КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему:

Технологія інтелектуального захисту інформації критично важливих об'єктів

Андрєєв Марк Анатолійович

(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
Делембовський М.М.
„___" _____20___ року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Технологія інтелектуального захисту інформації критично важливих об'єктів

(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 Андрєєв Марк Анатолійович
(прізвище, ім'я та по батькові повністю)
125 «Кібербезпека та захист інформації»
(спеціальність)
Безпека інформаційних і комунікаційних систем
(освітня програма)
Група БІКСм-24
Керівник Шабала Є.Є.
(прізвище та ініціали)
Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент Терентьєв О.О.
(прізвище та ініціали)
Ідентичність підтверджую

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет:	автоматизації і інформаційних технологій
Випускова кафедра:	кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти:	магістр
Спеціальність:	125 «Кібербезпека та захист інформації»
Освітня програма:	Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

„___"_____20___ року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Андрєєв Марк Анатолійович

(прізвище, ім'я та по батькові здобувача)

1. Тема роботи **«Технологія інтелектуального захисту інформації критично важливих об'єктів»**

затверджена наказом ректора КНУБА № 1635/23.2/25 від «30» вересня 2025 року

2. Керівник роботи Шабала Євгенія Євгенівна

кандидат технічних наук, доцент

(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз захищеності критично важливих об'єктів

Р. 2. Архітектура системи інтелектуального захисту критично важливих об'єктів

Р. 3. Моделі та методи моніторингу загроз на критично важливі об'єкти

Р. 4. Розробка технології інтелектуального захисту критично важливих об'єктів

5. Графічний матеріал за розділами:

Р. 1. Актуальність, мета, завдання, об’єкт, предмет дослідження, наукова новизна, класифікація об’єктів критичної інфраструктури, потенційні впливи на об'єкти критичної інфраструктури.

Р. 2. Схема архітектури системи інтелектуального захисту критично важливих об'єктів, Архітектура системи штучного інтелекту для захисту критично важливих об’єктів, Модулі виявлення загроз, Застосування IoT в системах інтелектуального захисту критично важливих об’єктах.

Р. 3. Модель DDOS атаки на критичну інфраструктуру, Модель атак, спрямовані на використання вразливостей програмного чи апаратного забезпечення на критичну інфраструктуру, Методи моніторингу загроз на критично важливі об’єкти, Алгоритм реагування на інциденти загроз на критичну інфраструктуру

Р. 4. Завдання системи відеоспостереження для критично важливих об’єктів, Схема поюудови счистеми відеонагляду на критично ваєливих об’єктах, Ідентифікація за відбитком пальця, Використання дронів для охорони периметра критично важливого об’єкта, Застосування фреймворку Mitre ATT&CK. Процес моделювання векторів атак на компанію, Технологія інтелектуального захисту критично важливих об’єктів, висновки.

6. Консультанти розділів кваліфікаційної випускної роботи:

Розділ	Прізвище, ініціали та посада	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			
Розділ 4.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. Аналіз захищеності критично важливих об’єктів	Вересень 2025
Розділ 2. Архітектура системи інтелектуального захисту критично важливих об’єктів	Жовтень 2025
Розділ 3. Моделі та методи моніторингу загроз на критично важливі об’єкти	Листопад 2025
Розділ 4. Розробка технології інтелектуального захисту критично важливих об’єктів	Грудень 2025
Остаточне оформлення роботи	Грудень 2025

Направлення роботи для перевірки на плагіат	Грудень 2025
Попередній захист роботи	Грудень 2025
Направлення роботи на рецензування	Грудень 2025

8. Дата видачі завдання _____

Керівник _____ _____

Здобувач _____ _____

АНОТАЦІЯ

Андрєєв М. А. «Технологія інтелектуального захисту інформації критично важливих об’єктів»

У роботі досліджено теоретичні та практичні основи захисту інформації критично важливих об’єктів в умовах зростання кіберзагроз. Проаналізовано класифікацію об’єктів критичної інфраструктури, основні загрози й ризики їх функціонування, а також сучасний стан їх захищеності. Розглянуто нормативно-правові та організаційні аспекти забезпечення безпеки критичної інфраструктури.

У роботі запропоновано архітектуру системи інтелектуального захисту критично важливих об’єктів, що поєднує засоби фізичної безпеки, інформаційні та операційні технології, IoT, а також інтелектуальні методи аналізу даних. Досліджено моделі та методи моніторингу загроз, зокрема використання IDS/IPS, SIEM-систем, аналізу мережевого трафіку, систем виявлення уразливостей і фреймворку MITRE ATT&CK для моделювання векторів атак.

У практичній частині роботи розроблено технологію інтелектуального захисту критично важливих об’єктів із застосуванням систем відеоспостереження, контролю доступу, біометричної ідентифікації, RFID-технологій та безпілотних засобів охорони периметра. Запропоновано алгоритм реагування на інциденти безпеки та інтеграцію різних підсистем у єдину комплексну систему захисту.

Отримані результати підтверджують, що застосування інтелектуальних методів аналізу та комплексного підходу до захисту дозволяє своєчасно виявляти загрози, зменшувати ризики та підвищувати рівень безпеки і стійкості критично важливих об’єктів.

Ключові слова: інтелектуальний захист, критична інфраструктура, кібербезпека, виявлення загроз, управління ризиками.

SUMMARY

Andrieiev M. A. “Technology for Intelligent Information Protection in Critical Infrastructure.”

Master’s qualification thesis in specialty: 125 “Cybersecurity and Information Protection”, educational program: “Security of Information and Communication Systems”. – Kyiv National University of Civil Engineering and Architecture. – Kyiv, 2025.

The thesis examines the theoretical and practical foundations of information protection for critical infrastructure objects under increasing cyber threats. The classification of critical infrastructure objects, key threats and operational risks, as well as the current state of their security are analyzed. Regulatory and organizational aspects of ensuring critical infrastructure security are also considered.

An architecture of an intelligent protection system for critical infrastructure objects is proposed, combining physical security means, information and operational technologies, IoT solutions, and intelligent data analysis methods. Models and methods for threat monitoring are examined, including the use of IDS/IPS, SIEM systems, network traffic analysis, vulnerability detection systems, and the MITRE ATT&CK framework for modeling attack vectors.

In the practical part of the thesis, a technology for intelligent protection of critical infrastructure objects is developed using video surveillance systems, access control systems, biometric identification, RFID technologies, and unmanned perimeter protection tools. An incident response algorithm is proposed, as well as the integration of various subsystems into a unified comprehensive security system.

The obtained results confirm that the application of intelligent analysis methods and a comprehensive protection approach enables timely threat detection, risk reduction, and improvement of the security and resilience level of critical infrastructure objects.

Keywords: intelligent protection, critical infrastructure, cybersecurity, threat detection, risk management.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	*Андрєєв Марк Анатолійович* *Andrieiev Mark Anatoliiovych*

ЗВО	Київський національний університет будівництва і архітектури		
Тема (українською та англійською)	Технологія інтелектуального захисту інформації критично важливих об’єктів. Technology for Intelligent Information Protection in Critical Infrastructure.		
Освітній ступінь	магістр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп’ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист даних»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	к.т.н., доцент Шабала Євгенія Євгенівна		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	112	чотири	20
Розділ 1	Аналіз захищеності критично важливих об’єктів		
Розділ 2	Архітектура системи інтелектуального захисту критично важливих об’єктів		
Розділ 3	Моделі та методи моніторингу загроз на критично важливі об’єкти		
Розділ 4	Розробка технології інтелектуального захисту критично важливих об’єктів		
Висновки по роботі	Робота присвячена розробці інтелектуального захисту критичної інфраструктури. Запропонований підхід дозволяє своєчасно виявляти загрози та підвищити безпеку. Впровадження технології сприятиме надійності стратегічно важливих об'єктів.		
Ключові слова: Keywords:	Інтелектуальний захист, критична інфраструктура, кібербезпека, виявлення загроз, управління ризиками Intelligent protection, critical infrastructure, cybersecurity, threat detection, risk management		

Здобувач _____/ _____

Керівник _____/ _____

“___” _____ 20__

ЗМІСТ

ВСТУП

У сучасному світі технології розвиваються з неймовірною швидкістю, забезпечуючи численні можливості для покращення якості життя, підвищення ефективності виробництва і забезпечення комунікацій. Ці досягнення, що охоплюють штучний інтелект, інтернет речей, великі дані та хмарні обчислення, трансформують кожен аспект нашого існування, від повсякденних рутин до складних промислових процесів. Однак, ця технологічна революція також створює нові вразливості та ризики, зокрема в контексті захисту критично важливих об'єктів. Зі зростанням взаємозв'язку та інтеграції систем, потенційні наслідки кібератак та фізичних загроз стають все більш серйозними і масштабними. Тому, поряд з використанням передових технологій, надзвичайно важливо розробляти та впроваджувати ефективні стратегії захисту, які здатні адаптуватися до нових викликів і забезпечувати стійкість критичної інфраструктури. Проте, з цими досягненнями приходять і нові виклики. Один з найзначніших аспектів сучасного суспільства — це необхідність захисту критично важливих об’єктів, які є не-від’ємною частиною інфраструктури кожної країни.

Критично важливі об’єкти включають в себе енергетичні системи, транспортну інфраструктуру, фінансові установи, системи комунального забезпечен-ня та багато іншого. Їх безперебійна робота є ключовою для стабільності та без-пеки національної економіки і суспільства в цілому. Уявіть собі, що станеться, якщо раптово вийде з ладу електромережа, що забезпечує живленням велике місто, або якщо хакери проникнуть у систему управління залізничним транспортом. Наслідки можуть бути катастрофічними: від масштабних відключень електроенергії та транспортного колапсу до фінансових втрат та соціальної дестабілізації. Порушення їх функціонування може призвести до серйозних наслідків, таких як економічні збитки, соціальні незручності, а в деяких випадках навіть до загрози національній безпеці.

Технології, що забезпечують цей захист, постійно вдосконалюються, оскільки нові загрози і вразливості вимагають нових підходів і рішень. Це включає в

себе розробку передових систем виявлення вторгнень, використання штучного інтелекту для аналізу даних та прогнозування загроз, а також впровадження надійних механізмів шифрування та аутентифікації. Важливим аспектом є також забезпечення стійкості систем до фізичних атак, таких як терористичні акти або стихійні лиха, шляхом резервування критичних компонентів та розробки планів відновлення після аварій. Інтелектуальний захист не обмежується лише технологічними аспектами, але також охоплює організаційні і управлінські аспекти, які взаємодіють з технічними рі-шеннями для забезпечення комплексного підходу до безпеки.

У побудові технології інтелектуального захисту є практичний підхід до реалізації систем захисту, а це: різні методи, такі як моніторинг і виявлення загроз, управління ризиками, системи резервування і відновлення після аварій, а також навчання і підготовка персоналу. Крім того, важливо враховувати інтеграцію з іншими системами безпеки, такими як фізична охорона та системи контролю доступу, для створення єдиного захисного бар'єру. Це вимагає розробки чітких протоколів та процедур, а також проведення регулярних навчань та тренувань для персоналу, щоб забезпечити готовність до реагування на будь-які загрози.

Отже, захист критично важливих об’єктів є не лише технічною задачею, але й стратегічним пріоритетом для будь-якого суспільства. Уряди, бізнес та наукові установи повинні спільно працювати над розробкою та впровадженням ефективних стратегій захисту, які враховують унікальні характеристики кожної країни та її інфраструктури. Це також включає в себе забезпечення достатнього фінансування для досліджень та розробок у сфері безпеки, а також підтримку освіти та навчання фахівців з кібербезпеки та захисту критичної інфраструктури. В умовах постійних змін та зростання рівня загроз, ефективні рішення у сфері інтелектуального за-хисту є необхідними для забезпечення стабільності та безпеки.

1. АНАЛІЗ ЗАХИЩЕНОСТІ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ

1.1. Ідентифікація критично важливих об'єктів та їх класифікація

Підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей[1].

Критично важливі об'єкти (КВО) є ключовими компонентами інфраструктури будь-якої держави або суспільства, від функціонування яких залежить загальна стабільність і безпека. Їхнє належне функціонування забезпечує ефективну діяльність усіх секторів економіки та соціальних інститутів. З огляду на зростаючі загрози, як природного, так і антропогенного характеру, захист цих об'єктів є пріоритетним завданням для державних структур та організацій.

Класифікація КВО може бути проведена за різними критеріями:

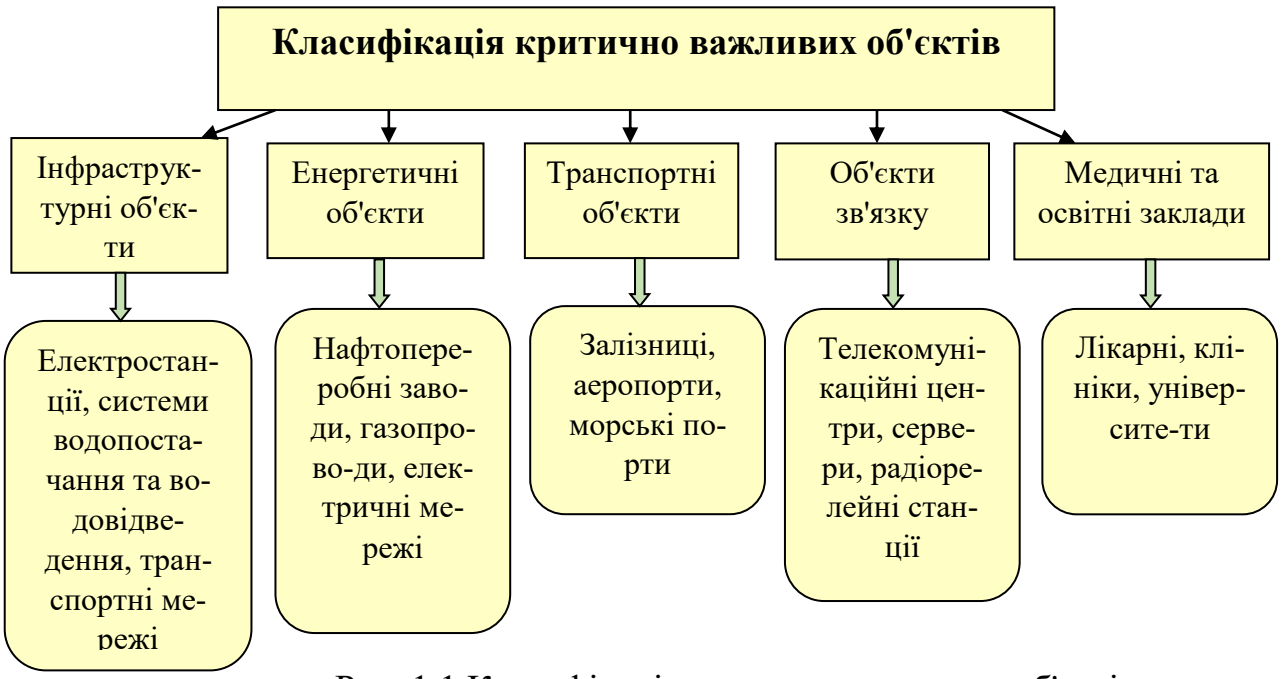


Рис. 1.1 Класифікація критично важливих об'єктів

Класифікація критично важливих об'єктів (КВО) може бути різною в залежності від специфіки і контексту, але в загальному випадку їх можна класифікувати за кількома основними критеріями.

Нижче наведено основні категорії та підкатегорії, які широко використовуються для класифікації КВО:

1. Інфраструктурні об'єкти - це об'єкти, які забезпечують основні функції суспільства та економіки:

Таблиця 1.1 –Приклад об’єктів інфраструктури

Назва	Приклад
Енергетичні об'єкти	**Електростанції**: атомні, теплові, гідроелектричні, вітрові, сонячні. **Газопроводи і нафтопроводи**: системи транспортування газу і нафти. **Трансформаторні підстанції**: об'єкти для розподілу електричної енергії.
Водопостачання і водовідведення	**Водозабірні станції**: системи для отримання води з природних джерел. **Очисні споруди**: установки для очищення стічних вод. **Резервуари для води**: сховища води для забезпечення населення.
Транспортні об'єкти	**Залізниці**: залізничні лінії і станції. **Аеропорти**: об'єкти для авіаційного транспорту. **Морські порти**: об'єкти для перевалки вантажів і пасажирів

2. Комунікаційні об'єкти - ці об'єкти забезпечують зв'язок і передачу інформації.

Таблиця 1.2 – Приклади комунікаційних об’єктів

Назва	Приклад
Телекомунікаційні центри	**Серверні кімнати і дата-центри**: об'єкти для зберігання та обробки інформації. **Радіорелейні станції**: об'єкти для передачі даних бездротовим способом.

Системи зв'язку	**Мобільні оператори**: вежі і базові станції для мобільного зв'язку. **Інтернет-провайдери**: інфраструктура для надання доступу до Інтернету.

3. Фінансові об'єкти - об'єкти, що забезпечують функціонування фінансової системи:

Таблиця 1.3 – Приклади фінансових об’єктів

Назва	Приклад
Банківські установи	**Центральні банки**: ключові фінансові установи, які контролюють національну валюту. **Комерційні банки**: банки, які здійснюють фінансові операції з клієнтами.
Фондові біржі	**Фондові ринки**: платформи для торгівлі цінними паперами.

4. Медичні та соціальні об'єкти - об'єкти, важливі для охорони здоров'я та соціального забезпечення.

Таблиця 1.4 – Приклади медичних і соціальних об’єктів

Назва	Приклад
Медичні заклади	**Лікарні та клініки**: установи для надання медичних послуг. **Лабораторії**: об'єкти для проведення медичних і наукових досліджень
Освітні заклади	**Університети і школи**: установи для навчання і виховання.

5. Екологічні об'єкти - об'єкти, що впливають на екологічну безпеку та природні ресурси.

Таблиця 1.5 – Приклади екологічних об’єктів

Назва	Приклад
Екологічні об'єкти	**Природні резервати і парки**: об'єкти для збереження біорізноманіття і природних ресурсів.
	Системи контролю за забрудненням: обладнання для моніторингу і управління екологічною ситуацією

6. Державні об'єкти - об'єкти, що мають стратегічне значення для держави.

Таблиця 1.6 – Приклади державних об’єктів

Назва	Приклад
Військові об'єкти	**Бази і склади**: місця зберігання військової техніки і боєприпасів. **Ракетні установки**: об'єкти для розміщення і запуску ракет.
Адміністративні будівлі	**Урядові установи**: приміщення для роботи державних органів.

7. Інші критично важливі об'єкти:

Таблиця 1.7 – Приклади інших критично важливих об’єктів

Назва	Приклад
Цивільні об'єкти	**Системи охорони правопорядку**: поліційні станції, системи відеоспостереження.
Культові об'єкти	**Храми і церкви**: релігійні установи, що мають важливе значення для певних груп населення.

Ця класифікація допомагає систематизувати критично важливі об'єкти і зрозуміти, які саме аспекти їх захисту є пріоритетними для забезпечення стабільності та безпеки суспільства.

1.2. Роль критично важливих об’єктів у забезпеченні безпеки та стабільності країни.

Критично важливі об'єкти — це об'єкти інфраструктури, чиє функціонування є життєво важливим для нормального функціонування держави або суспільства. Втрата їхньої працездатності може призвести до серйозних соціальних, економічних та безпекових наслідків.

До критичних інфраструктур відносяться фізичні та інформаційні технологічні об'єкти, мережі, послуги та активи, порушення або знищення яких може серйозно вплинути на здоров'я, безпеку, захищеність або економічний добробут громадян. Вони охоплюють багато секторів економіки, зокрема банківську справу,

фінанси, транспорт і розподіл, енергетику, комунальні послуги, охорону здоров'я, постачання продовольства, зв'язок, а також ключові державні послуги.

Деякі з цих критичних елементів є не стільки інфраструктурою, скільки мережами або ланцюгами постачання, які забезпечують доставку основних продуктів чи послуг.

Критичні об'єкти інфраструктури в Україні тісно взаємопов'язані і взаємозалежні. Об'єднання даних в єдиний реєстр, оптимізація галузі і впровадження ефективних методів ведення бізнесу вимагають розроблення універсальної методики для ідентифікації цих об'єктів.

Наявність потенційно небезпечних об'єктів і концентрація населення в їхніх районах можуть призвести до надзвичайних ситуацій, що викликають значні людські і матеріальні втрати.

Найбільш значущі об’єкти критичної інфраструктури України стали більш залежними від загально інформаційних технологій, включаючи інтернет-мережу, космічну радіонавігацію та зв'язок.

В умовах воєнного стану проблеми можуть поширюватися на цілі мережі об’єктів інфраструктури, викликаючи несподівані та серйозні збої в роботі спеціалізованого обладнання під час ракетних ударів.

Для підвищення рівня безпеки можна запропонувати три чинники визначення пріоритетності захисту потенційно-небезпечних об’єктів критичної інфраструктури:

- масштаб - втрата критично важливого елемента якого, оцінюється за розміром та національною значущістю;

- величина - ступінь впливу або втрати може бути оцінена як надзвичайна ситуація державного рівня;

- вплив часу – визначення проміжку часу, за який втрата об’єкта може мати серйозні наслідки [2].

Визначення критичної інфраструктури враховує такі елементи:

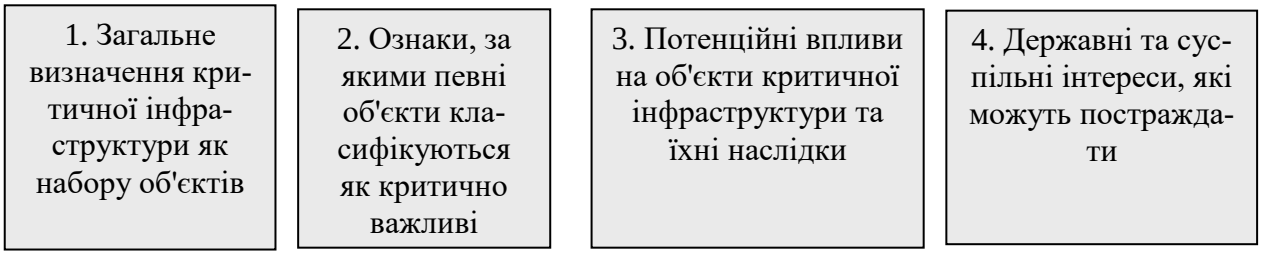


Рис. 1.2 Елементи визначення критичної інфраструктури

1. Загальне визначення критичної інфраструктури як набору об'єктів.

Загальне визначення критичної інфраструктури як набору об'єктів є концепцією, що описує критичну інфраструктуру як комплекс взаємопов'язаних фізичних та інформаційних об'єктів і систем, які забезпечують основні функції та послуги в суспільстві. Це визначення підкреслює, що критична інфраструктура складається з різних об'єктів, які разом забезпечують функціонування ключових секторів економіки і життєво важливих послуг, таких як енергетика, транспорт, комунальні послуги, охорона здоров'я, фінанси, та інші важливі галузі.

Поняття «структура» є близьким за суттю поняттю «система», яке у перекладі з грецької є цілим, О. П. Єрменчук кандидат юридичних наук 36 № 11(193) 2017 року думки експертів з права складеним з частин або з’єднанням. Відомо, що поняття «система» визначається як множина елементів, які знаходяться у взаємодії між собою і утворюють певну цілісність, єдність [3]. Як відомо, друга елементарна змістовна складова «інфра» означає «під» та вживається у значенні розташування під чимось, або нижче чогось.

