень 2-3)

Сценарій	Сектор	Головний інцидент	Технічні примітки	Ключові компоненти	Рівень стійкості
Саботаж системи аеропорту	Перевезення	Віджеж системи через компроміс OT	Застарілі ПЛК, SOC присутні, немає уніфікованих свердлів IT-OT	Готовність, захист, координація реагування	Сильний (Рівень 3–4)

Сценарій 1: Порушення національної електричної мережі - кібератака на державні системи SCADA електричної мережі ініціює широкомасштабні регіональні відключення електроенергії. Системи SCADA на базі Modbus TCP/IP не мають шифрування та автентифікації і, таким чином, сприйнятливі до командних ін'єкцій та викрадення сеансів. Погана конструкція сегментації мережі полегшує бічне переміщення між операційними зонами. Немає інвентаризації активів або рішень для управління інформацією про безпеку та подіями (SIEM), а відновлення відбувається вручну протягом 24 годин. Це підпадає під умови технічних вразливостей, використаних під час попередніх атак, таких як атака на мережу України 2015 року.

Ключові компоненти, що впливають: ситуаційна обізнаність, управління ризиками, активний захист;

Індикативний рівень стійкості: дуже низький (рівень 1).

Сценарій 2: Вимагацьке програмне забезпечення в розумній лікарняній системі - Зараження столичної лікарняної мережі програмами-вимагачами шифрує електронні медичні записи та калічить медичне обладнання з підтегомом IoT. Сегментація в лікарні мінімальна, зі спільним доступом між адміністративними робочими станціями та клінічними системами. Немає активного та функціонального механізму реагування на інциденти, де викликається захист кінцевих точок. 12-година відновлення спричиняє тимчасове порушення процесів

відділення інтенсивної терапії. Це тип викриття, який використовується в реальних атаках, таких як атаки WannaCry на мережі охорони здоров'я.

Ключові компоненти, що постраждали: готовність, стійкість інфраструктури, відновлення інцидентів;

Індикативний рівень стійкості: розвивається (рівень 2-3).

Сценарій 3: Інцидент кіберсаботажу в аеропорту - відбувається кібератака на процеси координації польотів та обробки багажу в міжнародному аеропорту. Сертифікований ISO/IEC 27001 аеропорт централізовано контролюється SOC (Центр операцій безпеки) без живих кібернавчань або вправ червоної команди між відділами. Багажна система працює зі застарілими ПЛК з фірмовою, не виправленою прошивкою і знаходиться під компрометацією ланцюга поставок або інсайдерською експлуатацією. Його можна відновити протягом 5 годин, але аналіз після інциденту визначає, що немає консолідації протоколів між IT та OT командами.

Ключові компоненти, що постраждали: готовність інфраструктури, активний захист, інтеграція реагування;

Індикативний рівень стійкості: сильний (рівень 3-4).

Хоча ці віньєтки мають концептуальний характер, вони є репрезентативними для потенційних реальних ситуацій і ілюструють ключові технічні недоліки, загальні для критичної інфраструктури. Емпіричне підтвердження за допомогою криміналістичного аналізу, червоного об'єднання та офіційного інтерв'ю з експертами з предметної області має бути включено до подальших досліджень для перевірки надійності та ефективності структури, що використовується.

3.5.4. Технологічна інтеграція та практичне значення

Запропонована структура зосереджена на стратегічному використанні нових технологій, таких як штучний інтелект (ШІ), машинне навчання (ML) та

автоматизовані інструменти виявлення загроз. Це основні технології, які полегшують прогнозний моніторинг, виявлення аномалій та реагування на інциденти в режимі реального часу. Наприклад, аналітика на основі штучного інтелекту може бути використана для аналізу даних журналу та виявлення потенційних загроз на основі поведінкових моделей. Структура підрахунку балів цієї моделі дозволяє це зробити, надаючи пріоритет рейтингам вище середнього для організацій, які використовують моніторинг у режимі реального часу та автоматизовані парадигми пом'якшення наслідків, що дозволяє бути гнучким щодо динамічних загроз. Використання таких технологій, як AI-CRM та системно-теоретичних методів, таких як STPA-Sec, вбудовано в дизайн фреймворку, який відповідає моделям, які мають проактивне моделювання загроз та адаптивні здібності до навчання.

Окрім технічної цінності, структура InfraGuard має прагматичне та стратегічне використання для лідерів критичної інфраструктури в державному та приватному секторах. Завдяки розбивці стійкості на кількісні елементи та відображеннюючи конкретні рівні зрілості, лідери можуть виявляти прогалини, витрачати належним чином та порівнювати ефективність з галузевими стандартами, такими як NIST CSF, ISO/IEC 27001 та COBIT. Цей структурний підхід пропонує канали для спілкування технічних відділів та керівництва, за допомогою яких політика кібербезпеки узгоджується з організаційними цілями, а також потребами відповідності. У цьому модель є не лише інструментом оцінки, а й показником розробки політики, бюджетування та нарощування потенціалу кіберстійкості. Для реального застосування виявлення загроз у системі InfraGuard можуть застосовуватися різні моделі AI/ML залежно від ситуації в інфраструктурі. Виявлення аномалій з журналів, наприклад, може використовувати ізоляційні ліси або автокодери, тоді як прогнозування трафіку часових рядів в аналізі мережі може працювати з повторюваними нейронними мережами на основі LSTM. Навчальні дані можуть включати журнали системних подій, журнали сповіщень IDS/IPS та

захоплення мережевих пакетів, які нормалізуються та очищаються від шуму за допомогою попередньої обробки. Інтеграція з існуючою інфраструктурою може бути досягнута за допомогою модульних механізмів виявлення на краю мережі або на платформах SIEM. Показники ефективності бенчмарку, такі як точність, відкликання та рівень помилкових позитивів, мають вирішальне значення для забезпечення операційної ефективності, а контрзаходи, такі як петлі зворотного зв'язку, адаптивний поріг та логіка прийняття рішень ансамблю, можуть бути використані для запобігання помилковим тривогам та обчислювальному перевантаження.

3.6. Висновкок по третього розділу

У цьому розділі я запропонував систематичний підхід до оцінки кіберстійкості критичної інфраструктури шляхом інтеграції рівнів зрілості можливостей та факторів безпеки, орієнтованих на домен. Розробляючи систему кібербезпеки InfraGuard, я пропоную реалістичну модель, яка не тільки окреслює зростання зрілості процесу безпеки, але й сегментує заходи стійкості на три стратегічні напрямки: Щит, Космос та Меч. Ці виміри складаються з рівнів, які вміщують діяльність з кібербезпеки по всьому спектру, починаючи від моніторингу та профілактики до готовності та відновлення. Модель пропонує концептуальні визначення, а також оперативні вказівки для організацій, які прагнуть підвищити свою позицію стійкості в більш складних умовах загроз.

Інтегруючи багаторівневу зрілість процесу безпеки та функціональні області, що відображають різні рівні кіберзахисту, можна розробити модель позитивної стійкості. Розроблена тут система кібербезпеки InfraGuard дозволяє організаціям набрати шість рівнів зрілості з точки зору їх стійкості, від неповних до дуже складних процесів, враховуючи різні функції, такі як ситуаційна обізнаність, активний захист, готовність інфраструктури та відновлення інцидентів. Упорядковуючи ці параметри в тверду матрицю, модель підтримує проактивне

виявлення загроз, миттєве реагування та цілеспрямований метод для впорядкованого зміцнення кіберстійкості.

Прогнози та рішення щодо превентивних заходів передбачають аналіз історичних тенденцій загроз, зрілості сучасного процесу та соціально-технічної готовності, які включені в багатошаровий дизайн структури. Включення таких тем, як "Кібер як щит" та "Кібер як простір", приділяє особливу увагу первинному виявленню, управлінню ризиками та обізнаності про інфраструктуру, які є драйверами потенційних вразливостей. Вони можуть бути використані організаціями для надання високого пріоритету модернізації, розробки планів резервного копіювання, що залежать від сценарію, та впровадження таких технологій, як моніторинг на основі штучного інтелекту, щоб уникнути збоїв до того, як відбудеться значний збій.

В цьому розділі передбачено рівні стійкості та цілі ефективності, отримані з офіційної оцінки ключових показників за географією. Кожен процес сегментований на рівні (від 0 до 5) і корелює з відчутними, очевидними ознаками: періодом відновлення, впровадженням технологій та оперативною однорідністю. Компанії можуть виміряти себе у своєму нинішньому статусі за прикладами та найкращими практиками, такими як NIST CSF або AI-CRM. Навіть без великої кількості даних, імітовані умови та якісний аналіз можуть бути використані в рамках моделі, щоб забезпечити порівняльні оцінки, які визначають прогалини в можливостях і можуть бути повернуті для покращення бажаних областей.

Я надаю графічний та структурований метод, який допомагає особам, які приймають рішення, досягти організаційної кіберстійкості як у стратегії, так і в операціях. Синхронізуючи можливості безпеки на різних рівнях зрілості та доменах, менеджери можуть більш ефективно використовувати ресурси, робити політику та планувати навчання співробітників. Крім того, здатність системи відображати різні частини інфраструктури та дотримання глобальних стандартів гарантує, що вона є ефективним керівництвом для глобальної співпраці,

заохочуючи колективні зусилля щодо покращення кіберзахисту та мінімізації більш широких соціальних та економічних наслідків кібератак.