Так, наприклад, інфраструктура може розглядатися як сукупність (комплекс) пов’язаних між собою або структур та галузей (виробничих або невиробничих), їх підприємств та організацій, сфер діяльності, або як сукупність об’єктів, які забезпечують нормальне (або основу) функціонування будь-якої системи. Вона може включати сукупність споруд, будинків, систем і служб, необхідних для функціонування галузей матеріального виробництва та забезпечення умов життєдіяльності суспільства. Інфраструктура розглядається ібяк капітальне обладнання,

яке використовується для надання суспільно доступних послуг, у тому числі транспортних та телекомунікаційних, з газо-, електро і водопостачання. Зустрічається також визначення інфраструктури як складові частини загального устрою економічного та політичного життя, які носять підпорядкований допоміжний характер у забезпеченні нормальної діяльності економічної або політичної системи [4].

Важливо, що ці об'єкти часто є взаємопов'язаними і залежними один від одного, і будь-яке їх порушення або знищення може мати серйозні наслідки для суспільства і економіки.

2. Ознаки, за якими певні об'єкти класифікуються як критично важливі.

Класифікація об'єктів як критично важливих є основою для розробки стратегій їх захисту та управління ризиками. Ознаки, за якими певні об'єкти класифікуються як критично важливі, можуть включати наступні критерії наведено в Таблиці 1.8.

Таблиця 1.8 – Ознаки класифікації критично важливих об’єктів

Назва ознаки	Визначення
Функціональна значимість	Об'єкти, які виконують основні функції, без яких неможливе забезпечення життєво важливих послуг або функціонування важливих систем (наприклад, електричні станції, водопроводи, системи охорони здоров'я).
Залежність суспільства або економіки	Об'єкти, від яких значною мірою залежать ключові аспекти економіки або соціального життя, такі як банки, транспортні мережі, системи зв'язку.
Масштаб впливу	Об'єкти, порушення або знищення яких призводить до значних негативних наслідків для великої кількості людей або територій (наприклад, нафтопереробні заводи, великі лікарні).
Стратегічна важливість	Об'єкти, які мають стратегічне значення для національної безпеки та оборони (наприклад, військові бази, стратегічні склади).
Складність та унікальність	Об'єкти, які є складними в технічному або організаційному плані і мають унікальні характеристики або

	функції, які важко відновити або замінити (наприклад, специфічне обладнання для промислового виробництва).
Економічний вплив	Об'єкти, чий збиток або знищення призводить до суттєвих економічних втрат, таких як великі підприємства або критичні елементи інфраструктури, які підтримують економічні операції (наприклад, важливі транспортні вузли).
Безпекові наслідки	Об'єкти, порушення яких може привести до значних загроз для громадської безпеки, такі як об'єкти, що зберігають небезпечні матеріали або системи, що забезпечують охорону правопорядку.

3. Потенційні впливи на об'єкти критичної інфраструктури та їхні наслідки**.**

Об'єкти критичної інфраструктури є надзвичайно важливими для стабільного функціонування сучасного суспільства. Різноманітні потенційні загрози, від природних катастроф до терористичних атак і кіберзагроз, можуть мати серйозні наслідки для цих об'єктів. Ефективне управління ризиками, моніторинг загроз і розробка планів дій для реагування на надзвичайні ситуації є критично важливими для забезпечення безпеки і стабільності критичної інфраструктури.

3. Державні та суспільні інтереси, які можуть постраждати.

Атака на критично важливі об'єкти може мати серйозні наслідки для як державних, так і суспільних інтересів. Вона здатна порушити функціонування ключових інститутів і систем, що забезпечують стабільність і безпеку держави і її громадян.

Зокрема, критична інфраструктура може визначатися як:

1. Сукупність об'єктів, систем і ресурсів.

2. Сукупність об'єктів інфраструктури держави.

3. Підприємства та установи в таких галузях, як енергетика, хімічна промисловість, транспорт, фінанси, інформаційні технології і телекомунікації, продовольство, охорона здоров'я, комунальні послуги.

4. Сукупність об'єктів, технологій, державних і наукових структур.

5. Об'єкти, системи, мережі або їх частини, які забезпечують важливі функції та послуги.

Ознаки критичної інфраструктури включають:

Таблиця 1.9 – Ознаки критичної інфраструктури

Критичність	Визначення ознаки	Характеристики ознаки
Критично важливі	це ті, без яких функціонування суспільства і держави стало б неможливим або суттєво ускладнилося. Вони мають особливе значення для забезпечення життєво важливих функцій і послуг	Неможливість заміни: Відсутність або зупинка цих об'єктів призводить до прямого порушення життєвих потреб людей і може мати катастрофічні наслідки. Наприклад, системи водопостачання, електропостачання або лікувальні установи. Високий рівень залежності: Громадяни, підприємства та інші сфери життя повністю залежать від безперебійної роботи цих об'єктів. Якщо ці об'єкти не функціонують, це спричиняє серйозні проблеми для повсякденного життя і безпеки. Значні наслідки в разі пошкодження: Порушення функціонування критично важливих об'єктів може викликати надзвичайні ситуації, великі матеріальні втрати і загрози для здоров’я та життя людей.
Найбільш важливі	це об'єкти, які відіграють ключову роль у забезпеченні функціонування основних секторів економіки та соціальних послуг. Хоча їх порушення не викликає миттєвих і катастрофічних наслідків, це все ж може призвести до значних проблем і дискомфорту.	Важливість для функціонування економіки: Ці об'єкти включають підприємства, що забезпечують постачання важливих товарів і послуг, таких як енергетика, транспорт або зв’язок. Їхні проблеми можуть спричинити перебої в економічних процесах. Потенційні затримки і збої: Порушення в роботі цих об'єктів може призвести до значних затримок у наданні послуг і негативних економічних наслідків, хоча і менш серйозних, ніж у випадку критично важливих об'єктів. Довгострокові наслідки: Негативний вплив на ці об'єкти може створити затримки в розвитку інфраструктури і тривалі соціальні

		та економічні проблеми.
Стратегічно важливі	це ті, що мають важливе значення для державних стратегій, довгострокового планування та національної безпеки. Вони забезпечують функціонування стратегічних секторів і служб, які підтримують державну політику і стратегічні цілі.	Вплив на національні стратегії: Ці об'єкти підтримують національні стратегії і політику, такі як оборона, енергетична безпека та забезпечення критичних ресурсів. Наприклад, стратегічні резерви, військові об'єкти або системи кібербезпеки. Довгострокове значення: Їхня роль полягає в підтримці національних інтересів на стратегічному рівні, забезпечуючи довгострокову стабільність і безпеку держави. Ризик для національної безпеки: Порушення в роботі стратегічно важливих об'єктів може загрожувати національній безпеці, економічній незалежності та стратегічним інтересам держави.

Отже, необхідно дослідити критерії, які визначають, що саме робить мережу інфраструктури або конкретний її елемент критично важливими. Приоритет у захисті слід визначати на основі галузевого та колективного досвіду, отриманого під час моніторингу таких об’єктів.

1.3. Загрози та ризики для критично важливих об’єктів

Відповідно до Кодексу цивільного захисту України, надзвичайною ситуацією є обстановка на окремій території чи суб’єкті господарювання на ній або водному об’єкті, що характеризується порушенням нормальних умов життєдіяльності населення, спричинена катастрофою, аварією, пожежею, стихійним лихом, епідемією, епізоотією, епіфітотією, застосуванням засобів ураження або іншою небезпечною подією, що призвела (може призвести) до виникнення загрози життю або здоров’ю населення, великої кількості загиблих і постраждалих, завдання значних матеріальних збитків, а також до неможливості проживання населення на такій території чи об’єкті, провадження на ній господарської діяльності [5].

Загроза розглядається як небезпечне явище, речовина, діяльність людини або стан, що може призвести до соціальних та економічних збитків, втрати життя, травмування або інших наслідків для здоров'я населення, втрати майна, засобів до існування та послуг, завдання шкоди довкіллю [6].

У національних законодавствах провідних країн світу загрози для критичної інфраструктури зазвичай поділяються на три основні категорії в залежності від їх походження. Однак існують деякі відмінності в підходах. Наприклад, у США і Канаді до загроз критичній інфраструктурі відносяться зловмисні дії (атаки терористів або злочинців), природні небезпеки (урагани, торнадо, землетруси, цунамі, повені, екстремальні погодні умови тощо) і техногенні надзвичайні ситуації (авіаційні катастрофи, ядерні аварії, пожежі, аварії в енергетичних системах, викиди небезпечних речовин тощо). Цей підхід дозволяє враховувати потреби всього суспільства у безпечному середовищі існування через ухвалення обґрунтованих управлінських рішень у сфері зниження ризику катастроф і мінімізації їх негативних наслідків для населення, об'єктів критичної інфраструктури та довкілля [7].

Загалом цей підхід передбачає виконання на рівні держави відповідних завдань, найбільш важливим із яких є включення заходів щодо зниження ризику катастроф у плани і програми соціальноекономічного розвитку [8]. Кінцевою метою при цьому є запобігання виникненню нових і зниження відомих ризиків катастроф шляхом здійснення комплексних та інклюзивних економічних, структурних, юридичних, соціальних, медико-санітарних, культурних, освітніх, екологічних, технологічних, політичних та інституційних заходів.

Зниження ризику катастроф має здійснюватися на місцевому, регіональному і загальнодержавному рівнях з урахуванням таких пріоритетів [8]: розуміння ризику катастроф; удосконалення організаційно-правових рамок управління ризиком катастроф; інвестиції в заходи зі зниження ризику катастроф з метою зміцнення потенціалу протидії; підвищення готовності до катастроф для забезпечення ефективного реагування та впровадження принципу «Зробити краще, ніж було» в діяльність із відновлення, реабілітації та реконструкції [7].

Критична інфраструктура містить не тільки фізичні об’єкти, але й величезні обсяги інформації, які є невід’ємною частиною її функціонування. Ця інформація, від даних про енергопостачання до фінансових транзакцій та операційних процесів, сама по собі стає ціллю для зловмисників і потребує особливого захисту.

Інтелектуальний захист критичної інфраструктури має враховувати не лише фізичні, а й інформаційні аспекти, забезпечуючи цілісність, конфіденційність та доступність даних. Захист інформації є критично важливим для попередження атак, що можуть вплинути на функціонування об’єктів, а також для зменшення негативних наслідків у разі успішної кібератаки.

Потенційні впливи на об'єкти критичної інфраструктури і їхні наслідки можуть бути різними за характером і масштабом. Основні категорії впливів і їхні наслідки включають:

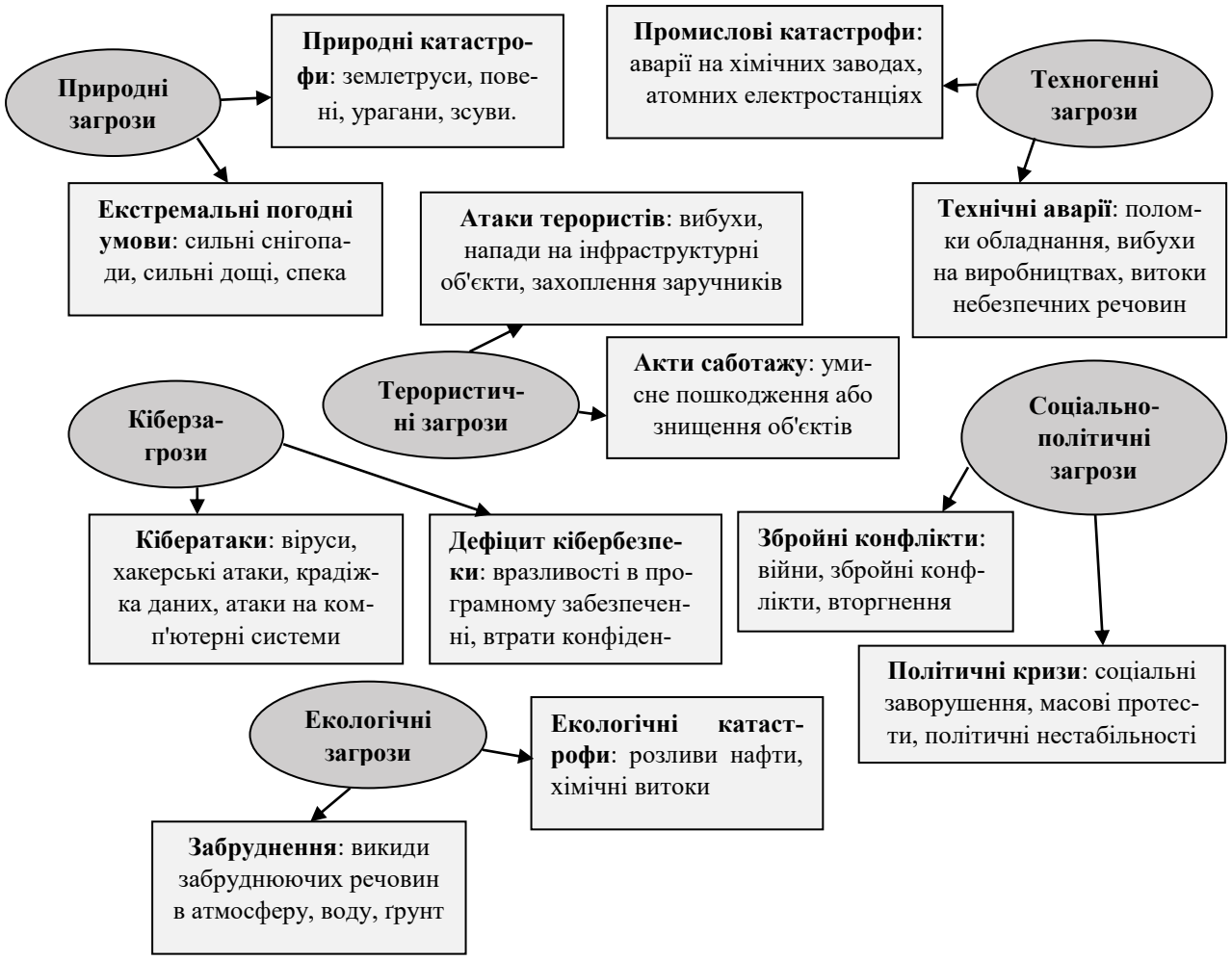


Рис. 1.10 Потенційні впливи на об'єкти критичної інфраструктури

Впливи на критично важливі об'єкти можуть бути різноманітними і мати серйозні наслідки для економіки, суспільства і довкілля. Важливо не тільки розуміти ці наслідки, але і вживати заходів для зменшення ризиків і підвищення стійкості інфраструктури.

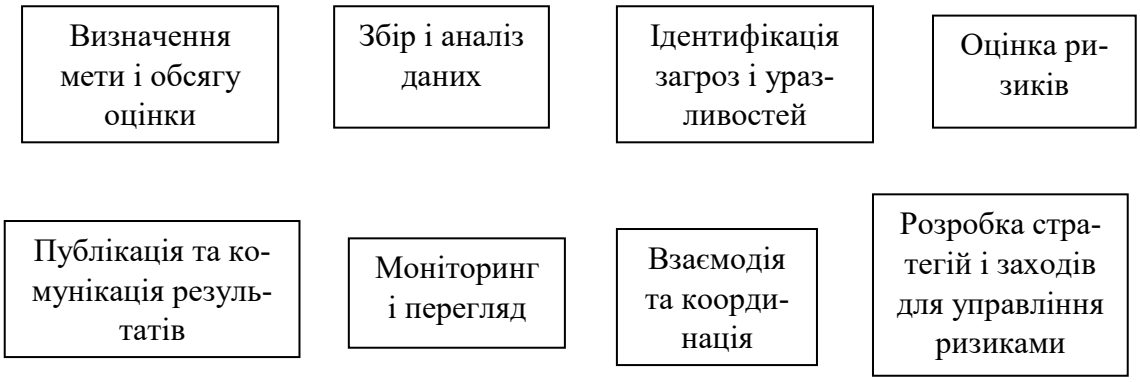
Наслідки впливів:

Важливо мати комплексний підхід до управління ризиками і впливами, що включає превентивні заходи, планування дій у надзвичайних ситуаціях, і стратегії відновлення для мінімізації негативних наслідків і забезпечення безперервного функціонування критичної інфраструктури.

Рис. 1.11 Наслідки впливів на критично важливі об’єкти

Проведення національної оцінки ризику в Україні є важливою складовою частиною стратегічного управління безпекою та захистом критичної інфраструктури.

Основні етапи та аспекти такого процесу включають:



3. **Визначення мети і обсягу оцінки:**

- Установлення цілей національної оцінки ризику, зокрема ідентифікації найбільш критичних загроз для національної безпеки та економіки.
- Окреслення обсягу оцінки, який може включати різні аспекти національної інфраструктури, такі як енергетика, транспорт, зв'язок, водопостачання тощо.

4. **Збір і аналіз даних:**

- Збір інформації про потенційні загрози, уразливості та можливі наслідки для різних секторів інфраструктури.
- Аналіз історичних даних про інциденти, що сталися, та сучасних загроз, врахування змін у глобальному і національному контексті.

5. **Ідентифікація загроз і уразливостей:**

- Визначення основних загроз, таких як природні катастрофи, техногенні аварії, зловмисні дії (тероризм, кібератаки) та соціально-політичні ризики.
- Оцінка уразливостей, які можуть підвищити ймовірність або серйозність наслідків загроз.

6. **Оцінка ризиків:**

- Проведення якісної та кількісної оцінки ризиків, включаючи ймовірність їх виникнення і потенційний вплив на критичну інфраструктуру.
- Розрахунок потенційних збитків та впливу на суспільство, економіку та навколишнє середовище.

7. **Розробка стратегій і заходів для управління ризиками:**

- Розробка рекомендацій і заходів для зменшення ризиків та підвищення стійкості критичної інфраструктури.

- Планування заходів з підготовки до надзвичайних ситуацій, включаючи плани евакуації, аварійного реагування та відновлення.

8. **Взаємодія та координація:**

- Налагодження ефективної взаємодії між державними органами, приватним сектором і громадськістю для забезпечення комплексного підходу до управління ризиками.
- Створення механізмів для регулярного обміну інформацією та координації дій між усіма учасниками процесу.

9. **Моніторинг і перегляд:**

- Запровадження систем моніторингу для оцінки ефективності впроваджених заходів і оновлення оцінки ризиків у відповідь на нові загрози або зміни в обставинах.
- Регулярний перегляд і коригування національної оцінки ризику з урахуванням змін у зовнішньому середовищі та внутрішніх умовах.

10. **Публікація та комунікація результатів:**

- Публікація основних результатів оцінки ризику для підвищення обізнаності серед усіх зацікавлених сторін.
- Комунікація результатів з метою залучення суспільства та бізнесу до процесу управління ризиками і забезпечення їхньої участі у реалізації заходів безпеки.

Цей процес допомагає не лише у забезпеченні безпеки критичної інфраструктури, але й у підвищенні загальної стійкості національної системи до різноманітних загроз і надзвичайних ситуацій.

У країнах ЄС для проведення національної оцінки ризику (National Risk Assessment) критичної інфраструктури рекомендується застосовувати матрицю ризику розміром 5 х 5.

Матриця ризиків — це інструмент для оцінки та управління ризиками, який використовують для ідентифікації та аналізу потенційних загроз і їх можливих наслідків.

Вона представляє собою таблицю або графік, де ризики класифікуються за двома основними критеріями: ймовірність їх виникнення і ступінь їхнього впливу (серйозності наслідків).

Ця матриця слугує засобом для візуалізації результатів оцінки та представлена на Рис. 1.12.

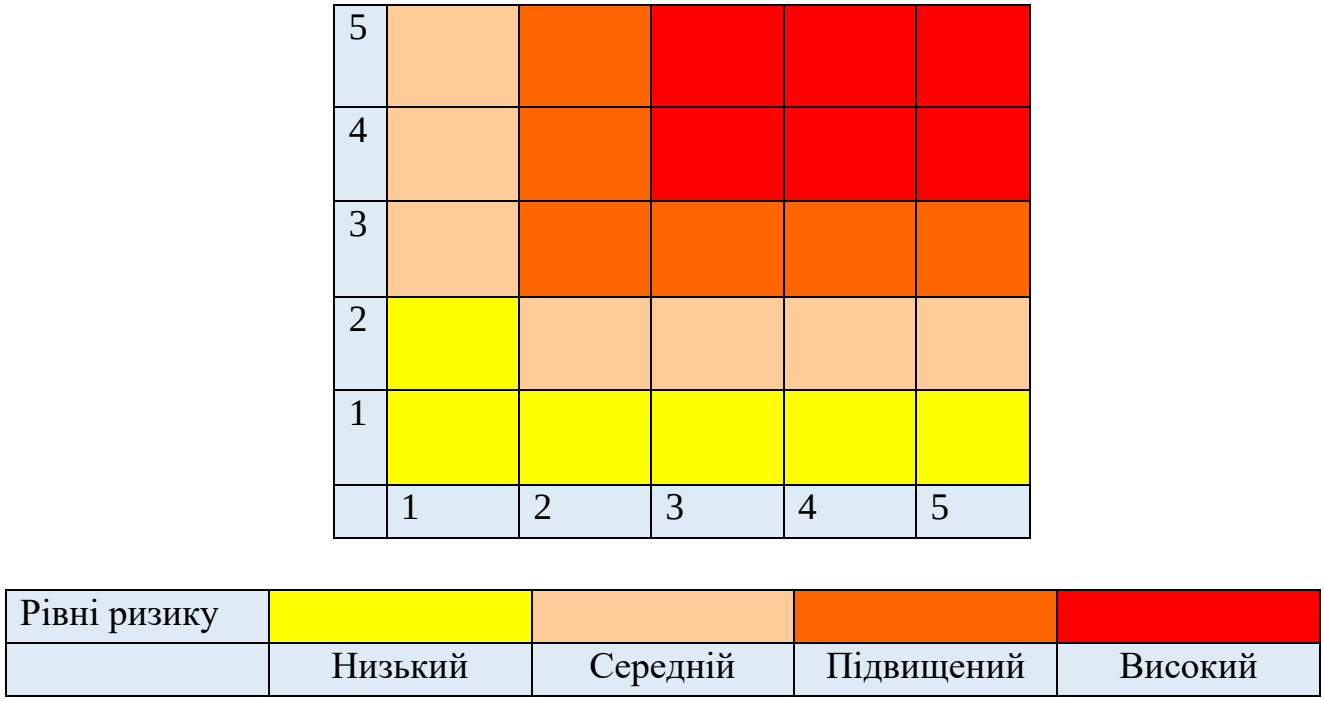


Рис. 1.12. Матриця ризиків на критично важливих об’єктах

Оцінка ризиків має здійснюватися на основі трьох різних категорій впливу, враховуючи негативні наслідки для людей (населення), економіки (та довкілля), а також політичні та соціальні наслідки. Для перших двох категорій наслідки оцінюються кількісно — як кількість загиблих (травмованих) осіб або економічні збитки в гривнях (євро). Для третьої категорії, що стосується соціальних та політичних аспектів, наслідки визначаються через якісні показники.

У Європейському Союзі кожна країна повинна проводити оцінку ризиків для кожної з цих категорій та створювати три окремі матриці ризику при оцінці ризиків для критичної інфраструктури.

Розуміння каскадних ефектів сучасних загроз є доволі складним через взаємозв’язок між інфраструктурними об'єктами та навколишнім середовищем. Нездатність зацікавлених сторін і політичного керівництва дійти згоди щодо прогно-

зування та зменшення негативних наслідків нових загроз, особливо природного походження, може призвести до серйозних збоїв у функціонуванні критичної інфраструктури в найближчому майбутньому.

У загальному випадку управління ризиками та їх часткове зниження передбачає застосування різних стратегій: уникнення ризику через припинення або відмову від діяльності, що його викликає; прийняття ризику для використання можливостей; усунення джерела ризику; зміна ймовірності виникнення ризику; коригування наслідків; розподіл ризику з іншими сторонами шляхом укладання контрактів чи фінансування; підтримання існуючого рівня ризику за погодженим рішенням.

У випадку складних взаємозв'язків і впливу основних факторів загроз природного і техногенного походження, ефективне зниження ризику економічних збитків вимагатиме комбінованого підходу, що включає кілька з цих стратегій, які можуть бути реалізовані на основі експертних оцінок. Зокрема, особливу увагу слід приділити розподілу ризику з іншими сторонами через укладання контрактів чи фінансування ризиків, що є новим і перспективним напрямком для нашої країни.

При цьому важливо враховувати, що матриця ризику для оцінки економічних збитків і впливу на довкілля в умовах надзвичайних ситуацій на регіональному рівні може відрізнятися від загального підходу. У техногенно навантажених регіонах України вплив природних загроз може бути посилений через фактори техногенного характеру, такі як пожежі, вибухи та інциденти на об'єктах критичної інфраструктури.

Основою для розробки нормативно-правових актів і програм у сфері захисту критичної інфраструктури є схвалення Кабінетом Міністрів України Концепції створення державної системи захисту критичної інфраструктури, розробленої Національним інститутом стратегічних досліджень. Важливим етапом є підготовка і подання до Верховної Ради України проекту Закону «Про захист критичної інфраструктури», який має врегулювати всі аспекти створення цієї системи, вклю-

чаючи визначення відповідального органу за координацію захисту критичної інфраструктури.

Серед пріоритетів — визначення функцій і повноважень центральних органів виконавчої влади у сфері захисту критичної інфраструктури, прав, обов'язків і відповідальності власників та операторів об'єктів, а також встановлення критеріїв для віднесення об'єктів до критичної інфраструктури, їх паспортизація та категоризація. Особливу увагу слід приділити формуванню критеріїв для віднесення об'єктів, зокрема потенційно небезпечних, до критичної інфраструктури, оцінці загроз, розробці планів забезпечення стійкості функціонування інфраструктури та створенню загальнодержавної системи взаємодії відповідно до компетенції відповідних міністерств.

1.4. Оцінка сучасного стану захищеності критично важливих об'єктів

Оцінка сучасного стану захищеності критично важливих об'єктів є ключовою частиною управління ризиками та забезпечення національної безпеки. Це процес, що включає в себе аналіз захищеності об'єктів, які мають критичне значення для функціонування суспільства і економіки.

Відповідно до затвердженого нею Порядку проведення моніторингу здійснюється шляхом проведення один раз на три роки оцінки стану захищеності об'єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури відповідно до їх повноважень, визначених Законом України «Про критичну інфраструктуру».

Критична інфраструктура сучасної держави являє собою складний комплекс різноманітних елементів, що включають організаційні структури, управлінські моделі, а також взаємозалежні функції і системи як у фізичному, так і у віртуальному середовищах. Управління критичною інфраструктурою здійснюється державними структурами на всіх рівнях, які мають різні сфери відповідальності та повноваження, а також власниками та операторами об'єктів і систем, що складають критичну інфраструктуру. У умовах глобалізації безпека національних інтересів,

виробництва, економіки і фінансів кожної країни значно залежить від чинників, що впливають на безпеку в інших країнах і на глобальному рівні.

Сьогодні відбувається формування нової концепції забезпечення безпеки, яка базується на спільних зусиллях громадян, суспільства, бізнесу і держави. Розвивається "культура управління ризиками", яка повинна стати основою політики захисту критичної інфраструктури і включає елементи, які представлені на Рис.1.13:

Рис. 1.13 елементи політики захисту критичної інфраструктури

Ці фактори визначають першу стратегічну мету політики захисту критичної інфраструктури: створення безпекового партнерства для підвищення безпеки та стійкості національної критичної інфраструктури.

У більшості країн світу, зокрема в Україні з урахуванням економічних реформ, об'єкти критичної інфраструктури здебільшого перебувають у приватній власності. Саме приватні оператори володіють більшістю таких об'єктів та лідирують у розробці новітніх технологій і технологій їх захисту.

У розвинених країнах основна відповідальність за безпеку об'єктів і систем критичної інфраструктури покладається на їх власників і операторів, які мають забезпечувати їх надійність і стійкість. Держава, в свою чергу, повинна забезпечувати адекватне інформування, створення належної нормативно-правової бази і стимулів для інвестування в безпеку критичної інфраструктури, а також умови для підтримання конкурентоспроможності бізнесу, який інвестує у захист цієї інфраструктури.

Ефективне державно-приватне партнерство є ключовим для підтримки високого рівня безпеки і стійкості критичної інфраструктури. У США та Німеччині акцент робиться на формуванні довіри між партнерами і створенні стимулів для співпраці.

Політика повинна сприяти як приватним власникам, так і державним органам у створенні системи захисту критичної інфраструктури, здатної протидіяти надзвичайним ситуаціям, знижувати ризики та наслідки. Обов’язковим є також створення стимулів для інвестицій у безпеку критичної інфраструктури та умов для підтримки конкурентоспроможності бізнесу.

Механізм державно-приватного партнерства допомагає стимулювати інвестиції в захист критичної інфраструктури шляхом адекватного інформування бізнесу про загрози і ризики, при цьому враховуючи, що витрати на безпеку не повинні підривати конкурентоспроможність і здатність надавати важливі послуги.

Що стосується України, до 2014 року державно-приватне партнерство регулювалося переважно в економічній сфері відповідно до Закону України «Про державно-приватне партнерство» від 01.07.2010 № 2404-VI, який не охоплював захист критичної інфраструктури. Однак події 2014-2015 років показали важливість залучення громадськості до захисту національних інтересів і критичної інфраструктури.

Україні необхідно розробити законодавчі рішення для регулювання державно-приватного партнерства в захисті критичної інфраструктури, створити нормативно-правову базу для врегулювання взаємних зобов'язань держави та приватно-

го сектору, впровадити практики аналізу ризиків та реагування на загрози, а також механізми взаємодії і узгодження дій.

Підвищення надійності і стійкості об'єктів вимагатиме додаткових фінансових витрат від операторів, що може призвести до зростання цін на послуги та товари. Це має бути враховано при визначенні об'єктів критичної інфраструктури та встановленні вимог до їх захисту. Ініціативи з підвищення захисту повинні бути зваженими і враховувати соціально-економічні аспекти, а також можливість перегляду тарифів на послуги.

Обмін інформацією є важливим інструментом для формування довіри між державними і приватними партнерами. Тому друга стратегічна мета політики щодо критичної інфраструктури полягає у налагодженні обміну інформацією, включаючи збір, аналіз та усвідомлення інформації про загрози і ризики, вразливості систем та механізми реагування.

Елементи критичної інфраструктури мають складні вертикальні та горизонтальні взаємозв'язки, що може призвести до каскадних і віддалених наслідків від відмови окремих елементів. Основна відповідальність за безпеку лежить на операторах, однак державні органи повинні мати детальну інформацію і співпрацю з приватним сектором. Важливим є створення нормативно-правової бази для обміну інформацією, що стосується безпеки критичної інфраструктури, і забезпечення захисту чутливої інформації від можливого зловживання.

Незважаючи на критичну важливість заходів з підвищення рівня захищеності та стійкості критичної інфраструктури, їх планування у будь-якій країні здійснюється у рамках бюджетних і ресурсних обмежень. У звязку з цим ще однією стратегічною ціллю політики у цій сфері має бути максимально ефективне використання ресурсів для захисту критичної інфраструктури.

Розбудоване партнерство як на національному, так і на міжнародному рівнях, координація дій та обмін інформацією між партнерами створюють передумови для досягнення такої цілі, в результаті чого виключаються дублювання функцій, а також розпорошення ресурсів серед окремих суб‘єктів процесу забезпечен-

ня захисту критичної інфраструктури. З огляду на важкі соціально-політичні та фінансово-економічні умови, в яких наразі перебуває Україна, встановлення такої цілі є особливо актуальним.

Україна має забезпечити формування загальнодержавної системи оцінки ризиків та загроз критичній інфраструктурі, належну координацію органів державної влади та узгодження дій різних залучених осіб, що потребуватиме визначення відповідального державного органу та надання йому відповідних повноважень. Очевидно, що стратегічні цілі державної політики України в сфері захисту критичної інфраструктури мають бути зафіксовані у вітчизняному законодавстві [9].

Що стосується спектру загроз критичній інфраструктурі в Україні, то його особливості в основному визначаються специфікою безпекової ситуації в країні. Бойові дії посилюють ризики для критичної інфраструктури, яка і до нинішньої кризи вже страждала від значного зношення основних фондів, проблем з екологічною та техногенною безпекою.

Це призводить до підвищення ймовірності аварій на об'єктах підвищеного ризику, таких як шахти, об'єкти енергетики, хімічні та металургійні підприємства, а також в системах життєзабезпечення. Загрози можуть виникати як через випадкові пошкодження або втрату контролю над технологічними процесами, так і внаслідок терористичних актів і диверсій.

1. Дослідження ступеня впровадження концепції захисту критичної інфраструктури у провідних країнах світу свідчить, що на сьогодні концепція критичної інфраструктури є дієвим інструментом, який використовується і в міжнародній, і в національних системах безпеки для захисту найбільш важливих систем, об’єктів і ресурсів.

Україна підтвердила свій євроінтеграційний вибір, і це передбачає, зокрема, її наближення до підходів ЄС у безпековій сфері. Також треба зважати на процеси реформування державного апарату в Україні, що закладають сприятливі організаційно-управлінські підвалини для запровадження концепції захисту критичної інфраструктури в нашій країні.

Зважаючи на це, упровадження в Україні концепції захисту критичної інфраструктури стане важливим кроком до вдосконалення існуючих державних систем та інституцій у сфері безпеки [10].

2. Заходи з захисту критично важливих об'єктів, систем та ресурсів в Україні реалізуються різними відомствами в межах їхніх завдань і повноважень, проте мають фрагментарний характер. Це призводить до паралельного функціонування систем, які призначені для захисту від різних типів загроз (техногенних, природних або соціально-політичних).

Серед таких систем є Єдина державна система запобігання та реагування на надзвичайні ситуації техногенного та природного характеру, Єдина державна система цивільного захисту населення та територій, а також Єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків. Наявність цих паралельних систем створює ризик бюрократизації проблеми і неефективного використання ресурсів на національному рівні.

3. Категоризація критично важливих об'єктів та елементів критичної інфраструктури України проводиться на основі галузевих (відомчих) підходів, враховуючи різні аспекти забезпечення національної безпеки (економічної, державної, політичної, енергетичної, екологічної, гуманітарної тощо).

Це призводить до різних визначень таких об'єктів, зокрема: підприємства, що мають стратегічне значення для економіки та безпеки держави; важливі державні об'єкти; об'єкти, що підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період; потенційно небезпечні та об'єкти підвищеної небезпеки; особливо важливі об'єкти електроенергетики, нафтогазової галузі; нерухомі пам'ятки культурної спадщини.

4. Хоча в становленні системи захисту національної безпеки України досягнуто значних успіхів, існує ряд труднощів і проблем у сфері захисту критичної інфраструктури, які потребують вирішення:

1.	Неузгодженість національної нормативно-правової бази з міжнародними стандартами, особливо в сфері захисту критично важливих об'єктів і інфраструктури, на тлі декларування євроінтеграційного курсу.
2.	Обмежені можливості обміну інформацією та недостатність інформаційного забезпечення щодо загроз для об'єктів критичної інфраструктури, а також відсутність міжвідомчого управління та інвентаризації ресурсів для попередження техногенних і природних загроз, які потребують покращення забезпечення інженерними засобами, обладнанням, технікою, інформаційними та кадровими ресурсами.
3.	Наявність прогалин у нормативних документах, відсутність вимог, методологій для оцінки загроз критичним об'єктам держави, а також загальної методології оцінки ризиків для критично важливих об'єктів, незважаючи на їхню тісну взаємозалежність, що може призвести до аварій.
4.	Відсутність ефективної практики державно-приватного партнерства в сфері безпеки, що потребує вдосконалення організаційних і правових основ такого партнерства.
5.	Міждисциплінарний характер завдань захисту критичної інфраструктури, які вимагають комплексних наукових досліджень та значних фінансових інвестицій через їхню складність.

Рис. 1.14 Проблеми у сфері захисту критичної інфраструктури

5. Сьогодні інформаційні та телекомунікаційні мережі є одними з основних і найуразливіших елементів критичної інфраструктури. Проте, впровадження концепції захисту критичної інфраструктури повинно охоплювати не лише захист від кіберзагроз, а й включати інші аспекти безпеки. Отже, проблема захисту критичної інфраструктури має більший вимір – вимір культури безпеки, культури сприйняття ризиків, культури управління останніми. Це перехід від старої радянської культури безпеки до сучасної, орієнтованої на захист людини, суспільства й держави [10].

2. АРХІТЕКТУРА СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО ЗАХИСТУ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ

2.1. Основні компоненти інтелектуального захисту критичних об'єктів

Захист критично важливих об'єктів, таких як енергетична інфраструктура, транспортні системи, фінансові установи та інші стратегічні об'єкти, є ключовим аспектом забезпечення національної безпеки. Інтелектуальний захист цих об'єктів стає все більш актуальним в умовах швидкого розвитку технологій і зростання кількості загроз. Основні компоненти інтелектуального захисту включають сенсори та системи моніторингу, аналітику та управління даними, механізми реагування на загрози, а також інтеграційні та комунікаційні системи.

Рис. 2.1 Основні компоненти інтелектуального захисту

1. Сенсори та системи моніторингу є першою лінією оборони у системі інтелектуального захисту критично важливих об'єктів. Системи моніторингу забезпечують безперервний нагляд за критично важливими об'єктами, передаючи інформацію до центрів управління для подальшого аналізу. Вони призначені для збору даних про стан об'єктів та їх оточення. До основних типів сенсорів відносяться: Фізичні сенсори, які вимірюють фізичні параметри, такі як температура, вологість, тиск, вібрація тощо. Оптичні сенсори, які використовуються для відеоспостереження, розпізнавання облич і реєстрації змін у навколишньому середовищі та кібер-сенсори, які збирають дані про мережевий трафік, виявляють аномалії та можливі кібератаки.

2. Аналітика та управління даними є критично важливою складовою інтелектуального захисту, оскільки вона дозволяє перетворювати величезні обсяги

даних, зібраних сенсорами, у корисну інформацію. Основні компоненти аналітики включають: Машинне навчання, яке використовується для виявлення патернів та аномалій у даних. Наприклад, алгоритми можуть навчатися на історичних даних для прогнозування можливих загроз. **Штучний інтелект:** Системи штучного інтелекту можуть автоматично реагувати на виявлені загрози, приймаючи рішення без участі людини та використовується аналіз великих даних, тобто технології обробки великих даних дозволяють обробляти та аналізувати інформацію з різних джерел, забезпечуючи комплексне розуміння ситуації.

3. Механізми реагування на загрози є основними для оперативного реагування на виявлені загрози та інциденти. Вони включають:

Автоматичне реагування: Системи автоматичного реагування можуть здійснювати дії у відповідь на виявлені загрози без втручання людини, наприклад, блокування мережевого трафіку або активація протипожежних систем.

Реакція в реальному часі: Якщо виникла критична ситуація, системи повинні забезпечити швидке реагування, координуючи дії з різними службами та підрозділами.

Планування та управління інцидентами: Розробка планів реагування на інциденти та управління ними є необхідною для ефективного реагування в умовах кризової ситуації.

4. Інтеграційні та комунікаційні системи. Для забезпечення ефективного захисту критично важливих об'єктів необхідна інтеграція різних компонентів системи в єдину архітектуру. Основні компоненти включають: інтеграційні платформи, які забезпечують зв'язок між різними системами та компонентами захисту, дозволяючи їм працювати як єдине ціле та комунікаційні системи, які Використовуються для передачі даних і команд між компонентами системи, забезпечуючи оперативний обмін інформацією та координацію дій.

2.2. Схема архітектури системи інтелектуального захисту критично важливих об’єктів

Схема архітектури системи інтелектуального захисту критично важливих об'єктів забезпечує комплексний підхід до управління безпекою. Кожен компонент системи відіграє ключову роль у забезпеченні ефективного захисту від різних загроз. Правильна інтеграція та координація між компонентами є критично важливою для досягнення максимальної ефективності системи захисту.

Система інтелектуального захисту критично важливих об'єктів складається з кількох основних компонентів, які забезпечують комплексний підхід до захисту.

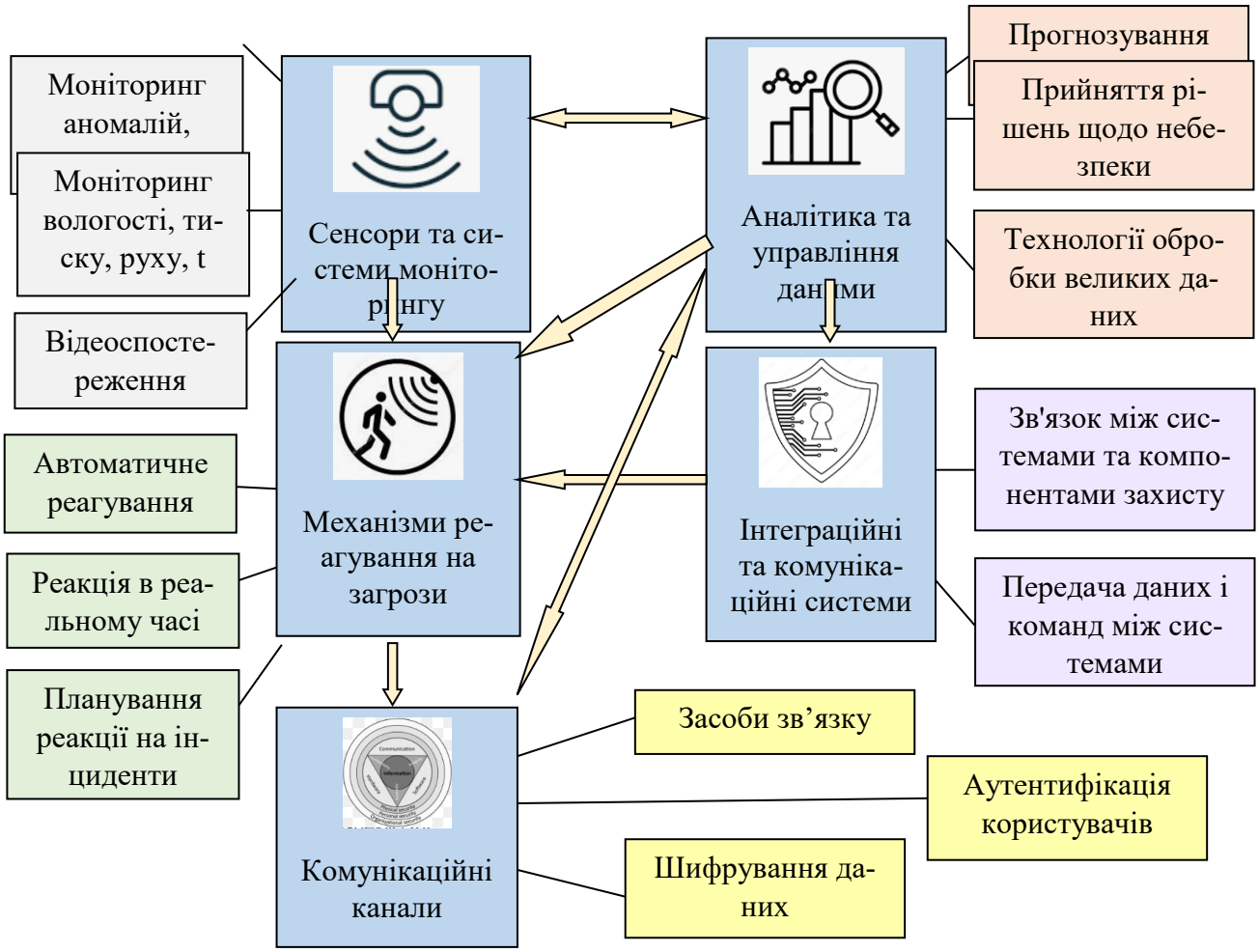


Рис. 2.2. Схема архітектури системи інтелектуального захисту критично важливих об'єктів

Зв'язки між Компонентами системи інтелектуального захисту критично важливих об’єктів:

1. **Зв'язок між сенсорами і аналітикою**. Сенсори збирають дані про стан об'єктів і навколишнє середовище. Ці дані передаються до аналітичних систем для подальшої обробки. Аналітика використовує дані для виявлення аномалій, загроз і патернів, що дозволяє вчасно реагувати на можливі інциденти.

2. **Зв'язок між аналітикою і механізмами реагування**. Після аналізу даних, виявлені загрози або аномалії передаються до систем реагування. Аналітичні системи формують рекомендації для механізмів реагування або автоматично ініціюють дії, наприклад, блокування небажаного мережевого трафіку або активацію системи пожежогасіння.

3. **Зв'язок між механізмами реагування і інтеграційними платформами**. Механізми реагування підключаються до інтеграційних платформ для координації дій між різними компонентами системи. Інтеграційні платформи забезпечують, щоб інформація про загрози і дії реагування передавалася всім необхідним елементам системи.

4. **Зв'язок між комунікаційними системами і аналітикою**. Комунікаційні системи забезпечують зв'язок між аналітичними платформами та зовнішніми агентами (службами екстреної допомоги, управлінськими органами). Це дозволяє оперативно передавати інформацію про загрози і стан реагування.

5. **Зв'язок між інтеграційними платформами та сенсорами**. Інтеграційні платформи обробляють дані, отримані від сенсорів, і забезпечують їх інтеграцію з іншими компонентами системи. Це дозволяє забезпечити єдиний центр управління для моніторингу та реагування.

Комунікаційні канали включають електронну пошту, мобільні повідомлення, радіозв'язок для передачі важливих інформаційних потоків. Протоколи Безпеки: Шифрування даних, аутентифікація користувачів і захист від несанкціонованого доступу.