ЗАГАЛЬНИЙ ВИСНОВОК

У дипломній роботі розглянуто актуальну науково-прикладну проблему забезпечення кіберстійкості об’єктів критичної інфраструктури в умовах зростання інтенсивності та складності сучасних кіберзагроз. Проведений аналіз показав, що критична інфраструктура є ключовим елементом національної безпеки, економічної стабільності та соціальної життєздатності держави, а порушення її функціонування внаслідок кібератак може мати масштабні негативні наслідки.

У ході дослідження було проаналізовано сучасний стан і тенденції розвитку критичної інфраструктури, визначено основні типи загроз для її інформаційних та кіберфізичних компонентів, зокрема атаки типу ransomware, APT-кампанії, DDoS-атаки, уразливості операційних технологій та людського фактору. Показано, що традиційні підходи до кіберзахисту, орієнтовані переважно на запобігання атакам, є недостатніми, оскільки не враховують здатність системи адаптуватися, відновлюватися та зберігати критичні функції під час інцидентів.

Значну увагу в роботі приділено аналізу нормативно-правової бази у сфері кібербезпеки об’єктів критичної інфраструктури. Розглянуто законодавство України, підзаконні акти, державні стратегії та міжнародні стандарти (ISO/IEC 27001, ISO/IEC 27005, NIST CSF, вимоги Директиви NIS2 ЄС). Установлено, що чинні нормативні документи визначають загальні вимоги до кіберзахисту, однак не містять єдиної формалізованої методики кількісної оцінки кіберстійкості, що ускладнює процес прийняття управлінських рішень.

На основі аналізу наукових джерел і сучасних підходів до оцінювання стійкості запропоновано методику оцінки кіберстійкості об’єктів критичної інфраструктури, яка базується на ризик-орієнтованому підході та інтегрує технічні, організаційні й управлінські аспекти кіберзахисту. Методика передбачає формування системи критеріїв і показників, що відображають здатність об’єкта

запобігати кібератакам, виявляти інциденти, реагувати на них та відновлювати функціонування з мінімальними втратами.

У рамках роботи розроблено інформаційно-аналітичний механізм для реалізації запропонованої методики, який дозволяє автоматизувати процес збору та обробки даних, розрахунок показників кіберстійкості та формування рекомендацій щодо підвищення рівня захищеності. Практичне застосування запропонованого підходу продемонструвало його придатність для використання в різних секторах критичної інфраструктури та можливість адаптації до специфіки конкретних об’єктів.

Отримані результати підтверджують доцільність переходу від виключно захисних моделей кібербезпеки до концепції кіберстійкості, яка забезпечує комплексний підхід до управління ризиками та безперервністю функціонування критичних систем. Практична цінність роботи полягає в можливості використання розробленої методики під час проведення аудитів кібербезпеки, оцінювання ризиків, планування заходів із підвищення стійкості та підтримки прийняття управлінських рішень у сфері захисту об’єктів критичної інфраструктури.

Перспективи подальших досліджень пов’язані з удосконаленням моделей оцінки кіберстійкості з урахуванням застосування штучного інтелекту, аналізу великих даних, автоматизованого моніторингу загроз у реальному часі, а також розширенням методики для міжсекторальних і транскордонних об’єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] // Закон України. – 2017. – Режим доступу до ресурсу:.
2. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації [Електронний ресурс] // Указ Президента України від 13.02.2017 року № 32/2017. – 2016. – Режим доступу до ресурсу:
3. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] // Постанова КМ України від 19.06.2019 р. № 518. – 2019. – Режим доступу до ресурсу:.
4. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави [Електронний ресурс] // Постанова КМ України від 23.08.2016 р. № 563. – 2016. – Режим доступу до ресурсу:.
5. Стратегія національної безпеки України [Електронний ресурс] // Указ Президента України від 26.05.2015 року № 287/2015. – 2015. – Режим доступу до ресурсу:.
6. Доктрина інформаційної безпеки України [Електронний ресурс] // Указ Президента України від 25.02.2017 року № 47/2017. – 2017. – Режим доступу до ресурсу:.
7. Гончар С.Ф. Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. - №1(25). С. 158-163.
8. Гончар С.Ф. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Вісник Національного університету «Львівська політехніка» «Комп’ютерні системи та мережі». – 2014. - №806. – С. 34-39.

9. Гончар С.Ф. Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури / Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №80. – С. 27-32.
10. Гончар С.Ф. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №81. – С. 12-19.
11. Гончар С.Ф. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об’єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф., Ониськова А.В. // Моделювання та інформаційні технології. – 2017. - №82. – С. 40-48.
12. Гончар С.Ф. Концепція створення автоматизованої системи управління кібербезпекою об’єктів критичної інфраструктури / Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №83. – С. 70-76.
13. Гончар С.Ф. Актуальність досліджень і розробки систем захисту інформації для географічно розподілених автоматизованих систем управління технологічними процесами: матеріали міжнародної науково-практичної конференції «Кібербезпека-2013», Ялта, 2013. С. 33–37.
14. Гончар С.Ф. Особливості забезпечення кібербезпеки промислових систем управління: тези доповідей міжнародної науково-практичної конференції «Проблеми та перспективи розвитку енергетики, електротехнічних технологій та автоматизації в сільському господарстві» Київ, – 2013. – С. 36-37.
15. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв’язання», Київ, 2014. – С. 92-95.
16. Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Соціокультурний аспект забезпечення інформаційної безпеки об’єктів критичної інфраструктури : тези доповідей ХХ Всеукраїнської науково-практичної конференції «Проблеми

створення, розвитку та застосування високотехнологічних систем спеціального призначення», Житомир, 2014. – С. 195-196.

17. Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Забезпечення інформаційної безпеки об’єктів критичної інфраструктури України : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2015. – С. 95-96.
18. Гончар С.Ф., Леоненко Г.П., Левченко С.М. Критерії віднесення об’єктів до критичної інфраструктури з урахуванням світового досвіду : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2016. – С. 40-41.
19. Гончар С.Ф., Леоненко Г.П., Ткаченко В.В. Пріоритетні напрями розвитку нормативно-правового забезпечення інформаційної безпеки критичної інфраструктури України. : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2016. – С. 41-42.
20. Гончар С.Ф., Комаров М.Ю., Леоненко Г.П. Система управління інформаційною безпекою. Аналіз нормативної бази : Матеріали XX Ювілейної Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», 2018р., Київ, 2018. – С. 250-251.
21. Dipak Kumar Jana. Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security / Dipak Kumar Jana, Ramkrishna Ghosh. // Journal of Information Security and Applications. – 2018. – №40. – С. 173–182.
22. Erica D. Borghard. Can States Calculate the Risks of Using Cyber Proxies?
23. / Erica D. Borghard, Shawn W. Lonergan. // Orbis. – 2016. – №60. – С. 395–416.
24. Jangirala Srinivas. Government regulations in cyber security: Framework, standards and recommendations / Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar. // Future Generation Computer Systems. – 2019. – №29. – С. 178–188.

25. Joe Kim. Cyber-security in government: reducing the risk / Joe Kim. // Computer Fraud & Security. – 2017. – №7. – С. 8–11.
26. Лукічева Л.І. Управлінські рішення: підручник для студентів вищих навчальних закладів
27. Л. И. Лукичева, Д. Н. Егорычев ; под ред. Ю. П. Анискина. - 5-е изд., стер. – М.: Омега-Л, 2010. –384 с.
28. Мадера А.Г. Моделювання та прийняття рішень в менеджменті: посібник для майбутніх топ-менеджерів / А. Г. Мадера. –М.: ЛКИ, 2010. –688 с.
29. Менеджмент: підручник для студентів вищих навчальних закладів / А. Н. Алексеев, Е. С. Бурикин, О. И. Горелов и др.; под общ. ред. И. Н. Шапкина. – М.: Юрайт: ИД Юрайт, 2011. –690 с.
30. Орлов А.І. Прийняття рішень. Теорія і методи розробки управлінських рішень: навчальний посібник для студентів вищих навчальних закладів / А. І. Орлов. –М.; Ростов н/Д: МарТ, 2005. –496 с. Прийняття рішень [Електронний ресурс] / Розроб. корпорації
31. Пужаев А.В. Управлінські рішення: навчальний посібник для студентів. / А. В. Пужаев. –М.: КНОРУС, 2010. –192 с.
32. Райн Б. Стратегічний облік для керівника / Б. Райн; Пер. с англ. под ред. В. А. Микрюкова. –М.: Аудит: ЮНИТИ, 1998. – 616с.
33. Рапопорт Б.М. Оптимізація управлінських рішень / Б. М. Рапопорт. –М.: ТЕИС, 2001. –264с.
34. Ременников В.Б. Розробка управлінського рішення: навчальний посібник для вищих навчальних закладів / В. Б. Ременников. –М.: ЮНИТИ-ДАНА, 2000. –140с.
35. Ременников В.Б Управлінські рішення: навчальний посібник для вищих навчальних закладів/ В. Б. Ременников. - 2-е изд., перераб. и доп. –М.: ЮНИТИ-ДАНА, 2005. –144 с.
36. Розанова В.А. Психологія управління: навчальний посібник / В. А. Розанова. - 2-е изд., перераб. и доп. –М.: Бизнес-школа Интел-Синтез, 2000. – 384с.