2.3 Інтеграція системи інтелектуального захисту критично важливих об'єктів з існуючими системами захисту

Кіберзагрози, природні катастрофи та техногенні аварії представляють серйозні виклики для забезпечення національної безпеки. Системи захисту повинні бути не тільки потужними, але й гнучкими, здатними адаптуватися до нових загроз. Інтеграція інтелектуальних систем захисту з існуючими структурами є ключовим аспектом для підвищення ефективності безпеки. Системи інтелектуального захисту використовують передові технології для проактивного моніторингу та реагування на загрози. Ключові компоненти таких систем включають:

Таблиця 2.1 – Компоненти технології інтелектуального захисту

Компоненти технології інтелектуального захисту	
Назва компоненти	**Призначення компоненти**
Штучний інтелект	Використовується для аналізу великих обсягів даних і виявлення аномалій, що можуть свідчити про загрози.
Аналіз великих даних (Big Data)	Дозволяє обробляти та аналізувати дані з різних джерел, забезпечуючи детальне розуміння ситуації.
Машинне навчання	Застосовується для прогнозування потенційних загроз на основі історичних даних та трендів.
Інтернет речей (IoT)	Забезпечує інтеграцію фізичних пристроїв в єдину мережу для збору даних та моніторингу.

Традиційні системи безпеки стикаються з обмеженнями, такими як людський фактор, повільна швидкість обробки та недостатня ефективність при аналізі великих обсягів даних. У цьому контексті штучний інтелект може забезпечити швидкість реагування та ефективність у запобіганні втручаннях у роботу систем критичної інфраструктури. Перевагою рішень для систем захисту зі штучним інтелектом є:

- автоматизація процесів моніторингу та виявлення загроз. Виключення людського фактору, здатність ШІ-алгоритмів постійно відстежувати та сканувати

систему в реальному часі на предмет потенційних порушень безпеки та аномальних подій системи;

- постійний аналіз і навчання на минулих інцидентах. Здатність ШІ до машинного навчання, дозволяють системі вдосконалювати свої алгоритми і адаптувати їх до реагування на нові загрози. Можливість самонавчання дозволяє системі виявляти ризики та нівелювати їх до того, як вони переростуть у повномасштабні загрози;

- інтегрування з іншими системами безпеки. Створення єдиної системи безпеки на основі ШІ забезпечить швидкий обмін даними та взаємодію.

Не дивлячись на переваги впровадження систем зі штучним інтелектом є певні проблеми, однією з яких є конфіденційність. ШІ збирає і обробляє величезні обсяги даних, деколи і приватного характеру. Баланс між безпекою і конфіденційністю впливає на впровадження таких систем [11]. Розгортання систем, що базуються на штучному інтелекті, вимагає значних інфраструктурних та фінансових витрат. Навчання і підтримка алгоритмів ШІ потребують висококваліфікованого персоналу, що додатково збільшує витрати. Синергія штучного інтелекту з новими технологіями, такими як Інтернет речей (IoT) та мережі 5G, відкриває нові можливості для превентивного виявлення загроз і швидкого реагування на них. Сучасні загрози, такі як шифрувальники LockBit, значно скоротили час, необхідний для атаки на систему — тепер це може зайняти лише півгодини. Технології ШІ здатні збирати дані про атаки, класифікувати їх і підготовляти для аналізу. Спеціалісти з кібербезпеки використовують ШІ для створення звітів, що спрощують обробку даних та прийняття рішень. Крім того, система безпеки з інтегрованим ШІ може генерувати рекомендації щодо дій для обмеження і запобігання подальшим атакам. Роль ШІ в захисті критично важливих об'єктів полягає у виявленні закономірностей за допомогою алгоритмів машинного навчання. Сучасний ШІ ще не досягає рівня, подібного до людського, ця область активно розвивається, і постійно з'являються нові та вдосконалені алгоритми.

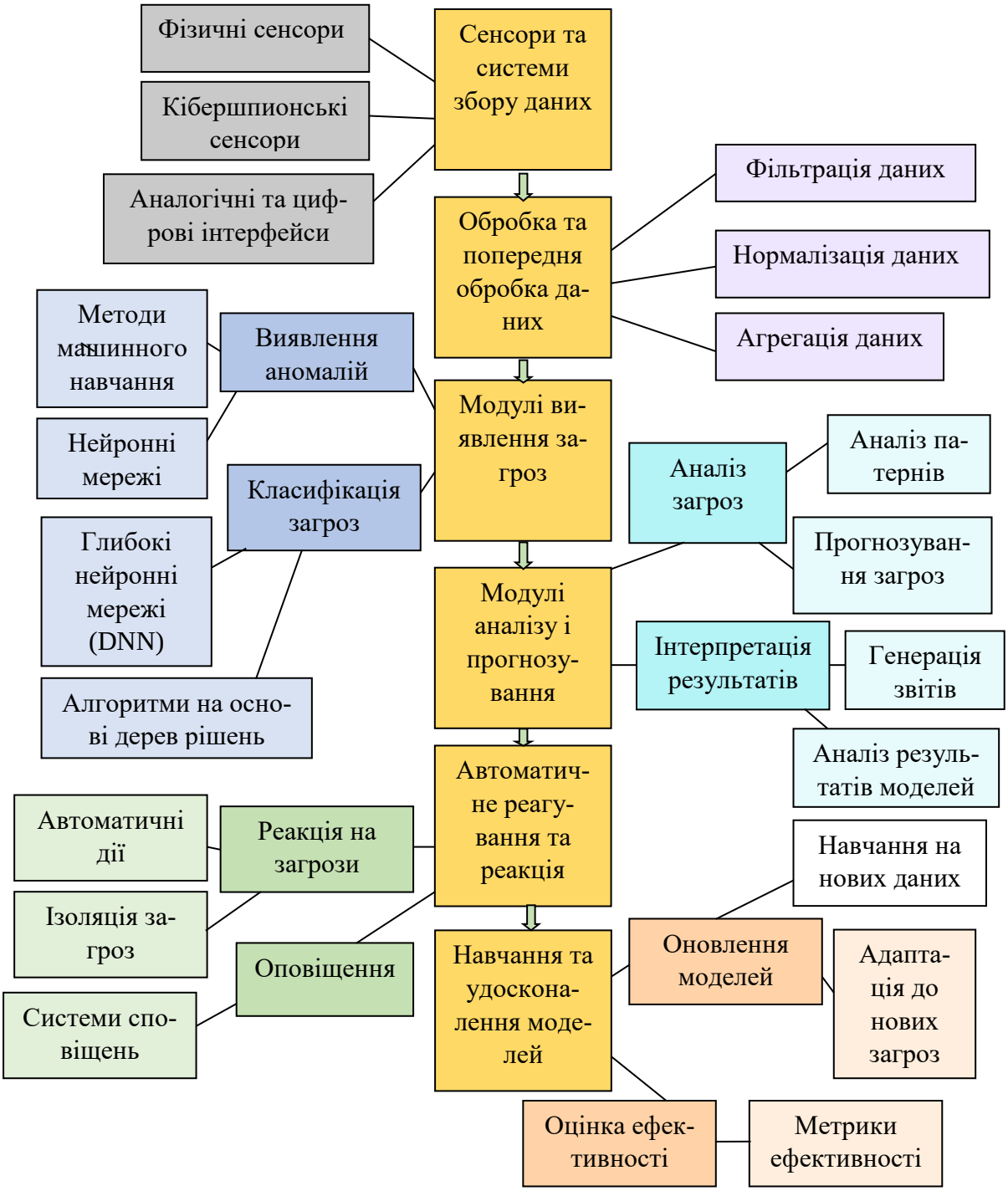


Рис. 2.3 Архітектура системи штучного інтелекту для захисту критично важливих об’єктів

Архітектура системи штучного інтелекту (ШІ) для захисту критичної інфраструктури включає кілька ключових компонентів, які працюють разом для забезпечення всебічного захисту. Ця архітектура забезпечує інтегрований підхід до захисту критичної інфраструктури, використовуючи штучний інтелект для автоматизації та підвищення ефективності системи безпеки.

1. Сенсори та системи збору даних

- Фізичні сенсори: Вимірюють різні параметри навколишнього середовища, такі як температура, вологість, тиск, рівень шуму.
- Кібершпионські сенсори: Збирають дані про мережевий трафік, активність користувачів, доступ до системи та інші кібер-параметри. Кібершпіонські сенсори є критично важливими для забезпечення кібербезпеки, оскільки вони допомагають моніторити, виявляти і реагувати на кіберзагрози в реальному часі. На Рис.2.4-2.9 наведено кілька прикладів таких сенсорів, які використовуються для захисту критичної інфраструктури:
- Мережеві інспектори

Рис. 2.4 Мережеві інспектори

Програмні та апаратні рішення для моніторингу мережевого трафіку:

Wireshark: Відомий інструмент для аналізу мережевого трафіку, який дозволяє переглядати та інтерпретувати пакети даних.

Snort: Інструмент для виявлення та запобігання вторгненням (IDS/IPS), який аналізує мережевий трафік на предмет аномалій і атак.

Системи виявлення інтрузій (IDS):

Рис. 2.5 Системи виявлення інтрузій (IDS)

Системи, що виявляють несанкціоновану активність у мережі або на окремих пристроях:

Suricata: Система IDS/IPS, яка може аналізувати мережевий трафік, виявляти загрози та блокувати атаки.

OSSEC: Інструмент для виявлення інтрузій, що аналізує журнали та події з різних джерел для виявлення аномалій.

Системи виявлення аномалій (ADS):

Рис. 2.6 Системи виявлення аномалій (ADS)

Алгоритми і системи, що використовують статистичні та машинно-навчальні підходи для виявлення відхилень від нормальної поведінки:

Darktrace: Платформа на основі штучного інтелекту, яка використовує методи машинного навчання для виявлення аномалій у мережевій активності.

Vectra AI: Використовує штучний інтелект для виявлення аномалій і загроз в мережевому трафіку та поведінці користувачів.

Системи аналізу журналів (SIEM):

Рис. 2.7 Системи аналізу журналів (SIEM)

Системи для централізованого збору, зберігання та аналізу журналів подій з різних джерел:

Splunk: Платформа для аналізу даних, що може збирати, індексувати і візуалізувати журнали для виявлення потенційних загроз.

Elastic Stack (ELK): Комбінація Elasticsearch, Logstash та Kibana для збору, обробки та візуалізації журналів подій.

Контролери доступу до мережі (NAC):

Рис. 2.8 Контролери доступу до мережі (NAC)

Системи для контролю і управління доступом до корпоративної мережі:

Cisco Identity Services Engine (ISE): Система для управління доступом до мережі, яка перевіряє пристрої перед наданням доступу.

Aruba ClearPass: Платформа для контролю доступу, яка забезпечує аутентифікацію і авторизацію користувачів і пристроїв.

Аналізатори поведінки кінцевих точок (EDR):

Рис. 2.9 Аналізатори поведінки кінцевих точок (EDR)

Інструменти для моніторингу і аналізу активності на кінцевих точках:

SentinelOne: Платформа EDR, яка використовує штучний інтелект для виявлення і реагування на загрози на кінцевих точках.

Sophos Intercept X: Інструмент EDR для виявлення і запобігання загрозам на кінцевих пристроях, включаючи шкідливі програми і експлойти.

- Аналогічні та цифрові інтерфейси: Інтегрують дані з різних джерел для обробки та зберігання.

2. Обробка та попередня обробка даних

Фільтрація даних: Видалення шуму та непотрібної інформації.

Шумом є неправдиві, випадкові або незначні дані, які можуть виникати через помилки вимірювань, збій у сенсорах, помилки запису або сторонні впливи. Типи шуму: Псевдо-шум, систематичні помилки, випадкові аномалії. Непотрібною інформацією є дані, які не мають прямого відношення до задачі, що вирішується, наприклад, зайві атрибути, які не впливають на результати або прийняття рішень.

Існують методи фільтрації даних:

Фільтрація шуму:

А) Згладжування (Smoothing): Методи, які згладжують дані для зменшення впливу випадкових коливань:

- Мувінг-аверидж (Moving Average): Розрахунок середнього значення даних в заданому вікні для згладжування.
- Гаусівське згладжування (Gaussian Smoothing): Використання гаусівського фільтра для згладжування даних.

Б) Фільтри Калмана (Kalman Filters): Алгоритми, які використовують прогнозування і корекцію для відокремлення шуму від корисних сигналів у динамічних системах.

В)Методи статистичного очищення: Виявлення і видалення аномальних значень, що відрізняються від загального тренду або середнього значення.

Видалення Непотрібної Інформації

А) Методи вибору ознак (Feature Selection): Техніки, які вибирають найважливіші ознаки для моделі, усуваючи ті, що не впливають на результат.

- Методи на основі кореляції: Вибір ознак на основі їх кореляції з цільовою змінною.
- Методи на основі важливості ознак: Використання алгоритмів, таких як дерева рішень або Random Forest, для оцінки важливості ознак.

Б) Методи зменшення розмірності (Dimensionality Reduction): Техніки, які зменшують кількість ознак, зберігаючи найбільш важливу інформацію.

- Аналіз головних компонент (PCA): Метод, який трансформує дані в новий простір з меншою кількістю вимірювань.
- t-SNE (t-Distributed Stochastic Neighbor Embedding): Метод, який зменшує розмірність даних, зберігаючи структуру сусідства.

В) Імпутація пропущених значень (Imputation): Заповнення пропущених даних на основі статистичних методів або моделей.

- Середнє або медіанне імпутування: Заповнення пропущених значень середнім або медіанним значенням.
- Імпутування на основі сусідніх значень: Використання значень сусідніх записів або аналогічних характеристик для заповнення пропущених даних.

Нормалізація даних: Перетворення даних в уніфікований формат для полегшення аналізу.

Агрегація даних: Об'єднання даних з різних джерел для отримання більш повної картини.

3. Модулі виявлення загроз

- Виявлення аномалій:
  - Методи машинного навчання: Наприклад, алгоритми кластеризації (K-means, DBSCAN), моделі виявлення аномалій (Isolation Forest, One-Class SVM).
  - Нейронні мережі: Автокодери для виявлення відхилень від норми.

Алгоритм K-means є одним з найбільш популярних методів кластеризації в машинному навчанні. Він розподіляє дані на KKK кластерів на основі схожості, де дані в одному кластері мають високий ступінь подібності між собою, а дані в різних кластерах мають менший ступінь подібності.

На Рис.2.10 представлено алгоритм застосування K-means для захисту критичної інфраструктури.

Рис. 2.10 Алгоритм застосування K-means для захисту критичної інфраструктури

Далі наведено опис алгоритму алгоритму застосування K-means для захисту критичної інфраструктури.

1. Збір Даних

Джерелами даних є: сенсори, системи моніторингу, журнали подій, мережевий трафік, дані з систем безпеки.

2. Застосування алгоритму K-means

2.1. Визначення кількості кластерів. Спершу визначається оптимальна кількість кластерів за допомогою методів, таких як "лікоть" (Elbow Method), середньоквадратичні помилки або аналіз силуетів (Silhouette Analysis).

2.2. Ініціалізація Кластерів

Потім відбувається ініціалізація центроїдів кластерів випадковими точками в даних, потім відбувається вдосконалення методів, таких як K-means++ для покращення результатів.

2.3. Кластеризація

Потім відбувається процес присвоєння до кластерів: Розподіл кожного зразка даних до найближчого центроїду кластеру. Далі йде оновлення центроїдів: перерахунок центрів кластерів як середньоарифметичних значень всіх точок, що входять до відповідного кластера.

В кінці йде перевірка збіжності: Повторення процесу присвоєння до кластерів і оновлення центроїдів, поки зміни не стануть незначними.

3. Аналіз і використання результатів

Першим етеапом є виявлення аномалій. На цьому етапі відбувається аналіз кластерів: ідентифікація аномальних або підозрілих кластерів, які можуть вказувати на потенційні загрози або атаки.

Потім йде моделювання аномалій: використовуються дані з кластерів для навчання моделей виявлення аномалій або загроз.

Далі йде адаптація систем безпеки. Адаптація систем безпеки для зосередження уваги на нових типах загроз, виявлених в кластеризованих даних.

Потім відбувається оптимізація реагування: налаштування процедур реагування на основі типів і характеристик виявлених загроз.

Останнім етапом є візуалізація даних, тобто графічне відображення. Тут відбувається візуалізація кластерів для кращого розуміння розподілу даних і виявлення тенденцій або патернів.

- Класифікація загроз:
  - Глибокі нейронні мережі (DNN): Наприклад, CNN для класифікації типів загроз.

Згорткові мережі, CNN, є найпоширенішими архітектурами для обробки зображень та розпізнавання облич. Вони ефективно використовують згорткові шари для виявлення локальних характеристик зображення, таких як границі, текстури та форми, а також пулінгові шари для зменшення розмірності даних. Ці мережі можуть бути глибокими, що дозволяє їм автоматично вивчати складні залежності між різними рисами обличчя. Згорткові мережі показали вражаючі результати в задачах розпізнавання облич і стали стандартом для багатьох систем розпізнавання облич [12].

Принцип роботи згорткових нейромереж базується на використанні згорткових шарів (convolutional layers) та пулінгових шарів (pooling layers), які дозволяють ефективно витягати різні ознаки з вхідних даних (Рис. 2.11). Основна ідея полягає в тому, що згорткові шари виконують локальні згортки між вхідними даними і фільтрами, а пулінгові шари зменшують розмір отриманого представлення.

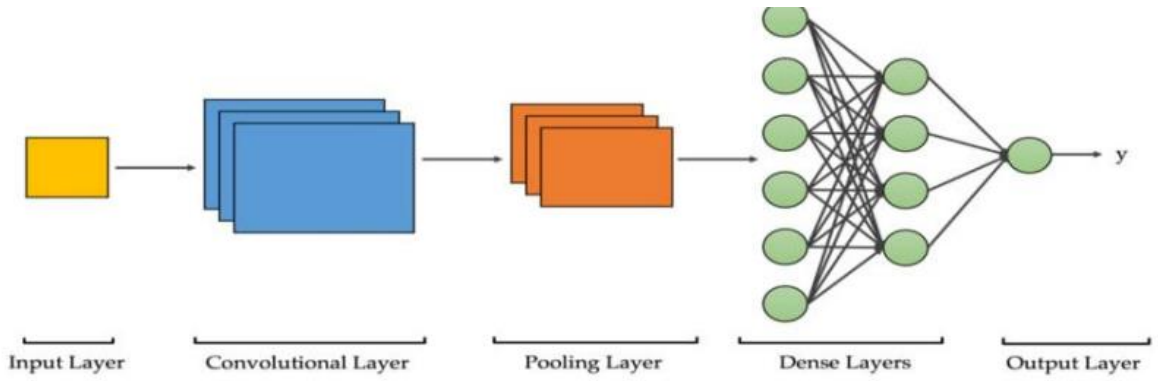


Рис. 2.11 Схема архітектури згорткової мережі

Модернізація звичайних згорткових нейронних мереж CNN може включати в себе різні підходи та техніки для поліпшення їх продуктивності та ефективності.

Основним методом модифікації є зміна архітектури CNN для роботи з більш специфічними даними або завданнями, це такі мережі як VGG, ResNet, Inception, MobileNet і багато інших.

Для роботи з тривимірними даними існує модифікована версія CNN, відома як 3D-CNN. 3D-CNN є модернізацією звичайних CNN або як їх іноді називають 2D-CNN, яка розширює можливості згорткових нейронних мереж для обробки тривимірних даних, таких як відео, медичні зображення та великі об'єми даних в тривимірних форматах.

Основні елементи такі як методи регуляризації, нормалізації, оптимізації, функції активації, механізм backpropagation залишаються, наявність слоїв згортки та пулінгу залишаються незмінними. Основні відмінності між 3D-CNN і 2D-CNN полягають у використанні тривимірних даних і фільтрів в 3D-CNN, а також в специфічній конфігурації їхніх архітектур [13].

- Алгоритми на основі дерев рішень: Random Forest, Gradient Boosting для класифікації загроз. Моделі машинного навчання, такі як Random Forest та Gradient Boosting, використовуються для класифікації загроз в різних областях, включаючи захист критичної інфраструктури.

Дерево рішень (Decision Tree) можна уявити як двійкове дерево, яке є відомим концептом в алгоритмах і структурах даних. Кожен вузол дерева відповідає за вхідну змінну і точку її розділення (для числових змінних). Листові вузли представляють собою вихідну змінну, що використовується для прогнозування загроз на критично важливих об’єктах. Для отримання прогнозів потрібно пройти через дерево до листового вузла і отримати значення класу. Дерева рішень швидко навчаються та роблять прогнози, демонструючи високу точність при вирішенні різних завдань і не вимагаючи складної підготовки даних.

Випадковий ліс (Random Forest) – дуже популярний та ефективний алгоритм машинного навчання [14]. Це вид ансамблевого алгоритму, який називається пакуванням (bagging). У ньому використовується той самий підхід, але для оцінки всіх статистичних моделей найчастіше використовуються дерева рішень.

Навчальні дані розбиваються на багато вибірок, для кожної з яких створюється модель. Коли потрібно зробити прогноз, його робить кожна модель, а потім прогнози усереднюють, щоб дати кращу оцінку вихідному значенню. В алгоритмі випадкового лісу для всіх вибірок з навчальних даних будуються дерева рішень.

При побудові дерев для створення кожного вузла вибираються випадкові ознаки. Окремо отримані моделі не дуже точні, але при їх об’єднанні якість прогнозування значно покращується. Якщо алгоритм з високою дисперсією, наприклад, дерева рішень, показує хороший результат на вхідних даних, то цей результат часто можна покращити, застосувавши пакування [15]. Схема алгоритму Random Forest представлена на Рис. Х. та описана нижче.

Вхідні дані: Набір даних з ознаками загроз.

Bootstrap Sampling: Випадкове створення підмножин даних для кожного дерева.

Tree 1, Tree 2, ..., Tree n: Кілька дерев рішень, що навчаються на різних підмножинах даних.

Voting (Majority): Голосування дерев для визначення фінального класу.

Результат: Класифікація загрози на основі голосування дерев.

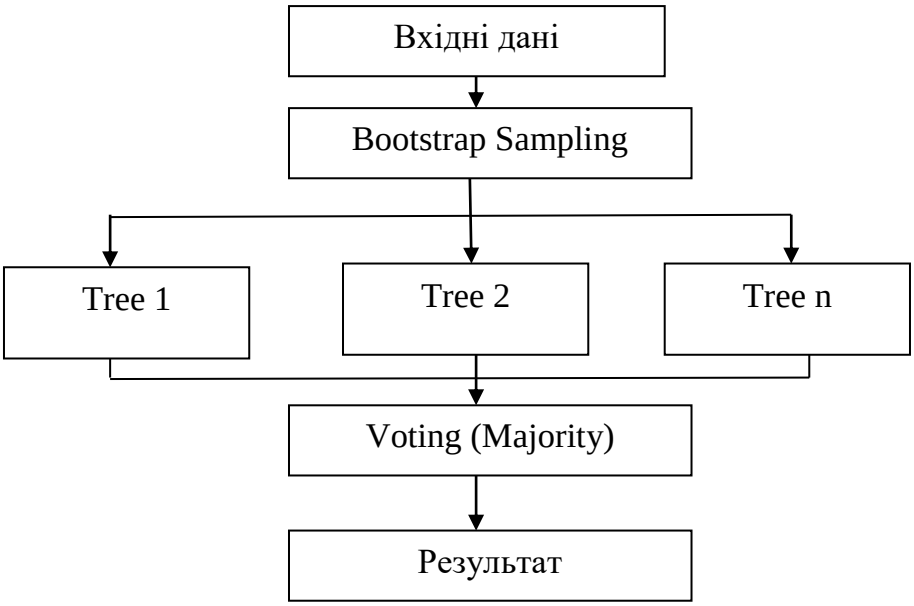


Рис. 2.12 Схема алгоритму Random Forest для класифікації загроз

4. Модулі аналізу і прогнозування

- Аналіз загроз: Аналіз патернів: Ідентифікація повторюваних шаблонів загроз та прогнозування загроз (Моделі прогнозування для визначення ймовірності майбутніх атак).
- Інтерпретація результатів:
  - Аналіз результатів моделей: Оцінка ймовірності загроз на основі отриманих даних.
  - Генерація звітів: Автоматичне створення звітів про стан безпеки.

На Рис. 2.13. представлена схема модулів аналізу і прогнозування. Ця схема ілюструє структуру та взаємозв'язки між різними модулями аналізу і прогнозування загроз, що забезпечують комплексний підхід до оцінки та управління ризиками в системах захисту критично важливих об'єктів. Аналіз і прогнозування загроз є ключовими аспектами системи інтелектуального захисту критично важливих об'єктів, спрямованими на підвищення ефективності забезпечення безпеки. У сучасному контексті, де ризики та загрози стають все більш складними і численними, традиційні методи захисту потребують інтеграції з передовими технологіями аналізу та прогнозування для адекватного реагування на потенційні атаки.

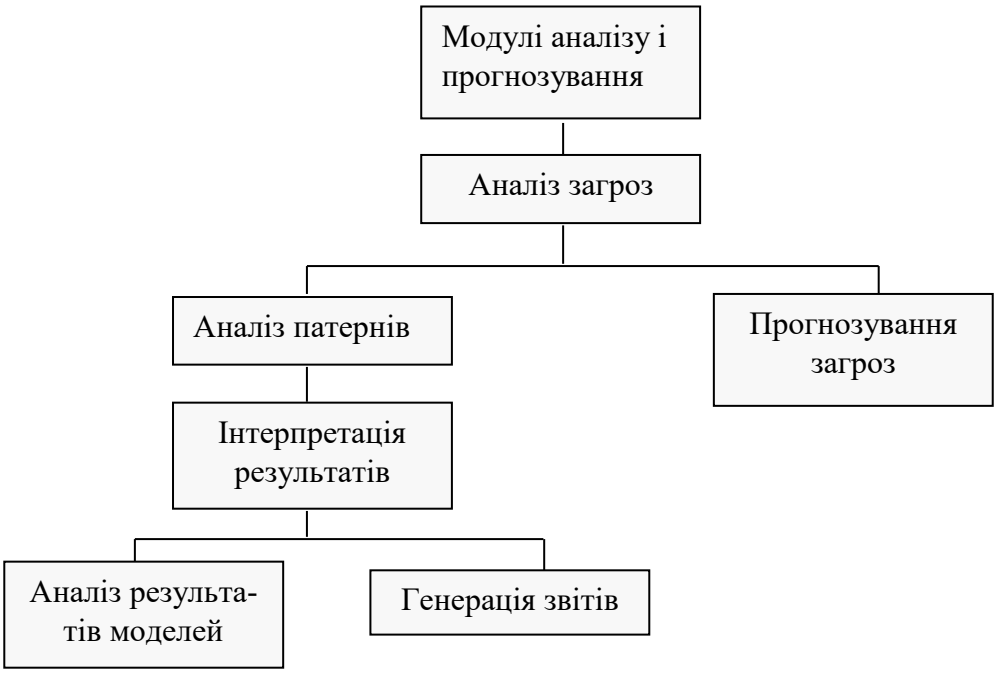


Рис. 2.13 Схема модулів аналізу і прогнозування

Модулі аналізу і прогнозування містить аналіз загроз, який включає в себе аналіз патернів та прогнозування загроз.

Аналіз патернів починається з ідентифікації повторюваних шаблонів загроз:

Збір даних: На цьому етапі збираються дані з різних джерел, таких як системи моніторингу, журнали подій, попередні інциденти та відгуки з систем кібербезпеки. Дані можуть включати інформацію про типи атак, їх джерела, час та місце виникнення, а також інші характеристики загроз.

Обробка даних: Зібрані дані очищаються та нормалізуються, щоб забезпечити однорідність і точність для подальшого аналізу. Це може включати видалення дублікатів, заповнення пропусків та перетворення даних у формат, зручний для аналізу.

Виявлення шаблонів: Використовуються алгоритми машинного навчання, такі як кластеризація або асоціативні правила, для виявлення повторюваних шаблонів у даних. Наприклад, алгоритм K-means може допомогти згрупувати схожі події для виявлення тенденцій.

Аналіз результатів: Визначаються типи загроз, які мають тенденцію до повторення. Це може допомогти у виявленні потенційних уразливих місць і покращенні реакції на загрози.

Прогнозування загроз – це модель прогнозування для визначення ймовірності майбутніх атак. Моделювання загроз містить в собі такі етапи:

Розробка моделей: Створюються та тренуються статистичні моделі та моделі машинного навчання, такі як регресія, дерева рішень, нейронні мережі або методи ансамблів, для прогнозування ймовірності майбутніх атак. Моделі використовують історичні дані про атаки та інші релевантні фактори.

Оцінка ризиків: Моделі прогнозування аналізують дані для оцінки ймовірності того, що певні види загроз можуть виникнути в майбутньому. Це включає в себе оцінку ймовірності атак, їх потенційного впливу і наслідків.

Аналіз і валідація: Результати прогнозування перевіряються на точність та надійність. Це може включати крос-валідацію і тести на нових даних для перевірки ефективності моделей.

Впровадження результатів: Прогнозовані загрози інтегруються в стратегії безпеки, що дозволяє проактивно вжити заходів для зменшення ризиків.

5. Автоматичне реагування та реакція

- Реакція на загрози:
  - Автоматичні дії: Наприклад, блокування доступу, відключення компонентів системи.
  - Ізоляція загроз: Відокремлення уражених частин системи для запобігання поширенню.
- Оповіщення:
  - Системи сповіщень: Автоматичні повідомлення адміністраторам про виявлені загрози та їх серйозність.

6. Навчання та удосконалення моделей

- Оновлення моделей:
  - Навчання на нових даних: Моделі постійно удосконалюються на основі нових даних і виявлених загроз.
  - Адаптація до нових загроз: Моделі адаптуються до нових типів атак та змін у поведінці загроз.
- Оцінка ефективності:
  - Метрики ефективності: Оцінка точності, відзиву та інших показників для поліпшення моделей.

Метрики ефективності є критично важливими для оцінки і вдосконалення моделей машинного навчання, особливо в контексті захисту критично важливих об'єктів. Вони дозволяють визначити, наскільки добре модель справляється з поставленими завданнями, і виявити області, що потребують поліпшення.

1. Точність (Accuracy). Точність визначає частку правильно класифікованих зразків серед усіх зразків. Вона є простою метрикою, яка обчислюється як відношення кількості правильних прогнозів до загальної кількості прогнозів.

$$\text{Точність} = \frac{\text{кількість правильних прогнозів}}{\text{загальна кількість прогнозів}} \quad (1)$$

Точність є корисною, коли дані збалансовані, тобто кількість зразків кожного класу приблизно однакова. Вона може бути менш корисною при значному дисбалансі класів.

2. Чутливість (або True Positive Rate). Чутливість вимірює здатність моделі правильно ідентифікувати позитивні зразки. Чутливість важлива у випадках, коли пропускання позитивних випадків має серйозні наслідки.

$$\text{Відклик} = \frac{\text{кількість правильно виявлених позитивних прогнозів}}{\text{кількість фактичних позитивних випадків}} \quad (2)$$

3. Прецизійність (Precision). Прецизійність вимірює точність позитивних прогнозів, тобто частку правильних позитивних прогнозів серед усіх передбачених позитивних випадків. Це критично важливо, коли важливо мінімізувати кількість хибнопозитивних результатів. Висока прецизійність потрібна, коли кожен неправильно ідентифікований позитивний випадок має серйозні наслідки.

$$\text{Прецизійність} = \frac{\text{кількість правильно виявлених позитивних випадків}}{\text{кількість всіх передбачених позитивних прогнозів}} \quad (3)$$

Оцінка точності, чутливості та інших показників допомагає в побудові ефективних і надійних систем захисту, що є критично важливим для забезпечення безпеки критично важливих об'єктів.

4. **Матриця невірних прогнозів (Confusion Matrix).** Матриця невірних прогнозів надає вичерпну інформацію про кількість правильно та неправильно класифікованих зразків для кожного класу. Дозволяє детально проаналізувати типи помилок моделі (хибнопозитивні, хибнонегативні) і допомагає в подальшій оптимізації.

5. **Коефіцієнт Джіні (Gini Coefficient).** Коефіцієнт Джіні вимірює нерівномірність розподілу позитивних і негативних випадків серед прогнозованих класів. Розраховується на основі розподілу позитивних і негативних випадків у моделях класифікації.

2.4. Інтеграція системи з існуючими системами безпеки критично важливих об’єктів

Інтеграція системи інтелектуального захисту критично важливих об'єктів з існуючими системами безпеки є важливою для забезпечення комплексного захисту і підвищення рівня безпеки.

На основі технології інтелектуального захисту критично важливих об'єктів пропонується інтеграція з наступними існуючими системами безпеки, яка представлена Рис. 2.14 та наведений опис в Таблиці 2.2.

Рис. 2.14 Інтеграція системи інтелектуального захисту критично важливих об'єктів з існуючими системами безпеки

Таблиця 2.2 – Інтеграція системи інтелектуального захисту критично важливих об'єктів з існуючими системами безпеки

Система	Опис	Переваги
Інтеграція системи штучного інтелекту з відеоспостереженням	Система відеоспостереження на критичних об'єктах може бути інтегрована з моделями штучного інтелекту, які аналізують відеопотік у режимі реального часу. Системи на базі конволюційних нейронних мереж (CNN) можуть виявляти і класифікувати аномальні поведінкові патерни, такі як підозрілі переміщення або несанкціоновані дії.	1. Автоматичне виявлення і класифікація загроз. 2. Зменшення кількості помилкових тривог завдяки точному аналізу. 3. Швидке реагування на потенційні інциденти без втручання людини.
Інтеграція систем прогнозування з існуючими системами кіберзахисту	Інтеграція систем прогнозування, таких як моделі машинного навчання, з існуючими кіберзахисними системами. Наприклад, використання алгоритмів, таких як Random Forest або Gradient Boosting, для прогнозування можливих кібератак на основі аналізу історичних даних про атаки та уразливості.	1. Проактивне виявлення і запобігання загрозам до їх реалізації. 2. Покращення захисту завдяки передбаченню нових атак. 3. Зменшення кількості успішних атак через попереджувальні заходи.
Інтеграція системи моніторингу з контролем доступу	Інтеграція систем контролю доступу з інтелектуальними системами для моніторингу аномальних спроб доступу. Наприклад, системи контролю доступу можуть бути підключені до аналітичних платформ, які використовують алгоритми машинного навчання для виявлення незвичних шаблонів доступу,	1. Поліпшене виявлення спроб несанкціонованого доступу. 2. Адаптивне управління доступом на основі поведінкових патернів. 3. Зменшення кількості помилкових тривог та

	таких як підозрілі спроби входу або зміну звичних маршруті доступу.	підвищення точності виявлення загроз.
Інтеграція системи захисту від DDoS-атак з інтелектуальними системами виявлення аномалій	Впровадження інтелектуальних систем для виявлення і запобігання DDoS-атакам. Наприклад, системи на основі алгоритмів класифікації та регресії можуть аналізувати трафік і виявляти аномалії, які вказують на можливі атаки, а потім автоматично реагувати на них шляхом блокування або перенаправлення трафіку.	1. Швидке виявлення і реагування на атаки DDoS. 2. Автоматизація процесу захисту без необхідності ручного втручання. 3. Поліпшення стійкості інфраструктури до високих навантажень.
Інтеграція систем раннього попередження з наявними системами реагування на надзвичайні ситуації	Використання інтелектуальних систем для раннього виявлення потенційних загроз і інтеграція з наявними системами реагування на надзвичайні ситуації. Наприклад, AI-системи можуть аналізувати дані з різних джерел (сенсори, моніторинг мережі) і передавати тривоги до систем управління надзвичайними ситуаціями для миттєвого реагування.	1. Раннє виявлення і своєчасне реагування на загрози. 2. Поліпшена координація між різними службами і системами. 3. Зменшення часу на прийняття рішень і покращення ефективності реагування.

Інтеграція систем інтелектуального захисту з існуючими системами безпеки критично важливих об'єктів дозволяє суттєво підвищити рівень захисту, забезпечити аналітичний підхід до управління загрозами і поліпшити загальну ефективність системи безпеки.

Ці інтеграції допомагають знизити вразливість об'єктів до атак і підвищити рівень готовності до надзвичайних ситуацій.

Проте, важливо ретельно планувати і реалізовувати такі інтеграції, враховуючи всі можливі виклики і потреби конкретних систем і об'єктів.

Серед відомих виробників систем безпеки для критично важливих обєктів можна виділити наступних – Таблиця 2.3.

Таблиця 2.3 – Виробники систем безпеки для критично важливих обєктів

Назва	Продукти	Опис
Hikvision	Камери відеоспостереження, системи відеоаналітики, системи контролю доступу.	Hikvision є одним з провідних постачальників відеоспостереження та безпеки, пропонуючи рішення для моніторингу, аналізу і контролю доступу на критичних об'єктах.
Siemens	Системи автоматизації і управління, системи відеоспостереження, системи контролю доступу, рішення для кібербезпеки.	Siemens надає рішення для управління і захисту критичних інфраструктур, зокрема в сфері автоматизації та кібербезпеки.
Schneider Electric	Системи управління енергетичними ресурсами, системи контролю доступу, рішення для відеоспостереження.	Schneider Electric спеціалізується на управлінні енергетичними ресурсами і безпеці, забезпечуючи захист критичних інфраструктур.
Axis Communications	Камери відеоспостереження, системи відеоаналітики, мережеві відеорегістратори.	Axis є відомим постачальником мережевих відео рішень, пропонуючи інноваційні рішення для відеоспостереження та аналітики.
Genetec	Платформи управління	Genetec надає програмні рішення для

	відеоспостереженням, системи контролю доступу, рішення для управління подіями і повідомленнями.	управління системами безпеки, включаючи інтеграцію відеоспостереження і контролю доступу.

2.5. Застосування IoT в системах інтелектуального захисту критично важливих об'єктах

В умовах швидкого розвитку технологій та зростаючої залежності від критично важливих об'єктів, таких як енергетичні станції, транспортні системи та системи водопостачання, захист цих об'єктів стає надзвичайно важливим. Інтернет речей (IoT) є однією з революційних технологій, яка обіцяє значні покращення в системах захисту критичних інфраструктур. Використання IoT дозволяє інтегрувати, автоматизувати та оптимізувати системи моніторингу і реагування на загрози.

Перевагами викоистання IoT є:

1. Раннє Виявлення Загроз: IoT-системи забезпечують своєчасне виявлення загроз завдяки безперервному моніторингу.

2. Автоматизація Реакцій: Системи можуть автоматично реагувати на загрози без людського втручання, знижуючи ризик помилок.

3. Обробка Великої Кількості Даних: IoT дозволяє зібрати і проаналізувати великі обсяги даних для виявлення складних патернів загроз.

Обмеженнями є:

1. Безпека Даних: Потреба в захисті даних від кібератак і несанкціонованого доступу.

2. Сумісність і Інтеграція: Проблеми інтеграції з існуючими системами через різні стандарти і протоколи.

3. Управління Даними: Потреба в потужних ресурсах для обробки великих обсягів даних.

IoT стає важливою складовою частиною сучасних систем захисту критично важливих об'єктів. Його можливості в зборі даних, автоматизації процесів і інтеграції з іншими системами забезпечують значні переваги для безпеки та ефективності роботи критичних інфраструктур.

Проте реалізація IoT вимагає врахування проблем безпеки, сумісності і обробки даних. Своєчасне впровадження і підтримка цієї технології може значно підвищити рівень захисту критичних об'єктів від потенційних загроз.

Загальна схема архітектури IoT представлена на Рис. 15

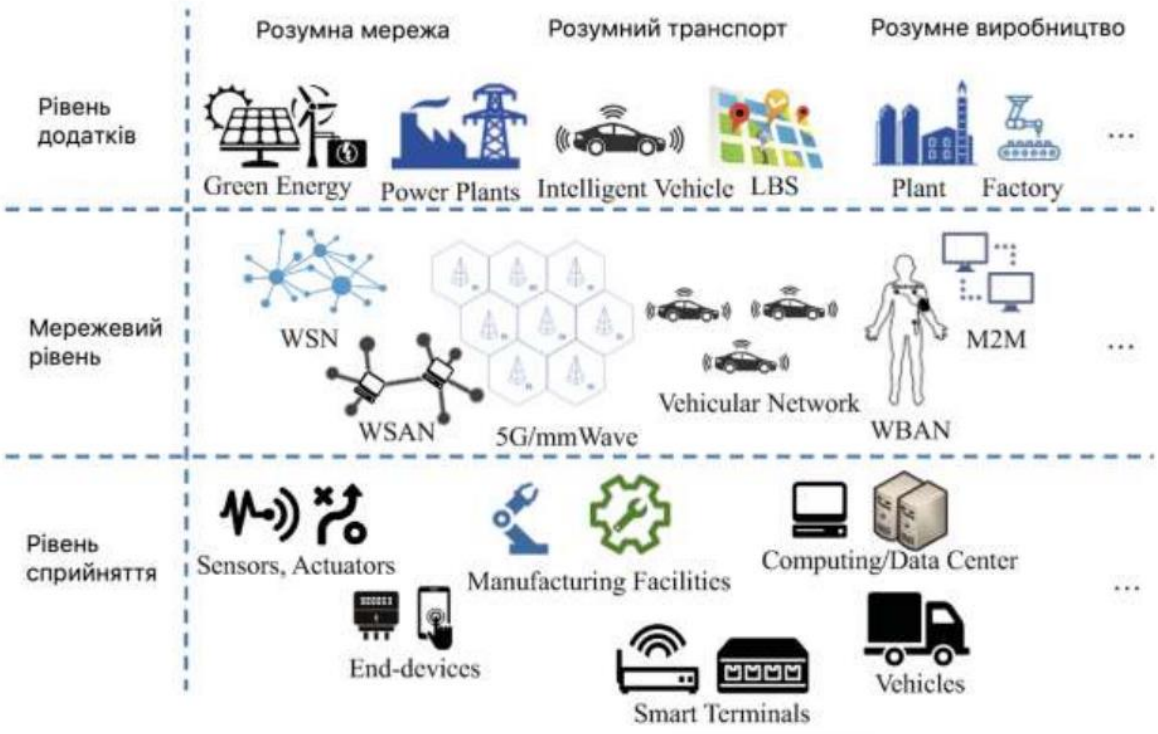


Рис. 2.15 Загальна архітектура IoT

Загальна архітектура системи IoT має чотири рівні: сприйняття, мережа, обробка та прикладний рівень.

Пристрої на рівні сприйняття, такі як датчики різних типів, сканери радіочастотної ідентифікації (RFID), камери спостереження, модулі глобальної системи позиціонування (GPS), конвеєрні системи, промислові роботи, відповідають за умови моніторингу, збір даних тощо.

Мережевий рівень відповідає за передачу даних до системи обробки наступного рівня та складаються з різних систем зв’язку, таких як WiFi, Bluetooth, Zigbee, LTE та протоколів IPv4 та IPv6.

Хмарні сервери та бази даних відповідають за аналіз даних, обчислення, прийняття рішень і зберігання великої кількості даних. Прикладний рівень забезпечує потреби кінцевих користувачів [16].

Розробка схеми IoT для систем захисту критично важливих об'єктів є ключовим етапом для забезпечення комплексного, ефективного і адаптивного захисту інфраструктури. Вона дозволяє інтегрувати сучасні технології для покращення моніторингу, аналізу, автоматизації і прогнозування загроз, що значно підвищує рівень безпеки і стійкість до ризиків. Схема IoT в системах захисту критично важливих об'єктів представлена на Рис.2.16.

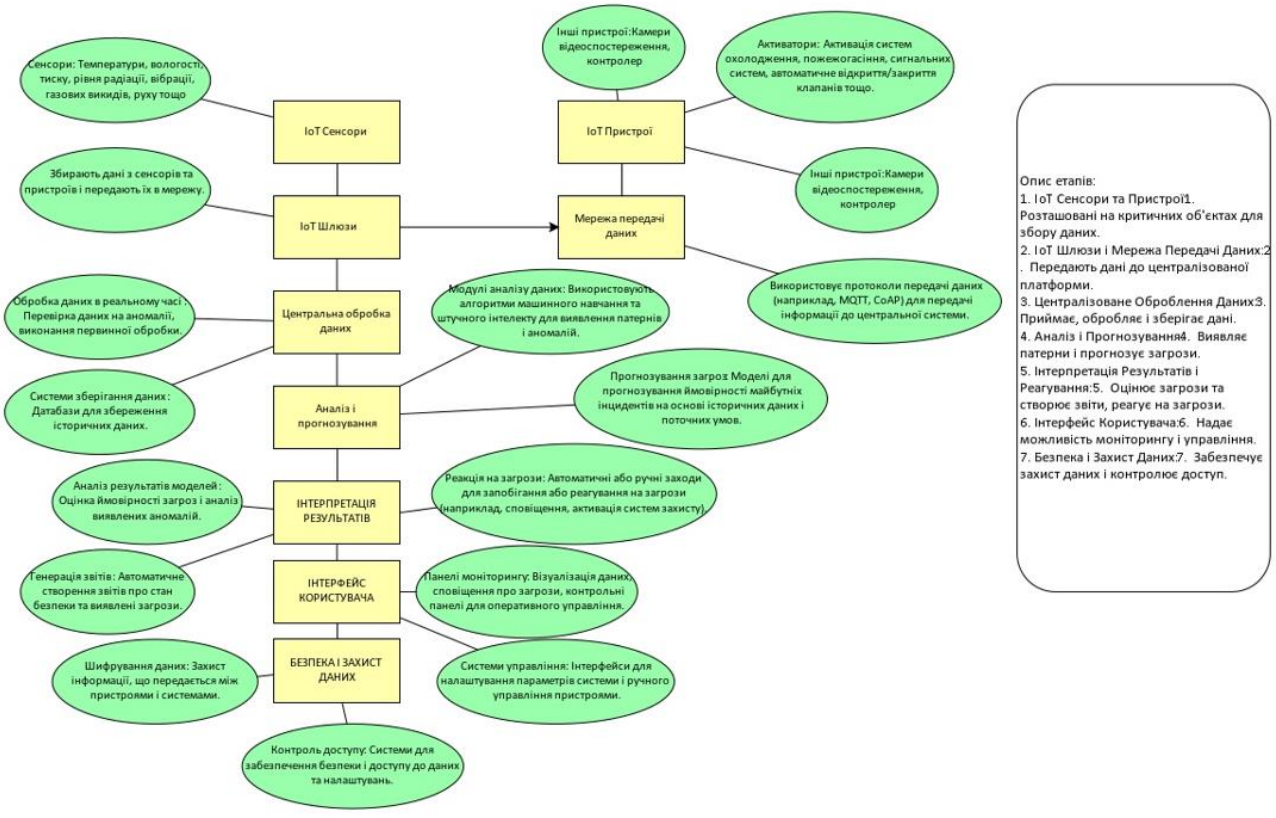


Рис. 2.16. Схема IoT в системах захисту критично важливих об'єктів

Інтернет речей (IoT) є потужним інструментом для підвищення безпеки критично важливих об'єктів. Його можливості в зборі і аналізі даних, автоматизації процесів і інтеграції з іншими системами безпеки надають значні переваги для

захисту інфраструктури. Попри це, реалізація IoT вимагає врахування викликів, таких як безпека даних, сумісність і управління великими обсягами даних. Правильне впровадження і підтримка цієї технології може значно підвищити рівень захисту критичних об'єктів і зменшити ризики від потенційних загроз.