37. Сміт Джейн. 30 хвилин для вибору правильного рішення / пер. с англ. П. Быстров. –М.: ЛОРИ, 2001. –80с.
38. A review of cyber security risk assessment methods for SCADA systems / Yulia Cherdantseva, Pete Burnap, Andrew Blyth та ін.]. // Computers & Security. – 2016. – №56. – С. 1–27.
39. Cyber security of critical infrastructures / Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke та ін.]. // ICT Express. – 2018. – №4. – С. 42–45.
40. Cheol-Kwon Lee. Introduction of a Cyber Security Risk Analysis and Assessment System for Digital I&C Systems in Nuclear Power Plants / Cheol-Kwon Lee. // IFAC Proceedings Volumes. – 2013. – №46. – С. 2140–2144.
41. Development of a cyber security risk model using Bayesian networks / Jinsoo Shin, Hanseong Son, Rahman Khalil, Gyunyoung Heo. // Reliability Engineering & System Safety. – 2015. – №134. – С. 208–217.
42. Jong Woo Park. Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants / Jong Woo Park, Seung Jun Lee. // Nuclear Engineering and Technology. – 2019. – №51. – С. 138–145.
43. Joon-Eon Yang. Multi-unit risk assessment of nuclear power plants: Current status and issues / Joon-Eon Yang. // Nuclear Engineering and Technology. – 2018. – №50. – С. 1199–1209.
44. Dynamic risk management response system to handle cyber threats / G. Gonzalez-Granadillo, S. Dubus, A. Motzek та ін.]. // Future Generation Computer Systems. – 2018. – №83. – С. 535–552.
45. Meir Kalech. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques / Meir Kalech. // Computers & Security. – 2019. –
46. №84. – С. 225–238.
47. The industrial control system cyber defence triage process / Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras. // Computers & Security. – 2017. – №70. – С. 467–481.

48. Cyber-attack path discovery in a dynamic supply chain maritime risk management system / Nikolaos Polatidis, Michalis Pavlidis, HaralambosMouratidis.
49. // Computer Standards & Interfaces. – 2018. – №56. – С. 74–82.
50. Keyun Ruan. The Point of Diminishing Return on Cyber Risk Investment
51. / Keyun Ruan. // Digital Asset Valuation and Cyber Risk Management. – 2019. – С. 99–115.
52. Травін В.В. Підготовка та реалізація управлінських рішень: навчально-практичний посібник / В. В. Травін, М. І. Магура, М. Б. Курбатова. – М.: Дело, 2004. –80 с.
53. Тронин Ю.Н. Управлінські рішення: навчальний посібник для вищих навчальних закладів / Ю. Н. Тронин, Ю. С. Масленченков. –М.: ЮНИТИ-ДАНА, 2004. –310 с.
54. Уваров В. В. Стратегічний менеджмент і глобалізація світової економіки: Навчальний посібник / В.В.Уваров, І.М.П'ятибратов. –М.: Вид-во Міжнародного ун-ту бізнесу та упр.: МЗ-Пресс, 2001. –281с.
55. Управління та контроль реалізації соціально-економічних цільових програм: [монографія] /

под ред. В. В. Кульбы, С. С. Ковалевского; Ин-т проблем управления им. В. А. Трапезникова РАН. –М.: ЛИБРОКОМ, 2009. –400 с.

56. Урубков А.Р. Курс MBA з оптимізації управлінських рішень: практичний посібник з використання моделей лінійного програмування / А. Р. Урубков. – М.: Альпіна Бізнес Букс, 2006. –176 с.
57. Учитель Ю.Г. Розробка управлінських рішень: підручник для студентів вищих навчальних закладів / Ю. Г. Учитель, А. І. Терновий, К. І. Терновий. - 2-е вид., перероб. і доп. –М.: ЮНІТІ-ДАНА, 2007. –383 с.
58. Хайниш С.В. Нестандартні ситуації: практикум для господарських керівників / С.В. Хайниш. –М.: Экономика, 1992. –206с.

59. Цветков А.Н. Методи вирішення творчих завдань: навчально-практичний посібник / А. Н. Цветков, В. Е. Зарембо. –М.: КНОРУС, 2009. –152 с.
60. Цигичко В.Н. Керівнику - про прийняття рішень / В.Н.Цигичко. - 2-е вид., випр. і доп. –М.: ІНФРА-М, 1996. –272с.
61. Кабінет міністрів України. (2016, Серп. 23). Постанова № 563, Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. [Електронний ресурс]. Доступно: Дата звернення: Серп. 02, 2016.
62. В.В. Домарев, Безпека інформаційних технологій. Методологія створення систем захисту. Київ, Україна: ТОВ «ТІД «ДС», 2002.
63. С.Ф. Гончар, Г.П. Леоненко, та О.Ю. Юдін, "Анализ угроз и уязвимостей индустриальных автоматизированных систем управления", Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, № 2 (26), с. 9-14, 2013.International Electrotechnical Commission. 2009. IEC 62443-1-1, Industrial communication network – Network and system security. Part 1-1: Terminology,concepts and models. [Online]. Available: https://webstore.iec.ch/publication/7029. Accessed on: Aug. 02, 2016.
64. Мохор В.В. Настанови з кібербезпеки (ISO/IEC 27032:2012) / В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.
65. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». – К.: НАДУ, 2014. – С. 92-95.
66. Лефевр В.А. Алгебра совісти / Лефевр В.А.; [пер. с англ. В. Лефевр и Е. Юдиной]. - М.: Когито-Центр, 2003. – 426 с.
67. Ловцов Д.А., Сергєєв Н.А. Управління безпекою ергасистем / За ред. Д.А. Ловцова, - 2-е вид. випр. і доп. – М.: РАУ-Університет, 2001. – 224 с.

68. Силов В.Б. Прийняття стратегічних рішень в нечіткій обстановці. – М.: ІНПРО – РЕС, 1995. – 228с.Ємелін В.І.
69. Методи та моделі оцінки та забезпечення інформаційної безпеки автоматизованих систем управління критичними системами: дис. … доктора техн. наук : 05.13.19 / Ємелін Вадим Іванович. – СПб., 2012. – 238 с.
70. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.
71. Теорія ймовірностей і математична статистика. Базовий курс з прикладами і завданнями / [Кібзун А. І., Горяінова Е. Р., Наумов А. В., Сиротін А. Н.]. – М.: ФІЗМАТЛІТ, 2002. – 224 с.Гончар С.Ф.
72. Особливості забезпечення кібербезпеки індустріальних систем управління : тези доповідей міжнародної науково- практичної конференції «Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК», Київ, – 2013. – С. 36-37.
73. Мохор В.В. Настанови з кібербезпеки (ISO/IEC 27032:2012) /
74. В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.
75. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.
76. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.
77. Information technology – Security techniques – Information security risk management: BS ISO/IEC 27005:2008.
78. Industrial communication networks – Network and system security: IEC 62443.– Part 3.
79. Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін

О.Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. Випуск 1 (25).

80. Особливості забезпечення кібербезпеки індустріальних систем управління / Гончар С.Ф. // Тези доповідей міжнародної науково-практичної конференції “Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК”, Київ, – 2013. – С. 36-37.
81. Мохор В.В. Настанови з кібербезпеки (ISO/IEC 27032:2012) / В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.
82. Грицай Г., Тиморін А., Гольцев Ю., Ільїн Р. Безпека промислових систем у цифрах. – М.: Positive Technologies, 2012.
83. Теоретико-методологічний аспект забезпечення інформаційної безпеки об’єктів критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Вісник Національного університету “Львівська політехніка”: “Комп’ютерні системи та мережі”. №806. – 2014. – 34 с.
84. Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models.
85. Сантіапіллай, Ф.П. ; Ратнаяке, Р.М.С. Метод визначення пріоритетів на основі ризиків для планування та розподілу ресурсів у державному секторі. ТКМ Дж. 2022, 34, 829–844.
86. Бідголі, М. ; Гроссклагс, Дж. Звітність кінцевого користувача про кіберзлочинність: що ми знаємо і що ми можемо зробити, щоб покращити її. У матеріалах Міжнародної конференції IEEE 2016 року з кіберзлочинності та комп'ютерної криміналістики (ICCCF), Ванкувер, Британська Колумбія, Канада, 2-14 червня 2016 року; Інститут інженерів з електротехніки та електроніки (IEEE): Піскатауей, Нью-Джерсі, США, 2016.
87. Данг, Л.Н. ; Кахсай, І.Т.; Джеймс, Л.Т.Н. ; Джонс, Л.Дж. ; Ріос, тобто ; Мезук, Б. Корисність дослідження та обмеження текстових даних у Національній системі звітності про насильницькі смерті: огляд та рекомендації. Ін'єка. Епідемія.2023, 10, 23.