2.6. Інструменти для обробки і аналізу даних для захисту критично важливих об'єктів

Обробка і аналіз даних є критично важливими для забезпечення безпеки критично важливих об'єктів. Ці процеси дозволяють виявляти потенційні загрози, реагувати на інциденти в реальному часі та приймати обґрунтовані рішення на основі отриманої інформації.

Для цього використовуються різноманітні інструменти, які допомагають збирати, очищати, зберігати, обробляти та аналізувати дані. В Таблиці 2.4 наведено детальний огляд основних інструментів для обробки даних, які можна використати для критично важливих об’єктів.

Таблиця 2.4 – Інструменти для обробки даних

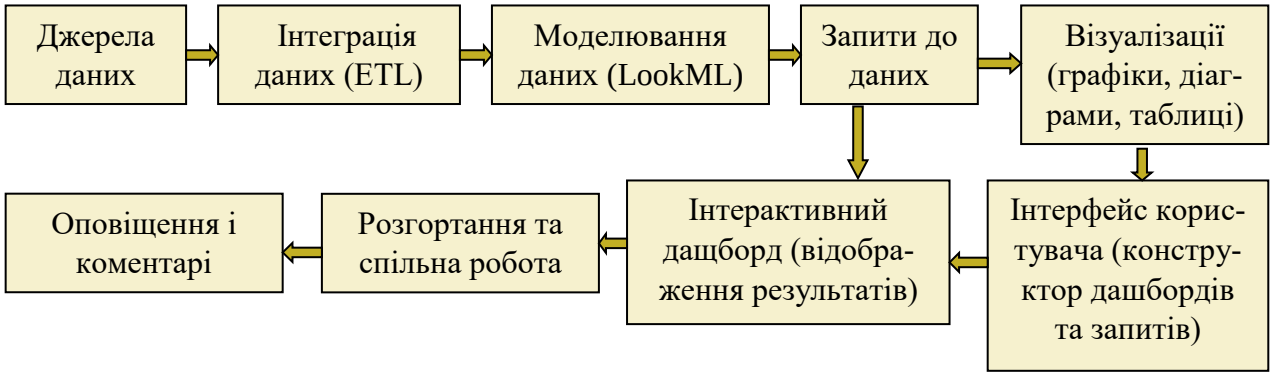
Назва інструменту	Опис
Системи управління базами даних (DBMS)	
Реляційні бази даних	
MySQL	Відкрите джерело, популярне для веб-додатків.
PostgreSQL	Відоме своєю надійністю та розширеними можливостями.
Oracle DB	Професійна система для великих підприємств, з розширеними функціями управління даними.
Microsoft SQL Server	Інструмент для корпоративних рішень з інтегрованими аналітичними можливостями.
Нереляційні бази даних	
MongoDB	Документоорієнтована база даних, що забезпечує гнучкість у зберіганні неструктурованих даних.
Cassandra	Система, розроблена для роботи з великими обсягами даних і забезпечення високо масштабованих рішень.

Redis	Вирізняється високою швидкістю для роботи з даними в пам'яті, використовується для кешування.
Інструменти для обробки даних	
Платформи для обробки потокових даних	
Apache Kafka	Система для обробки потокових даних в реальному часі, забезпечує масштабованість і високу доступність.
Apache Flink	Платформа для обробки даних у реальному часі з підтримкою складних обчислень.
Платформи для обробки великих даних	
Apache Hadoop	Фреймворк для розподіленої обробки великих даних, що використовує HDFS для зберігання і MapReduce для обробки.
Apache Spark	Інструмент для обробки даних у пам'яті, що забезпечує високу швидкість обробки і підтримує машинне навчання.
Інструменти для очищення та нормалізації даних	
ETL Інструменти	
Talend	Платформа для інтеграції даних з можливостями для очищення, перетворення та завантаження.
Apache Nifi	Інструмент для автоматизації обробки даних, що забезпечує швидке та гнучке інтегрування різних джерел даних.
Інструменти для аналізу даних	
Машинне навчання та статистичний аналіз	
Scikit-learn	Бібліотека для машинного навчання на Python, що включає різноманітні алгоритми для аналізу даних.
TensorFlow	Платформа для розробки і тренування моделей глибинного навчання.
R.	Статистична мова програмування для аналізу даних, з великим набором пакетів для статистичних розрахунків
Аналітика великих даних	
Tableau	Інструмент для візуалізації даних, що дозволяє створювати інтерактивні графіки та дашборди.
Power BI	Платформа для бізнес-аналітики від Microsoft, яка забезпечує інтеграцію з різними джерелами даних і створення звітів.
Інструменти для візуалізації даних	
Plotly	Бібліотека для створення інтерактивних графіків та візуалізацій даних.

D3.js	JavaScript бібліотека для створення динамічних і інтерактивних графічних елементів.

Інструменти для обробки і аналізу даних грають ключову роль у забезпеченні ефективного захисту критично важливих об'єктів. Використання сучасних технологій дозволяє збирати, очищати, зберігати та аналізувати дані, що забезпечує своєчасне виявлення загроз та реагування на них. Для критично важливих об'єктів, таких як енергетичні інфраструктури, транспортні системи та системи національної безпеки, інтерактивні дашборди можуть бути особливо корисними в управлінні та захисті.

Для аналізу даних критично важливих обєктів пропонується в якості допоміжного інструменту використання дашборда Looker. Looker забезпечує інтеграцію даних, моделювання, створення дашбордів і спільну роботу, що робить його потужним інструментом для бізнес-аналітики. Його гнучкість у моделюванні даних за допомогою LookML і можливість створювати інтерактивні візуалізації роблять Looker важливим компонентом для організацій, які прагнуть до ефективного аналізу та прийняття рішень на основі даних. На Рис.2.16 представлено схематичне зображення роботи інтерактивних дашбордів у Looker. Схема показує ключові компоненти і взаємодії в системі, які допомагають зрозуміти, як дані перетворюються на корисну інформацію через інтерактивні дашборди.



2.16 Схематичне зображення роботи інтерактивних дашбордів у Looker

3. МОДЕЛІ ТА МЕТОДИ МОНІТОРИНГУ ЗАГРОЗ НА КРИТИЧНО ВАЖЛИВІ ОБ'ЄКТИ

3.1. Оцінка наслідків кібератак на критичну інфраструктуру

Критична інфраструктура охоплює важливі системи і об'єкти, які є необхідними для функціонування суспільства та економіки, такі як енергетика, водопостачання, транспорт, зв'язок та фінансові системи. Критично важливі об'єкти інфраструктури є основою стабільного функціонування сучасного суспільства. Вони включають енергетичні системи, водопостачання, транспортні мережі, системи зв'язку, фінансові структури та інші важливі компоненти, від яких залежить безперебійна діяльність держави та економіки.

Однак ці об'єкти піддаються численним загрозам, які можуть серйозно вплинути на їх функціонування. Основні загрози для критичної інфраструктури можна поділити на кілька категорій, які представленя на Рис. 3.1.

Рис. 3.1 Основні загрози критичній інфраструктурі

Кібернапади: атаки з використанням вірусів, троянів, програм-вимагачів, фішингових атак, які можуть призвести до витоку даних або зупинки роботи систем.

Hacking: несанкціонований доступ до критичних систем для крадіжки або пошкодження інформації.

Denial of Service (DoS/DDoS): атаки, які призводять до перевантаження системи і її недоступності для користувачів.

Терористичні атаки: вибухи, стрілянина, руйнування важливих об'єктів.

Вандалізм: навмисні руйнування або пошкодження критичних об'єктів.

Природні катастрофи: повені, землетруси, урагани, які можуть знищити фізичні об'єкти інфраструктури.

Поломки обладнання: збої в роботі критичних систем через дефекти в технічному обладнанні.

Програмні збої: помилки в програмному забезпеченні, які можуть призвести до аварій або втрати даних.

Збої в управлінні: неефективне управління, корупція, недотримання стандартів безпеки.

Помилки персоналу: некваліфікованість або помилки співробітників, які можуть призвести до аварій або збитків.

Забруднення навколишнього середовища: аварії, що спричиняють екологічні катастрофи, можуть вплинути на функціонування критичних систем.

Конфлікти та війни: можуть спричинити руйнування інфраструктури та перебої у її функціонуванні.

Політична нестабільність: може призвести до саботажу або зниження рівня безпеки критичних об'єктів.

Захист критично важливих об'єктів від загроз є складним і багатогранним процесом, що вимагає врахування різних моделей загроз і застосування відповідних заходів безпеки. Комплексний підхід до виявлення та нейтралізації загроз може значно зменшити ризики і забезпечити стабільне функціонування критичної інфраструктури в умовах сучасного світу.

Важливо постійно вдосконалювати методи захисту, адаптуючи їх до нових викликів та загроз.

Найбільш поширеними загрозами є кіберзлочини, які включають атаки на комп'ютерні системи і мережі з метою завдання шкоди, незаконного доступу до інформації або порушення роботи інфраструктури.

Кібератаки можна класифікувати за різними критеріями, такими як масштаб, метод реалізації, мотивація зловмисників і вплив на системи. До найбільш розповсюджених видів кібератак відносяться атаки DDoS (атаки на відмову в обслуговуванні), фішинг, впровадження шкідливих програм (malware) у комп'ютерні системи, злому паролів, викрадення даних, саботаж, шпигунство та інші.

Коли йдеться про критичну інфраструктуру держави, наслідки кібератак можуть бути надзвичайно серйозними. Наприклад, атаки на енергетичні системи можуть призвести до масового відключення електропостачання, порушення роботи промислових об'єктів і значного впливу на економіку країни.

Атаки на транспортні системи можуть викликати збої в русі транспорту, зупинку міжміських комунікацій і порушення логістичних процесів. Загрози для критичної інфраструктури можуть включати атаки на енергетичні системи, транспортні мережі, комунікаційні інфраструктури, фінансові установи, системи охорони здоров'я та інші.

Для ефективного захисту критичної інфраструктури держави необхідно розробити і впровадити спеціалізовані механізми захисту, які враховують особливості кожного сектора. Це може включати використання сучасних систем захисту, моніторинг і виявлення інцидентів, розробку політик безпеки, проведення тренінгів для персоналу, створення резервних копій та відновлення даних, а також налагодження співпраці з іншими державними органами, приватними компаніями і міжнародними організаціями.

Аналіз загроз для критичної інфраструктури держави охоплює оцінку потенційних сценаріїв атак, виявлення вразливостей та розробку заходів захисту. Для ефективного захисту критичної інфраструктури потрібно розробити комплексну стратегію, яка включає технічні, організаційні та правові заходи.

Кібератака росії на Україну стала першим випадком успішної кібератаки на енергетичну інфраструктуру. Випадок стався 23.12.2015 була проведена кібератака на внутрішню мережу «Прикарпаття обленерго» [17].

Внаслідок цього були зупинені 30 станцій, і близько 230 тисяч осіб залишилися без електропостачання протягом кількох годин. Кіберзлочинці змогли отримати доступ до мережі «Прикарпаття обленерго» завдяки зараженню комп'ютера одного з співробітників троянською програмою «BlackEnergy».

Оцінка наслідків кібератак на критичну інфраструктуру

Оцінка наслідків кібератак на критичну інфраструктуру включає в себе аналіз потенційних наслідків, які можуть виникнути у разі успішного нападу на системи критичної інфраструктури. Цей процес допомагає визначити масштаб і вплив можливих інцидентів на функціонування та безпеку інфраструктури, а також оцінити можливі збитки і наслідки.

Оцінка наслідків охоплює наступні аспекти:

- **Втрати функціональності**. Кібератаки можуть призвести до зупинки роботи систем, зниження продуктивності або відмови в обслуговуванні. Це особливо критично, коли йдеться про системи, що забезпечують життєво важливі послуги, такі як електропостачання, транспорт або медичні послуги.
- **Порушення безпеки**. Атаки можуть викликати порушення безпеки, включаючи злом систем аутентифікації та авторизації, несанкціонований доступ до конфіденційної інформації, втрату або пошкодження даних. Це може негативно вплинути на фінансову стійкість, репутацію і взаємодію з користувачами інфраструктури.
- **Втрати даних**. Оскільки критична інфраструктура зазвичай містить великі обсяги важливих даних, кібератака може призвести до їх втрати або пошкодження. Наприклад, втрата медичних записів може загрожувати безпеці пацієнтів, а втрата фінансових даних — фінансовим збиткам і порушенню довіри.

- **Фінансові збитки**. Успішні кібератаки можуть суттєво вплинути на фінансову стійкість організацій, що управляють критичною інфраструктурою. Це може включати втрату прибутку, значні витрати на відновлення систем і інфраструктури, втрату довіри партнерів і клієнтів, а також можливі судові позови і штрафи.

Оцінка наслідків кібератак для критичної інфраструктури вимагає використання аналітичних методів, статистичних даних, сценарного аналізу та експертної оцінки. Це дозволяє краще усвідомити потенційні ризики та наслідки атак, а також приймати ефективні заходи для попередження та реагування на такі загрози.

Оцінка потенціалу загрози має важливе значення для визначення масштабів ураження об'єкта критичної інфраструктури загрозами і ризиків від них. Чим більший потенціал у загрози, тим більший ризик від неї для об'єкта критичної інфраструктури.

Потенціал загрози може бути оцінений кількісно з використанням методів експертних оцінок. Для кількісної оцінки потенціалу загрози (П) автором пропонується розглядати його як функцію комплексу з n параметрів a_i загрози

$$П = f(a_1, a_2, ...a_n) \quad (4)$$

Кожен із цих параметрів оцінюється експертами за однаковою бальною шкалою. Конкретний вид функції П може бути різним, але, коли важливість параметрів a_i однакова, потенціал загрози можна представити як середнє арифметичне значення їх бальних оцінок:

$$П = (a_1 + a_2 + ... + a_n) / n \quad (5)$$

У разі, коли важливість параметрів a_i різна, використовується їх коефіцієнт значимості k_i.Тоді

$$П = (k_1 a_1 + k_2 a_2 + ... + k_n a_n) \quad (6)$$

причому $k_1 + k_2 + \ldots + k_n = 1$. Крім того, треба враховувати, що потенціал загрози як явища або події може змінюватися з часом t, а тому у загальному вигляді він буде мати такий вигляд

$$П = f(a_1, a_2, ...a_n; t) \quad (7)$$

Тим самим з’являється реальна можливість здійснювати прогнозування зміни потенціалу загрози у часі, а також прогнозування небезпеки від ураження нею об’єкта КІ [18].

Важливо відзначити, що комплексна оцінка потенціалу загрози є ключовим аспектом визначення рівня небезпеки для об'єкта критичної інфраструктури.

Якісна оцінка потенційних загроз має значний вплив на підвищення ефективності роботи органів державної безпеки, правоохоронних органів та спеціально уповноважених державних структур. Це сприяє покращенню захисту критичної інфраструктури і зміцненню державної безпеки.

Отже, ці атаки не тільки загрожують функціонуванню об'єктів критичної інфраструктури, таких як енергетичні системи, транспортні мережі та комунікаційні структури, але й можуть суттєво вплинути на економічну та соціальну стабільність.

3.2. Моделі атак на критично важливі об’єкти

К розповсюдженим кібератакам відносяться:

Фішинг та соціальна інженерія: Фішинг представляє собою форму обману, призначену для витягування особистої інформації від довірливих або необачних користувачів мережі. Основна мета шахраїв полягає в тому, щоб отримати особисті дані клієнтів.

Шахраї намагаються змусити користувачів самостійно надати конфіденційну інформацію, наприклад, шляхом надсилання електронних листів із запитаннями підтвердження реєстрації облікового запису. Ці листи містять посилання на веб-сайти, зовнішній вигляд яких повністю копіює дизайн відомих ресурсів.[19]

Фішинг передбачає застосування психологічних і технічних методів для здобуття конфіденційної інформації.

Спам-повідомлення, що можуть виглядати як офіційні листи від колег, використовуються для крадіжки облікових даних та отримання доступу до систем.

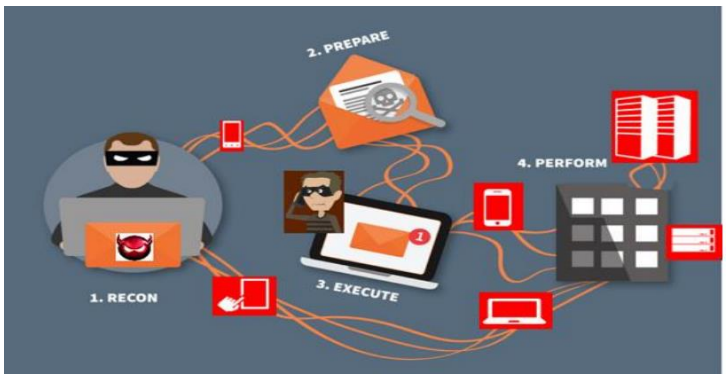


Рисунок 3.2 Ілюстрація механізму фішингової атаки

Модель фішингу має наступну структуру:

Рис. 3.3 Модель фішингу на критично важливі об’єкти

Соціальна інженерія – це спосіб зламу, в якому використовуються психологічні методи для обману людини.[20]

Шкідливе програмне забезпечення (malware) – це вид програмного забезпечення, який заважає нормальному функціонуванню комп'ютера, збирає конфіденційну інформацію або отримує несанкціонований доступ до приватних комп'ютерних систем. Воно може проявлятися у вигляді коду, скриптів, активного контенту чи іншого програмного забезпечення. Термін "шкідливий" використовується як

загальна назва для різних форм ворожого або непроханого програмного забезпечення.

Атаки з використанням вірусів, троянів та іншого шкідливого програмного забезпечення стають дедалі складнішими. Зловмисники можуть застосовувати ці інструменти для шпигунства, вимагання викупу або виконання інших зловмисних дій.

DoS та DDoS атаки мають на меті зробити комп'ютерні ресурси недоступними для призначених користувачів. Такі атаки спрямовані на перевантаження мережевих ресурсів об'єкта, що може призвести до тимчасової або повної відмови в обслуговуванні, завдаючи значних збитків і порушуючи нормальне функціонування критичної інфраструктури.

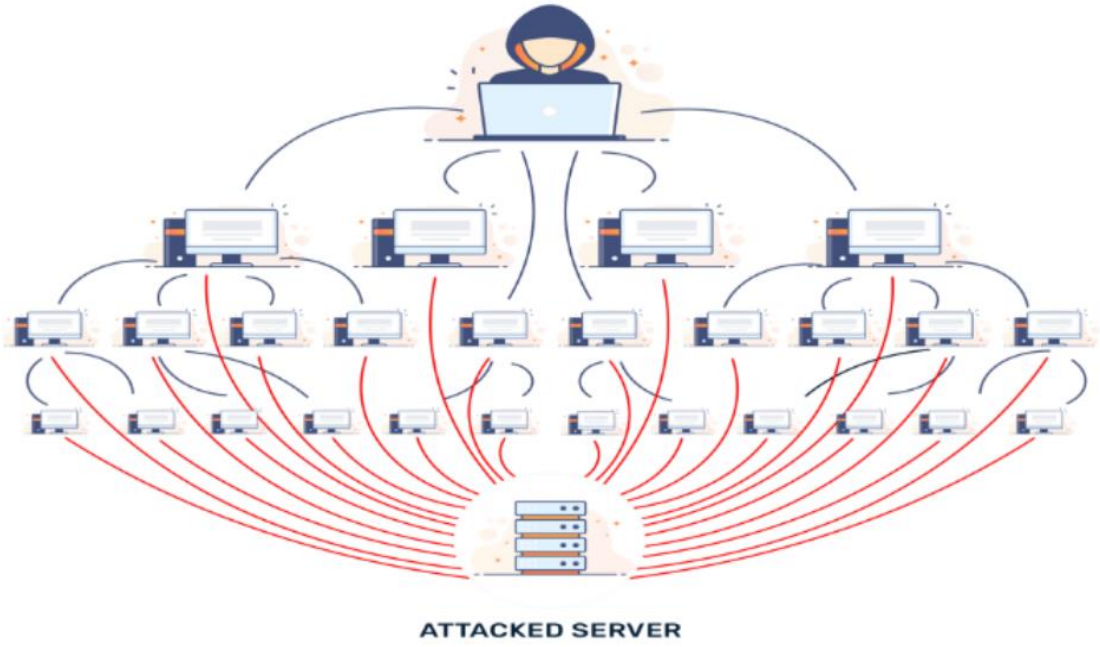


Рисунок 3.4 Ілюстрація DDOS атаки

На Рис. 3.5. Наведена модель DDOS атаки на критичну інфраструктуру. Ця модель допоможе візуально зрозуміти процес DDoS атаки та її вплив на критичну інфраструктуру.

Рис. 3.5 Модель DDOS атаки на критичну інфраструктуру

Експлуатація вразливостей ПЗ: Атаки, спрямовані на використання вразливостей програмного чи апаратного забезпечення, можуть призвести до незаконного доступу та викрадення конфіденційної інформації. Важливо регулярно оновлювати програмне забезпечення та встановлювати необхідні патчі для усунення потенційних вразливостей [21].

Регулярне оновлення програмного забезпечення, встановлення патчів та застосування комплексних заходів з захисту допомагають зменшити ризики і забезпечити безпеку критичних інфраструктур. Однак, важливо постійно вдосконалювати стратегії захисту, щоб адаптуватися до нових загроз і забезпечити надійний захист від атак.

На Рис. 3.6. Наведена модель атак, спрямовані на використання вразливостей програмного чи апаратного забезпечення на критичну інфраструктуру. Віддалені мережеві атаки здійснюються шляхом негативного впливу на розподілені обчислювальні системи через програмні засоби через зв'язкові канали.

Віддалені мережеві атаки є однією з найбільш поширених і небезпечних форм кібератак, що здійснюються через програмні засоби за допомогою мережевих каналів.

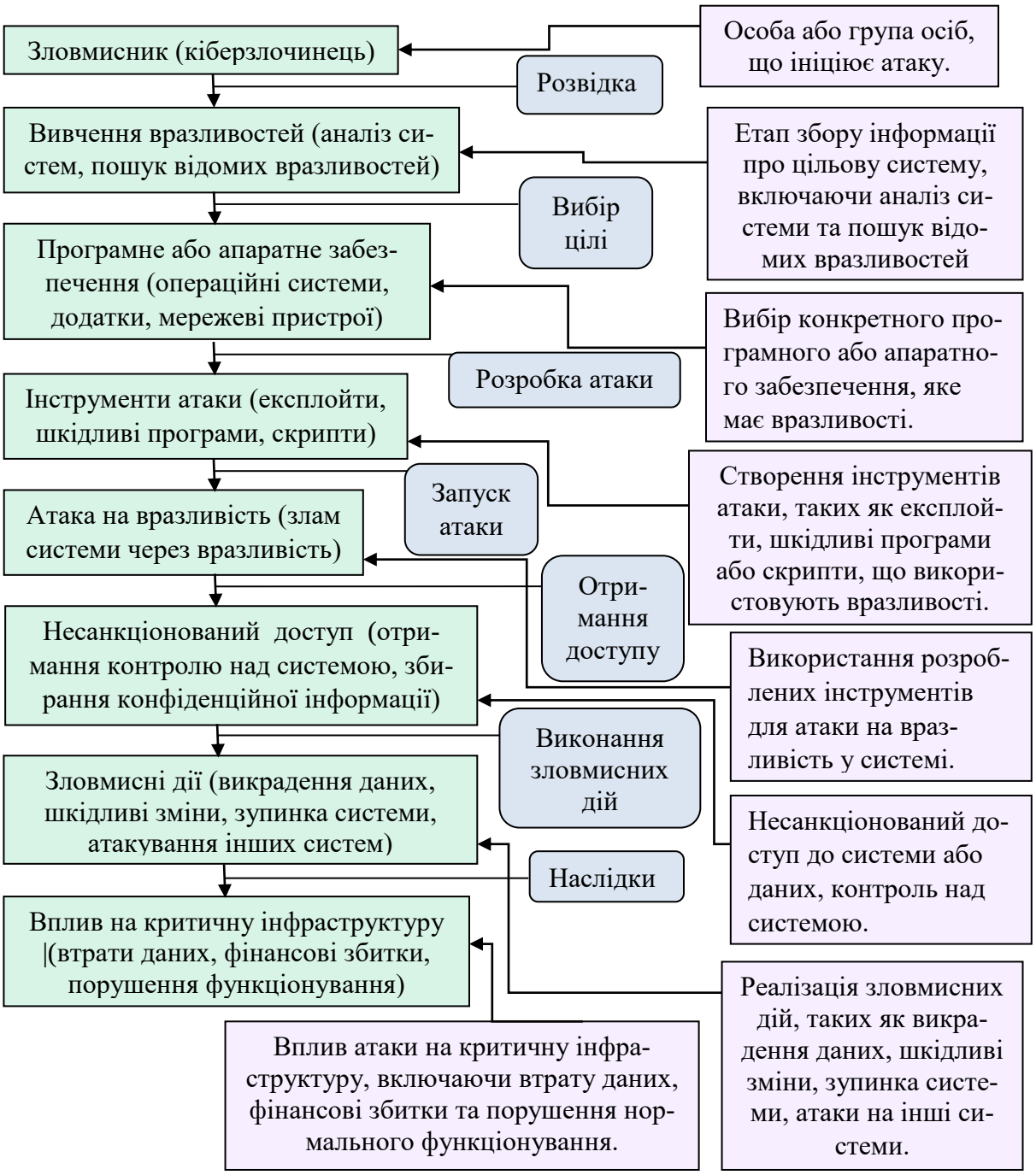


Рис. 3.6 Модель атак, спрямовані на використання вразливостей програмного чи апаратного забезпечення на критичну інфраструктуру

Ці атаки можуть серйозно впливати на розподілені обчислювальні системи, порушувати їх функціональність і безпеку. Основними видами таких атак є маніпуляції з маршрутизацією та DNS-атаки, які можуть призвести до перенаправлення трафіку або блокування доступу до критичних ресурсів. На Рис. 3.7. представлено алгоритм, як відбувається віддалена мережева атака на критичну інфраструктуру.

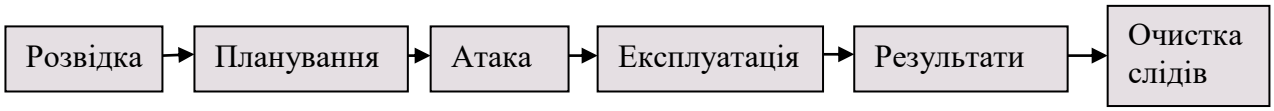


Рис. 3.7. Алгоритм віддаленої мережевої атаки на критичну інфраструктуру.

Розвідка: Збір інформації, визначення цілей. Розвідка є першим і критично важливим етапом у процесі віддалених мережевих атак на критичну інфраструктуру. Це етап, на якому зловмисники збирають інформацію про цільову систему, визначають потенційні слабкі місця та формують стратегію атаки. Точне та всебічне збирання інформації дозволяє атакуючим спланувати більш ефективний наступ, зменшуючи ймовірність виявлення та збільшуючи ймовірність успіху атаки. Для збору інформації і визначення цілей використовуються різні інструменти: Nmap (для сканування мережі та виявлення відкритих портів), Shodan (для пошуку пристроїв в Інтернеті та виявлення вразливих систем), Maltego (для збору та візуалізації інформації з різних джерел).

Планування: Аналіз вразливостей і підготовка до атаки. Планування є критичним етапом у віддалених мережевих атаках на критичну інфраструктуру. На цьому етапі зловмисники використовують зібрану інформацію для детального аналізу вразливостей цільової системи і розробки стратегії атаки. Правильне планування дозволяє максимізувати ймовірність успіху атаки, зменшуючи ризики виявлення та підвищуючи ефективність.

Аналіз вразливостей є основним етапом у підготовці до атаки. Цей процес включає: Ідентифікацію вразливостей у програмному забезпеченні (використання інструментів для виявлення відомих уразливостей у версіях ПЗ, що використовуються в цільовій системі; Аналіз конфігурацій (оцінка можливих помилок у конфігураціях системи або мережі, які можуть бути використані для атаки); Тестування вразливостей - на цьому етапі зловмисники проводять тестування, щоб перевірити, чи дійсно виявлені вразливості є активними:

1. Пенетраційне тестування: Симуляція атак для перевірки наявності вразливостей і визначення їх потенційного впливу.

2. Експлуатація вразливостей: Використання експлойтів для перевірки можливості успішного використання вразливостей. **Атака:** Реалізація атаки через маніпуляцію з маршрутизацією, DNS-атаки або інші методи.

Віддалені мережеві атаки на критичну інфраструктуру є однією з найбільших загроз сучасного кіберпростору. Ці атаки часто здійснюються через маніпуляції з маршрутизацією, DNS-атаки або інші методи, які дозволяють зловмисникам отримати контроль над інформаційними потоками та порушити роботу критичних систем. Основними типами атак є маніпуляція з маршрутизацією і DNS-Атаки. Маніпуляція з маршрутизацією є технікою, що включає зміну маршруту передачі даних між мережевими пристроями. Це може бути здійснено шляхом підміни маршрутних оголошень або маніпуляцій з таблицями маршрутизації, що дозволяє зловмисникам перенаправити трафік до своїх систем або перехопити його.

Типи маніпуляцій:

1. BGP (Border Gateway Protocol) Аттаки: Зловмисники можуть зловживати BGP для перепрямування трафіку через некоректно оголошені маршрути. Це дозволяє перехопити, змінити або навіть блокувати трафік.

2. ARP (Address Resolution Protocol) Спуфінг: Атака, яка дозволяє зловмиснику змінити таблицю ARP на локальному рівні, що призводить до перенаправлення трафіку через підроблені IP-адреси.

DNS атаки включають в себе маніпуляцію з DNS-записами або сервером, що дозволяє зловмисникам перенаправляти трафік на підроблені сайти або сервіси.

Типи DNS-Атак:

1. DNS Спуфінг: Зловмисник підмінює DNS-кеш зловмисними записами, що призводить до перенаправлення запитів на підроблені IP-адреси.

2. DNS Рекурсивний Спуфінг: Атака, що включає в себе маніпуляцію запитами DNS до рекурсивного DNS-сервера для отримання неправильних відповідей.
Існують також інші методи атак:

1. IP-Спуфінг. IP-спуфінг включає підробку IP-адрес для маскування ідентичності атакуючого або для обходу механізмів безпеки. Це дозволяє зловмисникам отримати доступ до захищених систем або перехопити мережевий трафік.

2. Man-in-the-Middle (MitM) атаки. Атака MitM передбачає перехоплення і можливу модифікацію комунікацій між двома сторонами без їхньої відомості. Це дозволяє зловмисникам отримати конфіденційні дані або впливати на передачу інформації.

3. Синхронізація з'єднань**.** Використання технік для перехоплення та маніпуляції з'єднаннями між клієнтами та серверами, включаючи атакування на рівні сесії, щоб контролювати або блокувати обмін даними. Експлуатація - використання отриманих даних для подальших дій.

Після здійснення віддалених мережевих атак на критичну інфраструктуру зловмисники часто фокусуються на використанні отриманих даних для досягнення своїх цілей. Етап експлуатації є критично важливим для зловмисників, оскільки він визначає, як саме вони будуть використовувати зібрану інформацію для максимізації шкоди або вигоди. Ця стаття розгляне, як отримані дані використовуються для подальших дій при віддалених мережевих атаках, а також можливі наслідки та стратегії захисту. Отримані дані можуть включати чутливу інформацію, таку як: особисті дані: включає імена, адреси, номери соціального страхування або фінансову інформацію, яку можна використати для шахрайства або крадіжки особистості; фінансову інформацію**:** дані кредитних карток, банківські реквізити або інформація про транзакції, що може бути використана для фінансових махінацій. Зловмисники можуть використовувати отримані дані для впровадження шкідливого ПЗ, наприклад: вимагання виплат (Ransomware): шкідливе ПЗ може зашифрувати дані і вимагати викуп за їх розшифрування; збір інтелектуальної власності: Витік або продаж технологічних патентів та інноваційних рішень.

Етап експлуатації в віддалених мережевих атаках на критичну інфраструктуру є ключовим для зловмисників, які намагаються отримати максимальну виго-

ду з отриманих даних. Оцінка впливу атаки є важливим етапом в розумінні реальних ризиків і шкоди, що може бути завдана внаслідок таких інцидентів.

Віддалені мережеві атаки можуть призвести до збоїв в роботі критичних систем, таких як енергетичні мережі, транспортні системи або комунікаційні канали. Наприклад, атаки можуть спричинити відмову в обслуговуванні або зниження продуктивності систем, що має серйозні наслідки для їхньої функціональності. Атаки можуть блокувати доступ до важливих ресурсів або даних, що ускладнює або робить неможливим виконання критичних завдань. Наприклад, у разі атаки на інформаційні системи підприємства може бути порушений доступ до даних, необхідних для управління виробництвом або надання послуг.

Витрати на відновлення систем і усунення наслідків атаки можуть бути значними. Це включає витрати на ремонт або заміну обладнання, оновлення програмного забезпечення та відновлення даних. Додатково, витрати можуть включати виплату викупу (у випадку атаки з вимаганням), штрафи та компенсації постраждалим клієнтам.

Через збої у функціонуванні систем підприємства може втратити прибуток, особливо якщо атака призводить до тимчасової зупинки або скорочення виробництва, зниження обсягу продажів або погіршення якості обслуговування клієнтів. Атаки можуть серйозно вплинути на репутацію організації. Втрата довіри з боку клієнтів, партнерів і громадськості може мати тривалі наслідки для бізнесу, зокрема зменшення клієнтської бази або погіршення бізнес-відносин.

Інциденти, пов’язані з безпекою, можуть погіршити імідж компанії, особливо якщо вони приводять до широкого розголосу в медіа або мають масштабний характер. Організації можуть отримати штрафи або інші санкції від регуляторних органів за недостатній рівень захисту даних або порушення законодавства про захист інформації. Очистка слідів -видалення слідів атаки та ускладнення розслідування. Віддалені мережеві атаки на критичну інфраструктуру часто супроводжуються спробами зловмисників приховати свою діяльність та ускладнити розслідування. Однією з основних стратегій таких атак є очищення слідів, що дозво-

ляє нападникам уникнути виявлення та відповідальності. Зловмисники намагаються приховати свій слід, щоб уникнути виявлення їхньої діяльності правоохоронними органами або спеціалістами з кібербезпеки.

Методи очистки слідів наведено на Рис. 3.8.

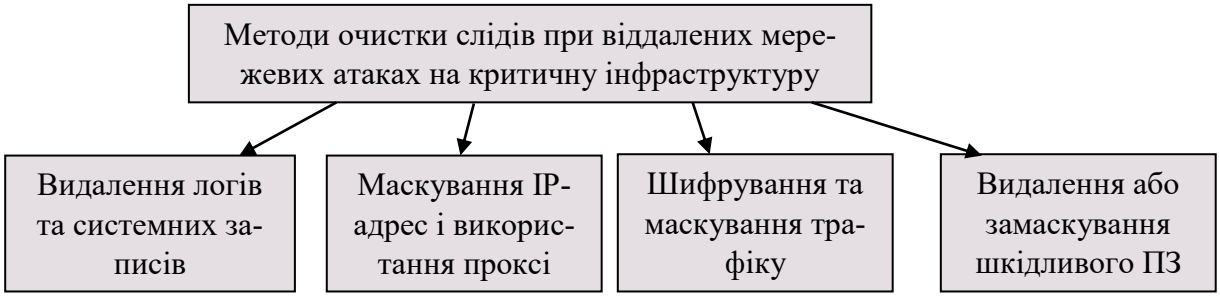


Рис. 3.8. Методи очистки слідів при віддалених мережевих атаках на критичну інфраструктуру

Видалення логів та системних записів. Очистка логів та зміна таймштампів: Зловмисники можуть видаляти або змінювати записи в логах систем для приховування своїх дій. Це включає видалення записів про входи, виходи, помилки або інші системні події.

Маскування IP-адрес і використання проксі. Анонімізація трафіку та використання динамічних IP-адрес: Зловмисники використовують проксі-сервери або мережі TOR для приховування реальних IP-адрес, що ускладнює трасування джерела атаки.

Шифрування та маскування трафіку. Зловмисники можуть шифрувати дані, що передаються між зараженими системами і командним центром, щоб ускладнити аналіз мережевого трафіку. Також можливе використання різних протоколів: зловмисники можуть використовувати нетипові або зашифровані протоколи для комунікації, щоб ускладнити виявлення їхньої діяльності.

Видалення або замаскування шкідливого ПЗ. Після завершення атаки, зловмисники можуть видаляти або маскувати шкідливе програмне забезпечення, щоб уникнути його виявлення під час сканування системи. Також можлива обфускація коду - використання технік обфускації коду для шкідливого ПЗ, щоб ускладнити його ідентифікацію та аналіз.

Фізичні атаки є серйозною загрозою для критичної інфраструктури, оскільки спрямовані на важливі системи та ресурси, що забезпечують функціонування суспільства.

На Рис.3.9 наведена модель можливих фізичних атак на критичну інфраструктуру.

Рис. 3.9 Модель здійснення фізичних атак на критичну інфраструктуру

Компрометація довірених осіб: Зловмисники можуть намагатися впливати на співробітників або адміністраторів об'єкта для отримання доступу до конфіденційної інформації або здійснення зловмисних дій.

3.3. Методи моніторингу загроз на критично важливі об’єкти

Моніторинг загроз дозволяє організаціям виявляти та реагувати на потенційні кіберзагрози. Це передбачає постійний збір та аналіз даних, щоб забезпечити раннє виявлення загроз і своєчасну реакцію на них. В таблиці 3.1 представлено методи моніторингу загроз на критично важливі об’єкти, які будуть використані для створення технології інтелектуального захисту критично важливих об’єктів.

Таблиця 3.1 – Методи моніторингу загроз на критично важливі об’єкти

Назва	Опис	Функції	Переваги	Недоліки
Системи управління безпекою інформаційних систем (SIEM)	SIEM-системи об'єднують дані з різних джерел безпеки, включаючи мережі, сервери та додатки, в єдину платформу для їхнього збору, зберігання та аналізу. Це дозволяє здійснювати кореляцію подій безпеки, виявлення аномалій, генерацію сповіщень та управління інцидентами.	1.Збір та кореляція даних з різних джерел. 2. Аналіз і виявлення аномалій та підозрілих активностей. 3. Генерація звітів та сповіщень про події безпеки. 4. Реагування на інциденти і управління подіями безпеки.	1.Централізоване управління безпекою. 2.Можливість детального аналізу подій. 3.Полегшення процесу відповідності нормативним вимогам.	1.Високі вимоги до ресурсів для обробки великих обсягів даних. 2.Потреба в належній конфігурації та підтримці.
Системи виявлення та запобігання вторгненням (IDS/IPS)	IDS та IPS системи спеціалізуються на виявленні та блокуванні несанкціонованих спроб доступу і небезпечних дій. IDS здійснює моніторинг мережевого трафіку і системних ресурсів для виявлення підозрілих активностей, тоді як IPS також автоматично реагує на загрози, блокуючи або обмежуючи небезпечний трафік.	1.Виявлення аномальних активностей в мережі. 2.Автоматичне блокування небезпечних дій. 3.Аналіз і звітність про виявлені загрози.	1.Швидка реакція на загрози. 2.Запобігання потенційним атакам в реальному часі.	1.Можливість помилкових спрацювань і вплив на законний трафік. 2.Потреба в постійній налаштуванні та оновленні сигнатур загроз.
Аналіз мережевого трафіку	Аналіз мережевого трафіку включає моніторинг і оцінку трафіку, що	1.Моніторинг і запис мережевого трафіку.	1.Можливість виявлення і аналізу ано-	1.Великий обсяг даних для аналізу.

	проходить через мережу. Це допомагає виявити аномалії та підозрілі дії, такі як DDoS-атаки або спроби зламу.	2.Виявлення нетипових патернів трафіку. 3.Аналіз і кореляція даних для виявлення загроз.	малій у мережевому трафіку. 2.Допомога у виявленні DDoS-атак та інших мережевих загроз.	2.Потреба в ефективних інструментах для обробки даних.
Аналіз системних журналів	Аналіз системних журналів включає моніторинг і оцінку журналів подій з різних системних ресурсів. Це дозволяє виявити аномальні події, що можуть вказувати на потенційні загрози.	1.Збір і зберігання системних журналів. 2.Аналіз і виявлення аномальних подій. 3.Генерація звітів і сповіщень про події безпеки.	1.Детальне вивчення активностей у системі. 2.Можливість виявлення підозрілих дій.	1.Великі обсяги даних для обробки. 2.Потреба в регулярному аналізі і підтримці.
Оцінка уразливостей	Оцінка уразливостей включає ідентифікацію та аналіз слабких місць у програмному та апаратному забезпеченні. Це дозволяє виявити проблеми, які можуть бути використані зловмисниками.	1.Сканування і оцінка уразливостей. 2.Рекомендації щодо усунення виявлених проблем. 3.Регулярні перевірки і оновлення безпеки.	1.Виявлення потенційних слабких місць. 2.Покращення загальної безпеки системи.	1.Постійна необхідність у скануванні і виправленні уразливостей. 2.Ризик пропущення нових уразливостей.

На Рис.3.10 представлена схема «Методи моніторингу загроз на критично важливі об’єкти», які будуть використані для створення технології інтелектуального захисту критично важливих об’єктів.

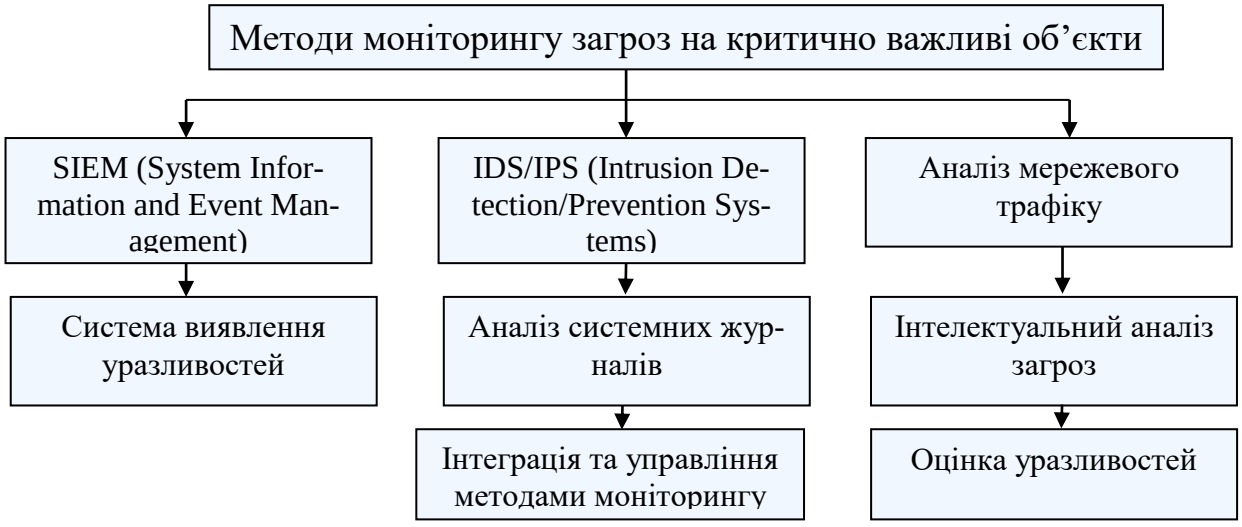


Рис. 3.10 Методи моніторингу загроз на критично важливі об’єкти

Схема показує, як різні методи моніторингу загроз взаємодіють між собою для забезпечення комплексного захисту критично важливих об'єктів. Інтеграція цих методів дозволяє здійснювати централізоване управління безпекою, своєчасно реагувати на загрози та зменшувати ризики для критичної інфраструктури.

Отже, моніторинг загроз є ключовим компонентом захисту критичної інфраструктури. Використання різних методів моніторингу, таких як SIEM-системи, IDS/IPS, аналіз мережевого трафіку, системних журналів, інтелект про загрози та оцінка уразливостей, дозволяє ефективно виявляти та реагувати на потенційні загрози.

3.4. Алгоритм реагування на інциденти загроз на критичну інфраструктуру

Алгоритм реагування на інциденти загроз на критичну інфраструктуру є ключовим компонентом стратегії кібербезпеки, що допомагає забезпечити швидке і ефективне реагування на кіберзагрози. Він забезпечує структурований підхід до управління інцидентами, що дозволяє мінімізувати наслідки атак і підтримувати стабільність критичних систем. Важливо забезпечити належну організацію кожного етапу, від виявлення загрози до відновлення та аналізу. На Рис. 3.11. наведено алгоритм реагування на інциденти загроз на критичну інфраструктуру.

Рис.3.11. Алгоритм реагування на інциденти загроз на критичну інфраструктуру

Моніторинг та Сигналізація. На цьому етапі використовується системи SIEM (Security Information and Event Management) для збору і аналізу даних про

безпеку, системи виявлення і запобігання вторгнень (IDS/IPS) для автоматичного виявлення аномалій.

Аналіз подій складається з розгляду сповіщень та подій, що вказують на можливі інциденти та проводиться первинний аналіз для визначення можливих загроз та виявлення підозрілих дій.

Оцінка серйозності та впливу – це визначення масштабів інциденту, його впливу на критичну інфраструктуру та потенційні наслідки.Також на цьому етапі відбувається оцінка ризиків та пріоритетів реагування.

Класифікація інцидентів. Характеризується визначенням типу атаки та встановленням категорії інциденту для відповідного реагування.