88. Сукмана, М. ; Майнель, С. Порівняння інструментів електронного уряду та оцінки безпеки для індонезійської системи електронного уряду. У матеріалах 4-ї Міжнародної конференції з інформаційної та мережевої безпеки (ICINS 2016), Куала-Лумпур, Малайзія, 28–31 грудня 2016 року; Асоціація обчислювальної техніки: Нью-Йорк, штат Нью-Йорк, США, 2016; стор. 96–103.
89. Нгуєн, Т.; Ван, С. ; Альхазмі, М. ; Наземі, М. ; Естебсарі, А. ; Дегганян, П. Стійкість електромереж для кібер-супротивників: стан модерн. Доступ до IEEE 2020, 8, 87592–87608.
90. Ратасич, Д. ; Халід, Ф.; Гейслер, Ф.; Гросу, Р. ; Шафік, М. ; Барточчі, Е. Дорожня карта до стійкого Інтернету речей для кіберфізичних систем. Доступ до IEEE 2019, 7, 13260–13283.
91. Бхусал, Н. ; Абдельмалак, М. ; Камруззаман, М. ; Бенідріс, М. Стійкість енергетичної системи: поточні практики, виклики та майбутні напрямки. Доступ до IEEE 2020, 8, 18064–18086.
92. Каріас, Дж.Ф.; Борхес, М.Р.С. ; Лабака, Л. ; Аррізабалага, С. ; Ернантес, Дж. Систематичний підхід до впровадження кіберстійкості в МСП. Доступ до IEEE 2020, 8, 174200–174221.
93. Чжан, Дж. ; Лі, Л. ; Лін, Г.; Фанг, Д. ; Тай, Й. ; Хуан, Дж. Кіберстійкість у охороні здоров'я Цифровий близнюк на рак легенів.IEEE Доступ 2020, 8, 201900–201913.
94. Бьорк, Ф.; Хенкель, М. ; Стірна, Дж. ; Здравкович, Дж. Кіберстійкість — Основи визначення. У нових вкладах в інформаційні системи та технології; Досягнення в інтелектуальних системах та обчисленнях; Springer: Cham, Швейцарія, 2015; стор. 311–316.
95. Фогель, Е. ; Діка, З.; Кланн, Д. ; Лангендьорфер, П. Стійкість у кіберсвіті: визначення, особливості та моделі. Future Internet 2021, 13, 293.

96. Стоіцеску, М. ; Фабр, Дж.С. ; Рой, М. Архітектура стійких обчислювальних систем: компонентний підхід для адаптивної відмовостійкості. Дж. Система. Архіт. 2017, 73, 6–16.
97. Проман, М. ; Mailloux, L.O.; Mills, R.F.; Young, W. Аналіз вимог до безпеки концептуальних систем: тематичне дослідження повітряної заправки. Доступ IEEE 2018, 6, 46668–46682.
98. Хуан, П. ; Го, С. ; Чжоу, Л. ; Лорх, Дж.Р. ; Данг, Й. ; Чинталапаті, М. ; Яо, Р. Сіра невдача: ахіллесова п'ята хмарних систем. У матеріалах семінару з гарячих тем в операційних системах (HotOS), Вістлер, Британська Колумбія, Канада, 7-10 травня 2017 року; Комп'ютерне товариство IEEE: Вашингтон, округ Колумбія, США, 2017; стор. 150–155.
99. Ліго, К. ; Котт, А. ; Лінков, І. Як виміряти кіберстійкість системи за допомогою автономних агентів: підходи та виклики. IEEE Eng. Уп. Ред. 2021, 49, 89–97.
100. Патель; Рой, С. ; Балді, С. Стійкість контролю широкого демпфування до кібератак: підхід динамічного циклу. IEEE Trans. Розумна мережа 2021, 12, 3438–3447.
101. Сафітра, М.Ф.; Любіс, М. ; Фахрурроджа, Х. Контратака кіберзагроз: основа для майбутнього кібербезпеки.Стійкість 2023, 15, 13369.
102. Бук, С.Х. ; Ахмед, С.Х. ; Хуссейн, Р. ; Юн, Й. Названа внутрішня кіберстійкість мережі даних для транспортних CPS. Доступ IEEE 2018, 6, 60570–60585.
103. Драуїцеа, М. ; Леонард, М. ; Ціолофан, С.Н. ; Мілітару, Г. Управління даними, інформацією та технологіями в кіберфізичних системах: громадська безпека як послуга та її системи. Доступ до IEEE 2019, 7, 92672–92692.
104. Моура, Дж. ; Хатчісон, Д. Підвищення стійкості в крайових хмарних системах. Доступ до IEEE 2022, 10, 45190–45206.

105. Філліпс, Т.; Маріновічі, Л.Д. ; РІГер, С. ; Оррелл, А. Масштабований аналіз стійкості за допомогою спільного моделювання енергетичних систем. Доступ до IEEE 2023, 11, 18205–18214.

106. Лагарі, С.У.А. ; Манікам, С. ; Аль-Ані, А.К. ; Рехман, С.У. ; Каруппая, С. SECS/GEMsec: Механізм виявлення та запобігання кібератакам на комунікації SECS/GEM у ландшафті Індустрії 4.0. Доступ IEEE 2021, 9, 154380–154394.

107. Зіглер, В. ; Шнайдер, П. ; Вішванатан, Х. ; Монтаг, М. ; Канугові, С. ; Резакі, А. Безпека та довіра в епоху 6G.IEEE Access 2021, 9, 142314–142327.

108. Ель-Мараді, А. ; Рахума, К. Вивчення кібербезпеки в цивільній авіації, включаючи розробку та застосування оцінки ризиків кібербезпеки авіації. Доступ до IEEE 2021, 9, 143997–144016.

109. Xin, X.; Keoh, S.L. ; Севеньяні, М. ; Саербек, М. ; Ху, Т.П. Перевірка адаптивної моделі для модульних додатків Industry 4.0. Доступ до IEEE 2022, 10, 125353–125364

110. Він, Дж. ; Юань, З.; Ян, Х.; Хуан, В. ; Ту, Й. ; Лі, Й. Моделювання надійності та оцінка міських мультиенергетичних систем: огляд стану техніки та майбутніх викликів. Доступ до IEEE 2020, 8, 98887–98909.

111. Чжен, З.; Ян, С. ; Ян, В. Аналіз стійкості мережевої системи дискретного часу за наявності розкриття інформації. Доступ до IEEE 2019, 7, 180147–180154.

112. Саху, С. ; Dragicevic, T.; Blaabjerg, F. Багатошарова парадигма стійкості проти кібератак у мікромережах DC.IEEE Trans. Електрон. 2021, 36, 2522–2532.

113. Пітерс, В. ; Хаджиосманович, Д. ; Дешене, Ф. Кібербезпека як соціальний експеримент. У матеріалах семінару з нових парадигм безпеки (NSPW 2014), Вікторія, Британська Колумбія, Канада, 15–18 вересня 2014 року; Асоціація обчислювальної техніки: Нью-Йорк, штат Нью-Йорк, США, 2014; стор. 15–24.

114. Фу, С. ; Яо, З. Оцінка ризику конфіденційності онлайн-соціальних мереж. У матеріалах Міжнародної конференції з мереж та мережевих додатків 2022 року (NaNA), Урумчі, Китай, 3-5 грудня 2022 року; IEEE: Piscataway, NJ, USA, 2022; стор. 144–151.

115. Юксель, С. ; Юксель, М.Е. ; Заїм, А.Х. Підхід до захисту конфіденційності в соціальних мережах. У матеріалах 5-ї Міжнародної конференції з систем та мережевих комунікацій, Ніцца, Франція, 22–27 серпня 2010 року; IEEE: Piscataway, NJ, USA, 2010; pp. 154–159.

116. Барбо, М. ; Cuppens, F.; Cuppens, N. ; Дагнас, Р. ; Гарсія-Альфаро, Дж. Оцінка стійкості кіберфізичних систем за допомогою кількісних показників. Доступ до IEEE 2021, 9, 46462–46475.

117. Кураші, Дж.М. ; Джамбі, К.М. ; Eassa, F.E. ; Хемахем, М. ; Алсламі, Ф.; Басухайл, А.А. На ту боці техніки моделювання атаки, що стосується стійкості в самокерованих автомобілях. Доступ до IEEE 2023, 11, 2652–2673.

118. Пріслан, К. ; Міхеліч, А. ; Бернік, І. Оцінка ефективності інформаційної безпеки в реальному світі з використанням багатовимірного соціально-технічного підходу. PLoS ONE 2020, 15, e0238739.

119. Асгарі, Х. ; Хейнс, С. ; Рисави, О. Ідентифікація загроз та оцінка ризиків безпеки для рекурсивної архітектури Інтернету. Система IEEE. Дж. 2018, 12, 2437–2448.

120. Амані, М. ; Джалілі, М. Електромережі як складні мережі: аналіз стійкості та надійності. Доступ до IEEE 2021, 9, 119010–119031.

121. Акбарян, Ф.; Тарнеберг, В. ; Фіцджеральд, Е. ; Кіл, М. Атакуйте стійкі хмарні системи управління для Індустрії 4.0. Доступ до IEEE 2023, 11, 27865–27882.

122. Рігер; Шульц, К. ; Керролл, Т.; МакДжункін, Т. Стійкі системи управління - Основа, бенчмаркінг та переваги.Доступ до IEEE 2021, 9, 57565–57577.

123. Гузман, Р.Е.П. ; Рівера, М. ; Вілер, П.В. ; Мірзаєва, Г.; Еспіноза, Е.Е. ; Рохтен, Дж.А. Система спільного використання потужності Microgrid для програмно визначених мереж та аналізу кібербезпеки. Доступ до IEEE 2022, 10, 111389–111405.

124. Маріно, Л. ; Вікрамасінге, К.С. ; Сінгх, В.К. ; Ніжний, Дж. ; РІГер, С. ; Маніак, М. Віртуалізований кіберфізичний випробувальний стен для виявлення аномалій машинного навчання: тематичне дослідження вітрової мережі. Доступ IEEE 2021, 9, 159475–159494.

125. Муельхі, С. ; Лааручі, М.Е. ; Канціла, Д. ; Чаучі, Х. Прогнозний формальний аналіз стійкості в кіберфізичних системах. Доступ до IEEE 2019, 7, 33741–33758.

126. Соіккелі, Дж. ; Казале, Г.; Муньос-Гонсалес, Л. ; Лупу, Е.С. Планування надмірності для економічно ефективної стійкості до кібератак. IEEE Транс. Надійна Безпека. Комп'ютер. 2023, 20, 1154–1168.

127. Борхес, Ф.С. ; Лауріндо, Ф.Дж.Б. ; Спінола, М.М. ; Гонсалвес, Р.Ф.; Маттос, К.А. Стратегічне використання штучного інтелекту в цифрову епоху: систематичний огляд літератури та майбутні напрямки досліджень.Інт. Дж. Інф. Manag.2021, 57, 102225.

128. Оловононі, Ф.О.; Рават, Д.Б. ; Лю, С. Стійке машинне навчання для мережевих кіберфізичних систем: опитування щодо безпеки машинного навчання для забезпечення машинного навчання для CPS. IEEE Commun. Вижив. Репетитор. 2021, 23, 524–552.

129. Мердок, С. ; Лівер, Н. Анонімність проти довіри до співпраці з кібербезпекою. У матеріалах 2-го семінару ACM з обміну інформацією та спільної безпеки (WISCS 2015), Денвер, Колорадо, США, 12 жовтня 2015 року; стор. 27–29.

130. Нікянен, Р. ; Kärkkäinen, Т. Підтримка кіберстійкості за допомогою семантичної Wiki. У матеріалах 12-го Міжнародного симпозіуму з відкритої співпраці (OpenSym 2016), Берлін, Німеччина, 17-19 серпня 2016 року.

131. Ернандес-Бехарано, М. ; Родрігес, Р.Дж. ; Мерсегер, Дж. Бачення покращення безперервності бізнесу за допомогою механізмів та рамок кіберстійкості. У матеріалах 16-ї Іберійської конференції з інформаційних систем і технологій (CISTI), Чавес, Португалія, 23–26 червня 2021 року.

132. Каріас, Дж.Ф.; Лабака, Л. ; Саррієгі, Дж.М. ; Ернантес, Дж. Визначення інвестиційної стратегії кіберстійкості в контексті промислового Інтернету речей. Датчики 2019, 19, 138.

133. Сукіасян; Бадікян, Х. ; Педроса, Т.; Лейтао, П. Безпечний обмін даними в промисловому Інтернеті речей. Нейрокомп'ютер 2022, 484, 183–195.

134. Санчес-Гордон, М. ; Коломо-Паласіос, Р. Безпека як культура: систематичний огляд літератури DevSecOps. У матеріалах 42-ї міжнародної конференції IEEE/ACM з семінарів з програмної інженерії (ICSEW 2020), Сеул, Республіка Корея, 27 червня-19 липня 2020 року; стор. 266–269

135. Альфаваз, С. ; Нельсон, К. ; Моханнак, К. Культура Інформаційної Безпеки: Концептуальна Основа Відповідності Поведінці. У матеріалах 8-ї Австралійської конференції з інформаційної безпеки (AISC 2010), Перт, Австралія, 30 листопада 2010 року; стор. 47–55.

136. Швейцер, Дж. Поінформованість про безпеку. У матеріалах Північно-східного симпозіуму ACM з безпеки персональних комп'ютерів (PCS), Уолтем, Массачусетс, США, 1 вересня 1986 року; стор. 13–20.

137. Циммер, Г.Г. Комп'ютери та обчислення в алгебраїчній теорії чисел. У матеріалах 2-го симпозіуму ACM з символічних та алгебраїчних маніпуляцій (SYMSAC), Лос-Анджелес, Каліфорнія, США, 23-25 березня 1971 року; стор. 172–179.

138. Альхазмі, Х. ; Малайя, Й.К. ; Рей, І. Вимірювання, аналіз та прогнозування вразливостей безпеки в програмних системах.Comput. Захист. 2007, 26, 219–228

139. Котенко; Ізрайлов, К. ; Буіневич, М. ; Саєнко, І. ; Шорі, Р. Моделювання розробки програмного забезпечення для енергетичних мереж з урахуванням виявлення та усунення вразливостей. Енергії 2023, 16, 5111

140. Біерман, Дж. ; Берент, Д. ; Фалтер, З.; Бхунія, С. Огляд атаки Colonial Pipeline Ransomware. У матеріалах 23-го Міжнародного симпозіуму IEEE/ACM з кластерних, хмарних та інтернет-обчислень (CCGridW 2023), Бангалор, Індія, 1–4 травня 2023 року; Інститут інженерів з електротехніки та електроніки Inc.: Піскатавей, Нью-Джерсі, США, 2023; стор. 8–15

141. Тіагараджан, К. ; Діксіт, К.К. ; Паннірсельвам, М. ; Мадхуваппан, К.А. ; Гадде, С. ; Шрот, Дж.Н. Аналіз зростання штучного інтелекту для безпеки додатків в Інтернеті речей. У матеріалах 2-ї Міжнародної конференції зі штучного інтелекту та розумної енергії (ICAIS 2022), Коїмбаторе, Індія, 23–25 лютого 2022 року; Інститут інженерів з електротехніки та електроніки Inc.: Піскатавей, Нью-Джерсі, США, 2022; стор. 6–12.

142. Носухі, М.Р. ; Шах, С.В. ; Пан, Л. ; Золотавкін, Ю. ; Нанда, А. ; Гаураварам, П. ; Досс, Р. Аналіз слабких ключів для механізму інкапсуляції постквантових ключів BIKE. IEEE Транс. Інф. Сухова сухо-медисх. 2023, 18, 2160–2174.

143. Кессвані, Н. ; Кумар, С. Підтримка кібербезпеки: наслідки, вартість та віддача. У матеріалах конференції ACM SIGMIS 2015 року з комп'ютерів та досліджень людей (SIGMIS-CPR 2015), Ньюпорт-Біч, Каліфорнія, США, 4-6 червня 2015 року; Асоціація обчислювальної техніки, Inc.: Нью-Йорк, штат Нью-Йорк, США, 2015; стор. 161–164.

144. Ананг; Ганді, А. ; Сукахьо, Ю.Г. Дизайн управління ризиками інформаційної безпеки: тематичне дослідження інформаційної системи людських ресурсів в Університеті XYZ. У матеріалах 4-ї Міжнародної конференції з комп'ютерної та інформаційної інженерії: цифрові промислові інновації на основі IT для добробуту суспільства (IC2IE 2021), Депок,

Індонезія, 14–15 вересня 2021 року; Інститут інженерів з електротехніки та електроніки Inc.: Піскатавей, Нью-Джерсі, США, 2021; стор. 198–203.

145. Мірч, М. ; Сліпий, К. ; Кох, С. ; Дудек, Г. Управління інформаційною безпекою в компаніях, що не входять до ІКТ, та не вукових компаніях: перспектива профілактичних інновацій. Комп'ютер. Захист. 2021, 109, 102383.

146. Чжан, К. ; Лі, С. Дослідження інтеграції бізнес-аналітики та інновацій та підприємницької освіти для комп'ютерних наук. У матеріалах 5-ї Міжнародної конференції з великих даних та освіти (ICBDE 2022), Шанхай, Китай, 26-28 лютого 2022 року; Асоціація обчислювальної техніки: Нью-Йорк, штат Нью-Йорк, США, 2022; стор. 212–216.

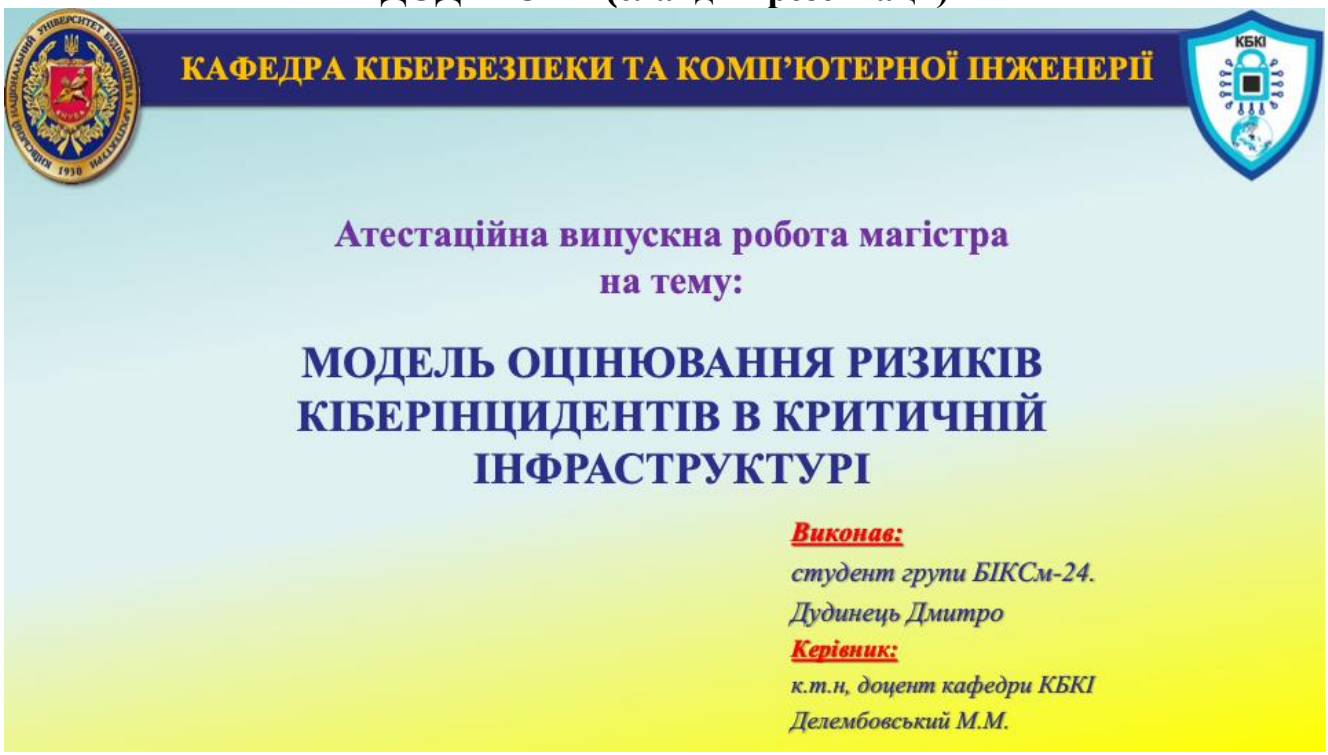
147. Тіньяне, М. ; Крістін, Д. Онтологія SMART Citizen Cyber Resilience (SC2R). У матеріалах 13-ї Міжнародної конференції з інформаційної безпеки та мереж (SIN 2020), Меркез, Туреччина, 4–7 листопада 2020 року; Асоціація обчислювальної техніки: Нью-Йорк, штат Нью-Йорк, США, 2020.

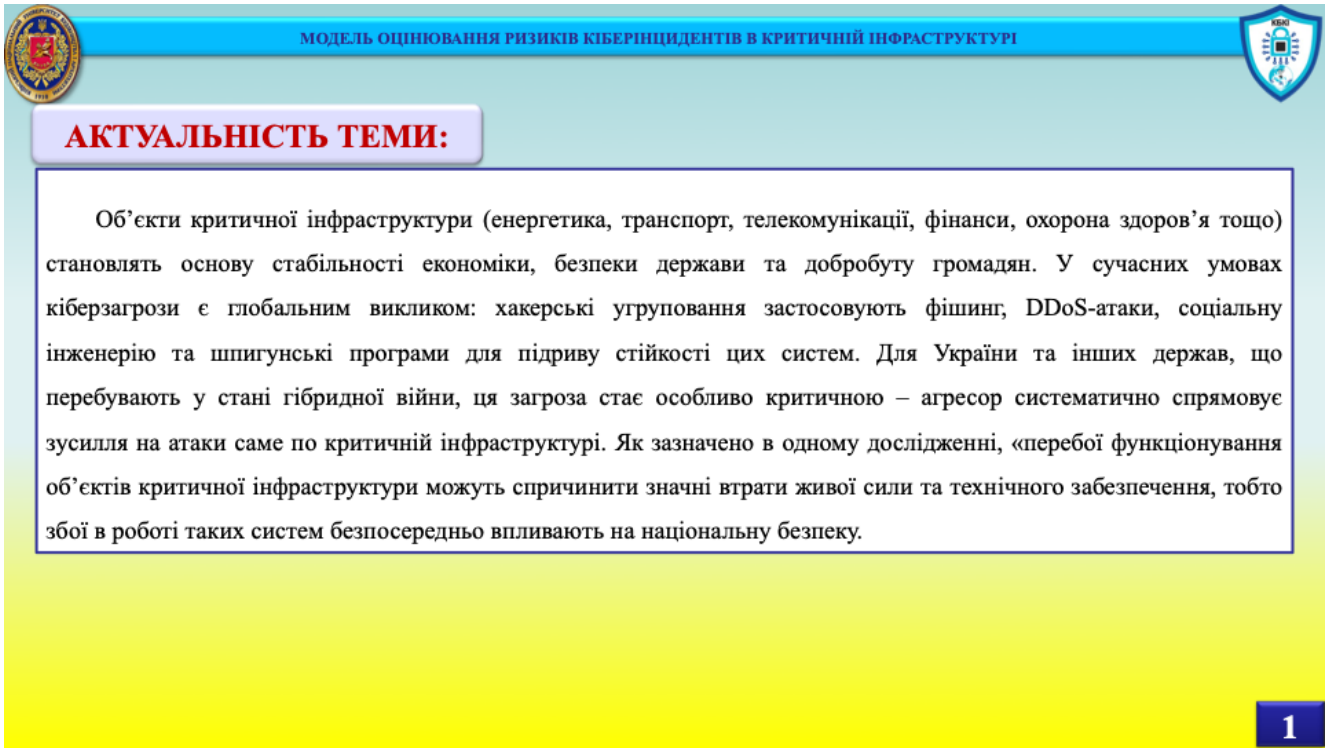
148. Джонсон, Ф. Демократія, процвітання, громадяни та держава. Може. Зовнішня політика Дж. 2002, 10, 23–40.

149. Лян, К. ; Лю, Дж.К. ; Лу, Р. ; Вонг, Д.С. Проблеми конфіденційності для обміну фотографіями в соціальних мережах. Інтернет-комп'ютер IEEE. 2015, 19, 58–63.

150. Абдуллаєва, Ф. Кіберстійкість та проблеми кібербезпеки інтелектуальних хмарних обчислювальних систем. Контроль результатів. Оптимізм. 2023, 12, 100268.

ДОДАТОК А(слайди презентації)





МЕТА:

Метою цієї роботи є розробка комплексної метрики кіберстійкості об'єктів критичної інфраструктури. Такий інструмент надасть змогу оцінювати, наскільки критична інфраструктура захищена від сучасних кіберзагроз та здатна швидко відновлювати роботу після атак.

ОБ'ЄКТ:

Об'єктом дослідження є критична інфраструктура – як складна система підприємств та мереж (включно з енергетичними, транспортними, телекомунікаційними, фінансовими тощо) – та процес забезпечення її стійкої роботи в умовах кібератак.

ПРЕДМЕТ:

Предметом дослідження виступають методи і показники оцінки кіберстійкості цих систем, зокрема чинники, що визначають здатність критичної інфраструктури витримувати атаки та швидко відновлювати роботу.

МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРІНЦИДЕНТІВ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

НАУКОВА НОВИЗНА:

Наукова новизна полягає в розробці комплексної метрики кіберстійкості КІ, яка вперше інтегрує кількісну оцінку ризиків (включаючи вразливості і ймовірності кібератак) з показниками готовності реагувати та відновлюватися після інцидентів. У рамках роботи запропоновано включити до метрики інноваційні компоненти: наприклад, оцінку ступеня використання передових технологій (штучного інтелекту, аналітики даних, систем раннього виявлення) при захисті КІ та показники співпраці з іншими суб'єктами (державними й приватними) у сфері безпеки. Також новизною є вперше запропоноване поєднання показників впливу кібератак (час відновлення, економічні збитки тощо) у єдиній метриці. Дана розробка дозволяє ліквідувати відомі недоліки існуючих методів (наприклад, упущення фактора часу чи взаємозв'язку оцінок ризиків) та забезпечує більш точну і релевантну оцінку кіберстійкості.

ПРОБЛЕМА ДОСЛІДЖЕННЯ :

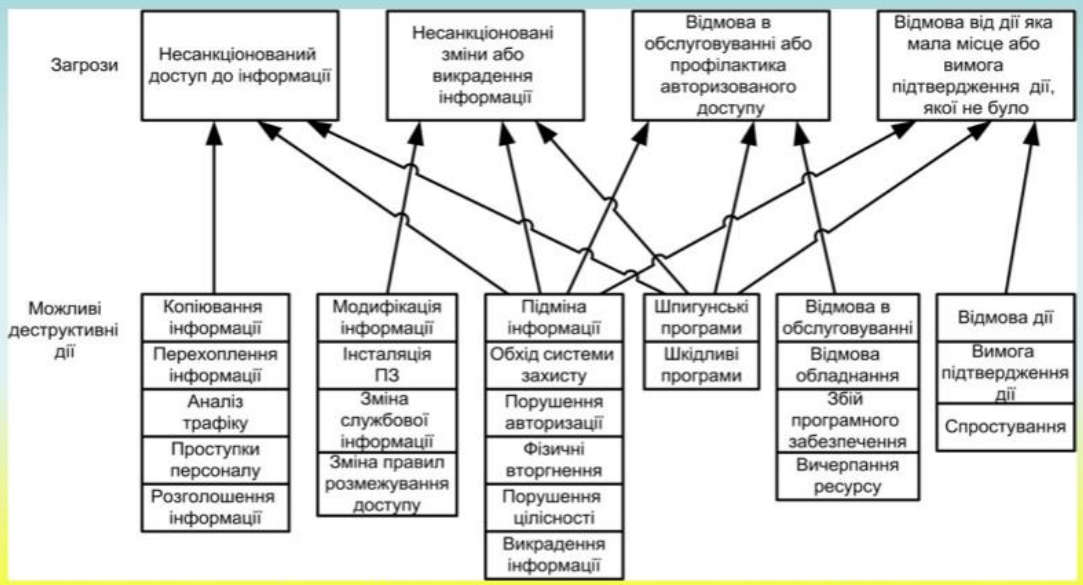
Існуючі підходи до оцінки кіберризиків не враховують усі аспекти складних сучасних загроз і можливостей відновлення. Зокрема, завдання сумарної оцінки ризику кібербезпеки об'єктів КІ досі не розв'язано повною мірою. Відомо, що оператори критичної інфраструктури часто не мають інструментів для комплексної оцінки та управління такими ризиками. Наприклад, навіть у транспортній галузі менеджери не мають засобів для жорсткої оцінки загального ризику (обмежені дані та моделі гальмують точне моделювання). Подібні висновки відображені і в роботах українських експертів: досвід кібератак (на кшталт «BlackEnergy» чи «NotPetya») виявив слабкі місця систем та показав необхідність вдосконалити механізми протидії і нормативну базу. Таким чином, існуючі рішення є недостатніми: це обґрунтовує необхідність створення нової, інтегрованої метрики кіберстійкості, яка покриватиме розширений спектр показників (оцінку вразливостей, потенціал реагування та відновлення, використання новітніх технологій і співробітництва) та вирішуватиме зазначені прогалини.

Структура кваліфікаційної роботи :

Вступ	Обґрунтовано актуальність теми, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено методи дослідження та практичну значущість роботи.
Перший розділ	Виконано аналіз предметної області, розкрито поняття та значення критичної інфраструктури, розглянуто нормативно-правове забезпечення кібербезпеки, проаналізовано наукові джерела та сформульовано проблему і постановку задачі дослідження.
Другий розділ	Досліджено сучасні кіберзагрози інформаційних систем об'єктів критичної інфраструктури, побудовано модель загроз, визначено ймовірність їх реалізації та виконано оцінювання небезпеки кібератак.
Третій роділ	Розроблено метрику кіберстійкості критичної інфраструктури, визначено її ключові компоненти, проведено оцінку рівнів стійкості та проаналізовано результати застосування запропонованого підходу.
Висновок	Узагальнено результати дослідження, сформульовано основні наукові та практичні висновки, визначено напрями подальших досліджень.

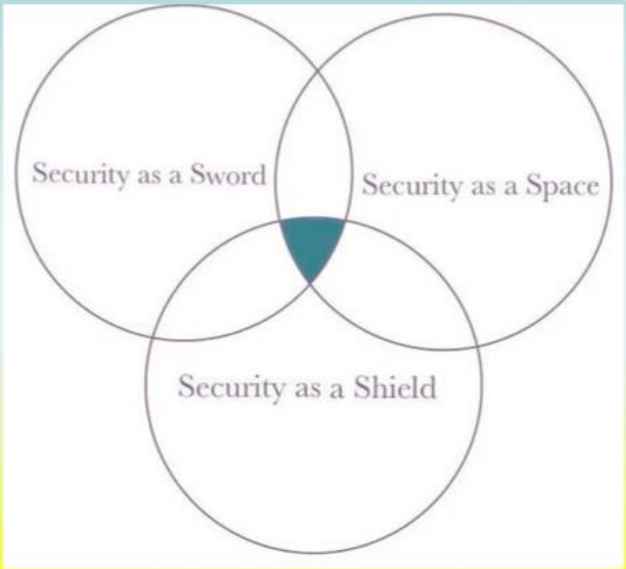
Методи дослідження:

Методи системного аналізу	Для дослідження структури та взаємозв'язків компонентів інформаційних систем об'єктів критичної інфраструктури.
Методи аналізу та оцінювання ризиків	Для визначення ймовірності реалізації кіберзагроз та оцінки їх потенційних наслідків.
Методи моделювання загроз і вразливостей	Для формування моделі кіберзагроз інформаційних систем ОКІ.
Ризик-орієнтований та процесний підходи	Для побудови метрики кіберстійкості та визначення рівнів зрілості безпекових процесів.
Методи порівняльного аналізу	Для зіставлення існуючих моделей і підходів до оцінки кіберстійкості.
Методи узагальнення та експертної оцінки	Для формування критеріїв, показників і шкал оцінювання кіберстійкості.



Взаємозв'язок між загрозами і деструктивними діями

Структурна модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури.



Класифікація підходів до кібербезпеки

Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

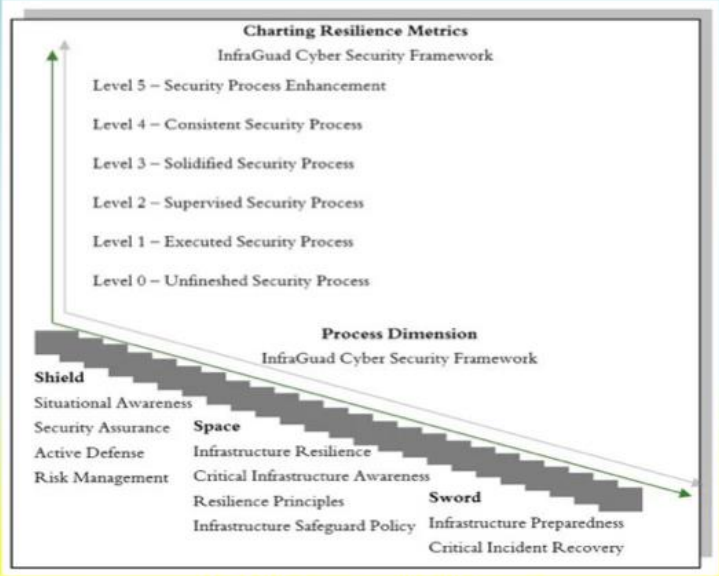
Домен	Компонент	Індикатор	Опис
Кіберпростір як щит	Ситуаційна обізнаність	Можливості виявлення та моніторингу загроз	Організація може проактивно спостерігати за оперативними змінами та виявляти потенційні кіберзагрози.
	Гарантія безпеки	Оцінки ризиків та контроль безпеки	Включає рутинні оцінки та дотримання суворих стандартів для забезпечення захисту системи.
	Активний захист	Швидке реагування на загрози	Передбачає використання інструментів та стратегій для виявлення та запобігання атакам до того, як відбудеться пошкодження системи.
	Управління ризиками	Ідентифікація та пом'якшення ризиків	Систематичний процес оцінки загроз та визначення пріоритетів заходів щодо пом'якшення наслідків.

Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

Домен	Компонент	Індикатор	Опис
Кіберпростір як космос	Стійкість інфраструктури	Надійність системи та можливості відновлення	Інфраструктура може підтримувати роботу та відновлюватися під час або після кіберінцидентів.
	Поінформованість про критичну інфраструктуру	Організаційна обізнаність про життєво важливі системи	Глибоке розуміння національного значення інфраструктури та пов'язаних з нею ризиків.
	Принципи стійкості	Стійкий дизайн та операційна філософія	Основоположні принципи побудови систем, які можуть витримувати збої.
	Політика захисту інфраструктури	Захисна політика та процедури	Офіційні документи та процедури захисту фізичної та цифрової інфраструктури від загроз.

Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

Домен	Компонент	Індикатор	Опис
Кіберпростір як меч	Готовність інфраструктури	Попереджувальна готовність та навчання	Наявність планів реагування на інциденти, навчання персоналу та моделювання сценаріїв.
	Відновлення критичних інцидентів	Швидкість відновлення та заходи безперервності	Можливість швидко та ефективно відновлювати функції системи після збоїв.



Графік показників стійкості

Рівні компетентності процесу в системі кіберстійкості InfraGuard:

Рівень 5:

Покращення процесу безпеки: Це найвищий рівень у структурі, де процеси безпеки були повністю оптимізовані. На цьому етапі процеси безпеки не тільки проходять гладко, але й постійно вдосконалюються та вдосконалюються на основі зворотного зв'язку та навчання на попередньому досвіді. Організації на цьому рівні досягли найвищого рівня зрілості в процесах безпеки, і кожен аспект оптимізований для повної ефективності. Організації на цьому рівні є лідерами в практиці кібербезпеки.

Рівень 4:

Послідовний процес безпеки: на цьому рівні процеси безпеки працюють послідовно та передбачувано. Процеси дають послідовні результати та відповідають встановленим стандартам якості. Послідовність тут є ключовою, а це означає, що організації можуть покладатися на процеси безпеки для досягнення передбачуваних результатів без особливих варіацій або невизначеності. Організації на цьому рівні досягли дуже високого рівня стійкості у підтримці кібербезпеки.

Рівні компетентності процесу в системі кіберстійкості InfraGuard:

Рівень 3:

Закріплений процес безпеки: на цьому рівні процеси безпеки стали надійними та усталеними. Процеси виявилися ефективними на практиці і стали невід'ємною частиною повсякденних операцій. Це вказує на те, що організації успішно побудували міцну основу для своєї безпеки, і ці процеси вважаються зрілими практиками в їх діяльності. Організації на цьому рівні досягли високого рівня стійкості в підтримці своєї критичної інфраструктури.

Рівень 2:

Контрольований процес безпеки: На цьому рівні процеси безпеки ретельно контролюються, щоб гарантувати, що всі дії відбуваються відповідно до запланованих та встановлених стандартів. Нагляд тут є вирішальним компонентом, і організації гарантують, що процеси безпеки розгортаються, як очікувалося, хоча все ще може бути місце для вдосконалення. Організації на цьому рівні прагнуть підвищити свою стійкість і планують необхідні кроки для досягнення вищого рівня.

Рівні компетентності процесу в системі кіберстійкості InfraGuard:

Рівень 1:

Виконаний процес безпеки: На цьому рівні виконуються процеси безпеки. Основні заходи безпеки були впроваджені, і процеси працюють відповідно до базового плану. Це початковий крок, який вказує на те, що організація вжила основних заходів для захисту своєї інфраструктури. Поки робота все ще залишається, був зроблений перший крок до стійкості.

Рівень 0:

Незакінчений процес безпеки: це найнижчий рівень у системі, де процеси безпеки незавершені. Деякі аспекти процесів, можливо, не були реалізовані або можуть не функціонувати належним чином. Це вказує на те, що для досягнення гідного рівня стійкості потрібна значна робота.

Резюме програми на основі сценаріїв

Сценарій	Сектор	Головний інцидент	Технічні примітки	Ключові компоненти	Рівень стійкості
Зрив електричної мережі	Енергія (електромережа)	Цільова кібератака SCADA	Modbus TCP/IP, без шифрування, плоска мережа, ручне відновлення	Ситуаційна обізнаність, управління ризиками, активний захист	Дуже низький (Рівень 1)
Розумна лікарня-вимагач	Охорона здоров'я	Вимагацьке програмне забезпечення та медичне порушення Інтернету речей	Слабка сегментація, відсутність ІЧ-координації, застарілі резервні копії	Готовність, Стійкість, Відновлення Інцидентів	Розвиток (Рівень 2-3)
Саботаж системи аеропорту	Перевезення	Віджеж системи через компроміс ОТ	Застарілі ПЛК, SOC присутні, немає уніфікованих свердлів IT-OT	Готовність, захист, координація реагування	Сильний (Рівень 3–4)

Дослідницькі сценарії для застосування Framework:

Сценарій 1:

Порушення національної електричної мережі - кібератака на державні системи SCADA електричної мережі ініціює широкомасштабні регіональні відключення електроенергії. Системи SCADA на базі Modbus TCP/IP не мають шифрування та автентифікації і, таким чином, сприйнятливі до командних ін'єкцій та викрадення сеансів. Погана конструкція сегментації мережі полегшує бічне переміщення між операційними зонами. Немає інвентаризації активів або рішень для управління інформацією про безпеку та подіями (SIEM), а відновлення відбувається вручну протягом 24 годин. Це підпадає під умови технічних вразливостей, використаних під час попередніх атак, таких як атака на мережу України 2015 року.

Ключові компоненти, що впливають: ситуаційна обізнаність, управління ризиками, активний захист;

Індикативний рівень стійкості: дуже низький (рівень 1).

Дослідницькі сценарії для застосування Framework:

Сценарій 2:

Вимагацьке програмне забезпечення в розумній лікарняній системі - Зараження столичної лікарняної мережі програмами-вимагачами шифрує електронні медичні записи та калічить медичне обладнання з підтегомом IoT. Сегментація в лікарні мінімальна, зі спільним доступом між адміністративними робочими станціями та клінічними системами. Немає активного та функціонального механізму реагування на інциденти, де викликається захист кінцевих точок. 12-година відновлення спричиняє тимчасове порушення процесів відділення інтенсивної терапії. Це тип викриття, який використовується в реальних атаках, таких як атаки WannaCry на мережі охорони здоров'я.

Ключові компоненти, що постраждали: готовність, стійкість інфраструктури, відновлення інцидентів;

Індикативний рівень стійкості: розвивається (рівень 2-3).

Дослідницькі сценарії для застосування Framework:

Сценарій 3:

Сценарій 3: Інцидент кіберсаботажу в аеропорту - відбувається кібератака на процеси координації польотів та обробки багажу в міжнародному аеропорту. Сертифікований ISO/IEC 27001 аеропорт централізовано контролюється SOC (Центр операцій безпеки) без живих кібернавчань або вправ червоної команди між відділами. Багажна система працює зі застарілими ПЛК з фірмовою, не виправленою прошивкою і знаходиться під компрометацією ланцюга поставок або інсайдерською експлуатацією. Його можна відновити протягом 5 годин, але аналіз після інциденту визначає, що немає консолідації протоколів між IT та OT командами.

Ключові компоненти, що постраждали: готовність інфраструктури, активний захист, інтеграція реагування;

Індикативний рівень стійкості: сильний (рівень 3-4).

ВИСНОВКИ

У дипломній роботі розглянуто актуальну науково-прикладну проблему забезпечення кіберстійкості об’єктів критичної інфраструктури в умовах зростання інтенсивності та складності сучасних кіберзагроз. Проведений аналіз показав, що критична інфраструктура є ключовим елементом національної безпеки, економічної стабільності та соціальної життєздатності держави, а порушення її функціонування внаслідок кібератак може мати масштабні негативні наслідки.

У ході дослідження було проаналізовано сучасний стан і тенденції розвитку критичної інфраструктури, визначено основні типи загроз для її інформаційних та кіберфізичних компонентів, зокрема атаки типу ransomware, APT-кампанії, DDoS-атаки, уразливості операційних технологій та людського фактору. Показано, що традиційні підходи до кіберзахисту, орієнтовані переважно на запобігання атакам, є недостатніми, оскільки не враховують здатність системи адаптуватися, відновлюватися та зберігати критичні функції під час інцидентів.

ВИСНОВКИ

Значну увагу в роботі приділено аналізу нормативно-правової бази у сфері кібербезпеки об'єктів критичної інфраструктури. Розглянуто законодавство України, підзаконні акти, державні стратегії та міжнародні стандарти (ISO/IEC 27001, ISO/IEC 27005, NIST CSF, вимоги Директиви NIS2 ЄС). Установлено, що чинні нормативні документи визначають загальні вимоги до кіберзахисту, однак не містять єдиної формалізованої методики кількісної оцінки кіберстійкості, що ускладнює процес прийняття управлінських рішень.

На основі аналізу наукових джерел і сучасних підходів до оцінювання стійкості запропоновано методику оцінки кіберстійкості об'єктів критичної інфраструктури, яка базується на ризик-орієнтованому підході та інтегрує технічні, організаційні й управлінські аспекти кіберзахисту. Методика передбачає формування системи критеріїв і показників, що відображають здатність об'єкта запобігати кібератакам, виявляти інциденти, реагувати на них та відновлювати функціонування з мінімальними втратами.

ВИСНОВКИ

У рамках роботи розроблено інформаційно-аналітичний механізм для реалізації запропонованої методики, який дозволяє автоматизувати процес збору та обробки даних, розрахунок показників кіберстійкості та формування рекомендацій щодо підвищення рівня захищеності. Практичне застосування запропонованого підходу продемонструвало його придатність для використання в різних секторах критичної інфраструктури та можливість адаптації до специфіки конкретних об'єктів. Отримані результати підтверджують доцільність переходу від виключно захисних моделей кібербезпеки до концепції кіберстійкості, яка забезпечує комплексний підхід до управління ризиками та безперервністю функціонування критичних систем. Практична цінність роботи полягає в можливості використання розробленої методики під час проведення аудитів кібербезпеки, оцінювання ризиків, планування заходів із підвищення стійкості та підтримки прийняття управлінських рішень у сфері захисту об'єктів критичної інфраструктури.

INDEX COPERNICUS

GS 141125-066 dated 14.11.2025

CERTIFICATE
OF PARTICIPATION AND PUBLICATION

Dmytro Dudynets

participated in the X Correspondence International Scientific and Practical Conference
Scientific researches and methods of their carrying out: world experience and domestic realities
held on November 14th, 2025 by
NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

and published scientific paper
МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРІНЦЕДЕНТІВ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

in Periodical scientific journal «**GRAIL OF SCIENCE**»
№ **58**; ISSN 2710-3056; Media Identifier R30-02704;
DOI 10.36074/grail-of-science.14.11.2025

0.6 ECTS credits (18 hours)
Recommended by the Academic Council of the Institute of Scientific and Technical Integration and Cooperation
Protocol № 45 from November 14th, 2025

IHTIC

Head of the
NGO «European Scientific Platform»
Chairman of the Organizing committee
GOLDENBLAT MIRIAM

Head of Community Outreach of the
LLC «International Centre
Corporative Management»
RACHAEL APARO

ДЯКУЮ ЗА УВАГУ!