Активні заходи. На цьому етапі відбувається впровадження контрзаходів для зупинки атаки або обмеження її впливу та відключення зловмисних доступів та ізоляція заражених систем.

Комунікація складається з двох підетапів: Інформування відповідних команд і осіб про інцидент та координації дій між різними підрозділами та зовнішніми партнерами **Відновлення функціональності** – це відновлення систем з резервних копій та виправлення пошкоджених систем і відновлення нормальної роботи критичної інфраструктури.

Аналіз і вдосконалення складається з проведення аналізу причин інциденту та впровадження змін для запобігання подібним атакам у майбутньому та оновлення політик безпеки та процедур реагування.

Документування інциденту містить в собі запис усіх дій, подій та рішень, прийнятих під час інциденту та збір доказів та підготовка звітів про інцидент.

Аналіз та звітування це два процеси: оцінка результатів реагування на інцидент та підготовка звітів для внутрішніх та зовнішніх зацікавлених сторін, включаючи регуляторів та аудиторів.

4. РОЗРОБКА ТЕХНОЛОГІЇ ІНТЕЛЕКТУАЛЬНОГО ЗАХИСТУ КРИТИЧНО ВАЖЛИВИХ ОБ’ЄКТІВ

4.1. Технічні засоби захисту критично важливих об’єктів

Технічні засоби захисту критично важливих об'єктів є невід'ємною частиною системи безпеки. Вони забезпечують базовий рівень захисту від фізичних загроз і допомагають забезпечити стабільну роботу критичної інфраструктури.

Інтеграція технічних, структурних та оперативних заходів дозволяє створити комплексну систему захисту, здатну протистояти сучасним загрозам.

Однак для досягнення максимальної ефективності необхідно постійно вдосконалювати засоби захисту, адаптуючи їх до нових викликів та загроз. Технічні захисту критично важливих об’єктів повинні мати такі функції:

1. Виявлення загроз, таких як проникнення, пожежа, витоки газу.
2. Генерація звукових і світлових сигналів для сповіщення про загрозу. Швидке сповіщення відповідних служб або персоналу через SMS, електронну пошту, мобільні додатки або автоматичні дзвінки.
3. Автоматичне виявлення підозрілих дій або поведінки за допомогою технологій відеоаналізу. Моніторинг і запис подій в режимі реального часу.
4. Автоматизоване управління доступом за допомогою карток, біометричних даних (відбитки пальців).

Класифікація технічних засобів захисту

Технічні засоби захисту можуть бути класифіковані на декілька категорій: технічні засоби, які включають системи відеоспостереження, сигналізації, системи контролю доступу та інші технічні пристрої та операційні засоби: охоронні послуги, системи протипожежного захисту, регулярні перевірки безпеки.

4.1.1 Вибір системи відео спостереження

Оскільки об'єкти критичної інфраструктури є цільовими для різних типів загроз, система відеоспостереження стає ключовим компонентом комплексного підходу до безпеки.

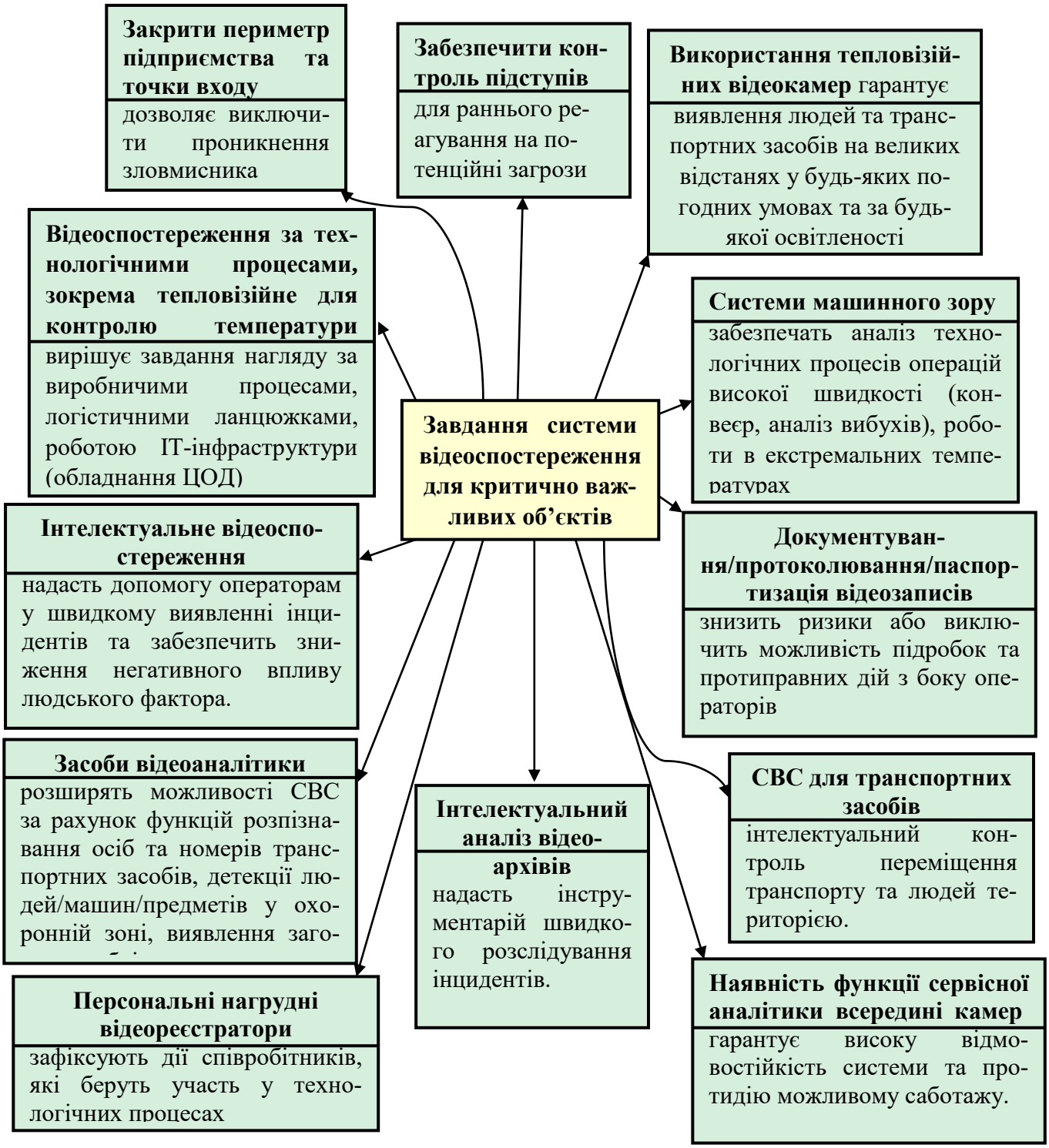


Рис. 4.1. Завдання системи відеоспостереження для критично важливих об'єктів

Звичайно, на об'єктах критичної інфраструктури системи відеоспостереження складають лише частину загальної системи безпеки. Вони працюють у зв'язці з системами контролю доступу, охорони периметра, оповіщення, диспет-

черизації та іншими компонентами. Однак цей список надає вам широкий спектр можливостей, які можна реалізувати з урахуванням конкретних потреб.

Система відеоспостереження є критичним компонентом безпеки на критично важливих об'єктах. Її ефективність залежить від правильної інтеграції компонентів, чіткої схеми побудови та регулярного обслуговування. Вона забезпечує моніторинг, зберігання, обробку і аналіз відеоданих, що сприяє покращенню загальної безпеки і швидкому реагуванню на інциденти.

На Рис.4.2. представлено схему побудови відеонагляду на критично важливих об’єктах.

Рис. 4.2 Схема побудови відеонагляду на критично важливих об’єктах

Сучасні системи відео нагляду включають:

- **IP-камери**: забезпечують високу якість зображення і можуть бути інтегровані з системами управління безпекою.
- **Камери з високою роздільною здатністю**: забезпечують чітке зображення навіть при поганих умовах освітлення.

IP-камера поєднує в собі можливості звичайної камери та міні-комп'ютера, оскільки крім оптики вона обладнана центральним процесором, мережевим модулем, процесором стиснення та пропонує цілу низку інтелектуальних функцій.

Принцип роботи ip-камер

Як і у звичайних камерах, в IP-моделях об'єктив фокусує картинку на матриці, яка у свою чергу перетворює світло на електричний сигнал. Він передається на процесор, що обробляє кольори, яскравість та інші параметри зображення. Після цього відео надходить на компресор, який стискає дані передачі їх через мережевий контролер.

Кожній IP-камері при підключенні надається власна IP-адреса, як і іншим пристроям, які працюють через інтернет. Він необхідний, щоб камера могла синхронізуватися з реєстратором, що відбувається за допомогою спеціальної програми або команди.

Без IP-адреси забезпечити спільну роботу та доступ до камери з мобільних гаджетів буде неможливо.

Основні компоненти IP-камери

1. **Об'єктив**: захоплює зображення.
2. **Сенсор зображення**: перетворює оптичний сигнал в електричний (внутрішній сенсор, наприклад, CMOS або CCD).
3. **Процесор відеообробки**: обробляє дані сенсора і стисне відео.
4. **Мережевий інтерфейс**: для підключення до мережі (Ethernet або Wi-Fi).
5. **Вбудована пам'ять або карта пам'яті**: для зберігання відео або конфігурацій.
6. **Джерело живлення**: заживлює камеру (може бути PoE - Power over Ethernet).
7. **Порти та роз'єми**: для підключення до зовнішніх пристроїв (наприклад, зберігання).

Завдяки наявності цифрових компонентів функціональність IP-камери стає практично безмежною, дозволяючи отримувати доступ до її даних із будь-якої точки планети, де є інтернет.

Для технології інтелектуального захисту критично важливих об’єктів 8 Мп PTZ IP-камера з PoE Reolink RLC-823A (Рис. 4.3).

Рис. 4.3 IP-камера Reolink RLC-823A

Reolink RLC-823A - сучасна IP камера відеоспостереження з роздільною здатністю запису 8 мегапікселів, підключенням по Ethernet, вбудованим PIR датчиком детекції руху, мікрофоном, динаміком, вбудованим прожектором, сиреною, PoE, а також слотом для microSD карт. Живлення: 12 В з наступними функціями – Таблиця 4.1[22].

Таблиця 4.1 – Функції та опис Reolink RLC-823A

Функція	Опис
Технологія Smart Detection	Завдяки вбудованій в камеру технології аналізу форм людей і транспортних засобів, Reolink RLC-823A забезпечує точне виявлення, що значно зменшує кількість помилкових тривог при русі тривіальних об’єктів. Виявлення людей/транспортних засобів. Точні сповіщення.
Подвійне попередження небажаних відвідувачів	Після виявлення зловмисника, прожектори та сирена камери Reolink RLC-823A вмикаються або активуються вручну, щоб попередити потенційного злочинця.
Інтерактивне спілкування в реальному часі	Вбудований мікрофон і динамік дозволяють слухати та говорити з тим, кого зафіксує камера, у режимі реального часу: «привіт» друзям або попередження ворогам.
Точне визначення та відстеження	Завдяки повороту на 360° і нахилу на 90° PTZ Reolink RLC-823A камера дозволяє переглядати світ під будь-яким кутом, а також може автоматично стежити за рухомою людиною. • Автоматичне відстеження; • Ручне панорамування та нахил.
Суперчітке нічне бачення	Reolink RLC-823A з інфрачервоними світлодіодами забезпечує інфрачервоне нічне бачення на відстані 60 метрів, а прожектори забезпечують кольорове нічне бачення. Ідеально підходить для відкритих майданчиків, які не завжди добре освітлені. • 4 ІЧ світлодіоди; • кольорове нічне бачення.
5-кратний оптичний зум для кращої видимості	Моторизований варіофокальний об’єктив камери Reolink RLC-823A забезпечує широкий кут огляду, а 5-кратний оптичний зум дозволяє збільшувати масштаб для дивовижних деталей або зменшувати для максимального охоплення.

Віддалений доступ та управління	Кількома клацаннями в додатку або клієнті Reolink завжди можна залишатися на зв’язку з підприємством. Виявивши щось підозріле, камера Reolink RLC-823A надішле на ваш пристрій миттєве push-повідомлення та електронний лист із знімком виявлення.
Гнучкі можливості зберігання	Ця інтелектуальна IP-камера Reolink RLC-823A підтримує цілодобовий безперервний запис за рухом і за розкладом. Відео можна зберігати на карту micro SD, Reolink NVR або FTP-сервер.

4.1.2 Вибір системи контролю доступу

Системи контролю доступу (СКД) є важливим елементом забезпечення безпеки будь-якої організації, зокрема для захисту критично важливих об'єктів. Вони дозволяють ефективно управляти доступом до приміщень та ресурсів, забезпечуючи контроль і облік переміщень осіб, а також захист від несанкціонованого доступу.

Системи контролю доступу використовуються в різних сферах, включаючи комерційні будівлі, промислові об'єкти, навчальні заклади, медичні установи та інші важливі інфраструктурні об'єкти. Для технології інтелектуального захисту використано 2 види: ідентифікацію по біометричним даним- це відбитки пальців та карткові системи доступу (RFID-мітки). Для ідентифікації по відбитку пальця було обрано біометричний термінал з Bluetooth ZKTeco MA300-BT/ID зі скануванням відбитку пальця і зчитувачем EM карт (Рис. 4.4).

Рис. 4.4 біометричний термінал з Bluetooth ZKTeco MA300-BT/ID

Цей термінал має наступні функціональні особливості:

- режими роботи: автономний / у складі СКУД з підключеним зовнішнім Wiegand обладнанням і контроллерами.
- підтримка Bluetooth-з'єднання для керування за допомогою застосунку ZKBioBT – за допомогою смартфона можна керувати замком, змінювати і додавати інформацію про користувачів, редагувати параметри контролю доступу.
- інтерфейси зв'язку Ethernet TCP/IP і RS485.

- додавання нових користувачів в автономному режимі за допомогою карти адміністратора.
- металевий корпус, клас захисту IP65 з можливістю зовнішнього монтажу.

Для того, щоб записати відбиток пальця або картку у MA300-BT на мобільний телефон треба встановити застосунок ZKBioBT. Після запуску застосунку, бачимо MA300-BT онлайн, додаємо його у систему, а далі можемо або відчинити двері або стати адміністратором системи. Для цього потрібно увійти у меню Setting (Рис. 4.5)

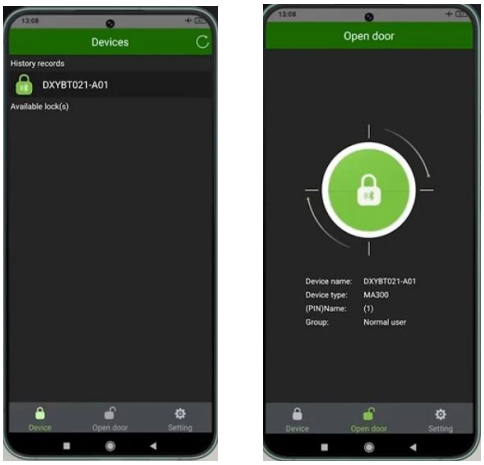


Рис. 4.5 Принцип роботи застосунку ZKBioBT

Далі Supervisor password mode та після запрошення системи створити відбиток адміністратора користувач стає адміністратором системи (Рис.4.6).

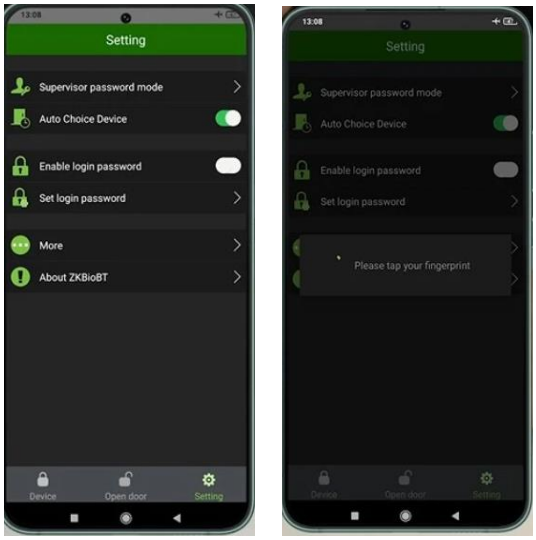


Рис. 4.6 Принцип роботи застосунку ZKBioBT

Теперь у мобільному застосунку маємо створити другого користувача. Для цього переходимо у вкладку User. Далі натискаємо плюс. Всі поля можемо заповнити: User ID, Name, Fingerprint status, Card status (Рис.4.7).

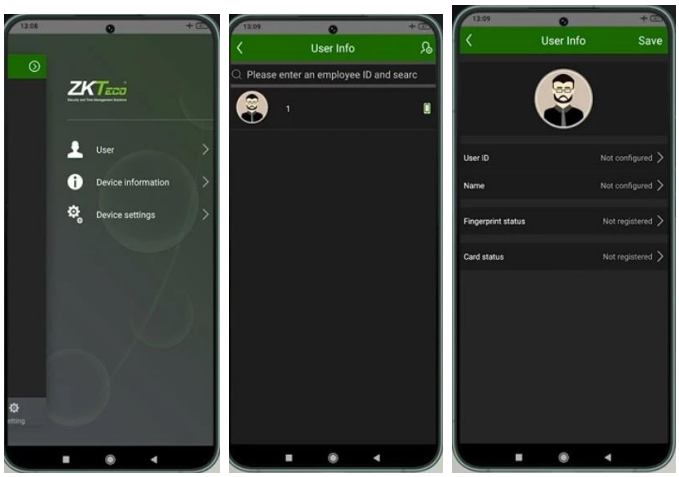


Рис. 4.7 Принцип роботи застосунку ZKBioBT

Наприклад, User ID - ставимо 2, тому що адмін це перший User ID. Name - вводимо ім'я. Натискаємо Fingerprint status, і робимо відбиток. Реєстрацію завершено (Рис. 4.8).

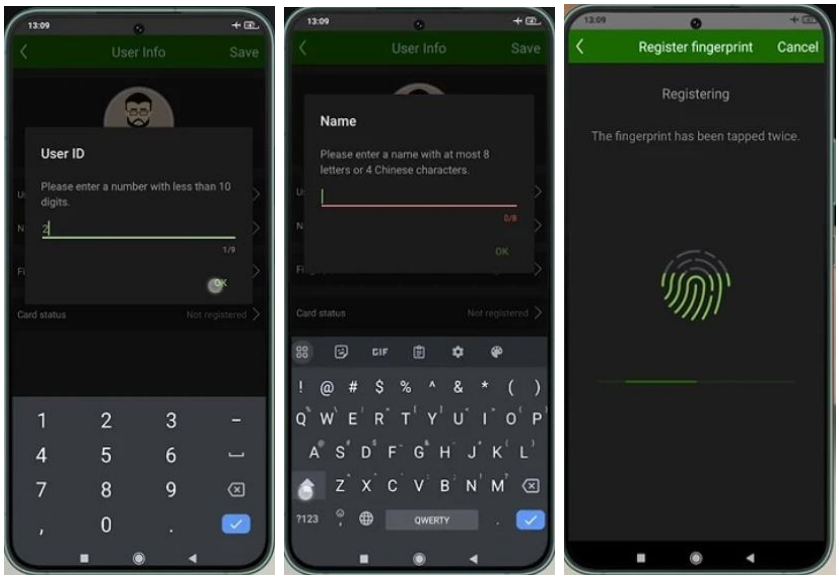


Рис. 4.8 Принцип роботи застосунку ZKBioBT

Цей термінал також підтримує PUSH-протокол ADMS. В такому випадку MA300 може знаходитись в одному місці, а програмне забезпечення ZKBio Time в іншому, і спілкуватися між собою через мережу інтернет [23].

В якості карткової системи доступу було обрано безконтактна RFID-картку ATIS EF-08 - сучасне рішення для систем контролю доступу, яке здатне працювати на двох частотах: EM-Marine 125 кГц і Mifare 13.56 МГц (Рис. 4.9). Ця функціональність робить картку винятково адаптивною до різних систем безпеки. Використання однієї карти замість двох спрощує адміністрування системи, скорочує витрати на обслуговування і підвищує рівень зручності для користувачів.

Рис. 4.9 Безконтактна RFID картка ATIS EF-08 EM-Marine

Картка має розширені можливості безпеки завдяки вбудованій криптографії, що забезпечує надійний захист даних. Можливість програмування картки для виконання різноманітних завдань, наприклад, реєстрації робочого часу або доступу до послуг, посилює її функціональність і робить складовою частиною комплексних систем безпеки.

Основні переваги RFID-картки ATIS EF-08:

1. Двочастотна підтримка: Картка підтримує частоти EM-Marine 125 кГц і Mifare 13.56 МГц, що забезпечує її сумісність з різними системами контролю доступу та усуває необхідність використання кількох карток.

2. Гнучкість використання: Завдяки своїй універсальності, ця картка ідеально підходить для різних організацій, включаючи корпорації, навчальні заклади та державні установи.

3. Покращена безпека: Вбудовані криптографічні функції гарантують захист інформації, що є ключовим для безпеки систем.

4. Зниження витрат: Застосування однієї картки, що підтримує кілька частот, знижує витрати на виготовлення та обслуговування і спрощує адміністративні процеси.

5. Практичність і портативність: Картка має стандартні розміри та легко поміщається в гаманець або на бейдж, роблячи її зручною для щоденного використання [24].

4.1.3. Вибір системи сигналізації та оповіщення

Системи сигналізації допомагають вчасно реагувати на загрози та інциденти. В якості побудови технології інтелектуального захисту було обрано комплект сигналізації із замком: централь Ajax Hub, бездротовий датчик руху Ajax MotionProtect, бездротовий smart замок ATIS SL-01 з кнопкою виходу та пультом, бездротове реле Ajax Relay, блок живлення BGW-122, роз'єм-power ATIS під затискач.

Комплект охоронної сингалізації із замком призначений для організації пультової або автономної охоронної системи, а також контролю доступу. Система побудована на базі централі Ajax Hub, до якої підключаються датчик та реле. При активації реле у програмі на смартфоні можна дистанційно відмикати smart замок.

Замок повністю автономний та самодостатній. Працює від батарейок, керується брелоками на вхід та вихід або кнопкою виходу для відвідувачів. При знятті з охорони Ajax замок також відкриватиметься.

Обрані характеристики наведені в Таблиці 4.2

Таблиця 4.2. – Обрані характеристики охоронної системи

Характеристики централі Ajax Hub	
Максимальна кількість бездротових пристроїв	100 пристроїв
Частота бездротових датчиків	протокол Jeweller (868 МГц)
Канали зв'язку	GSM (850/900/1800/1900 МГц), Ethernet
Вбудований акумулятор	Li-Ion
Ємність вбудованого акумулятора	2 А/ч
Час роботи без електроживлення	до 15 годин
Живлення	110 - 250 В AC
Діапазон робочих температур	-10°C ~ +40 °C
Характеристики датчик руху Ajax MotionProtect white	

Дальність детектування	до 12 м з імунітетом від тварин. Піросенсор Hi-End від компанії Excelitas
Лінза	Лінза Френеля із запатентованого матеріалу POLY IR, затримує біле світло і пропускає інфрачервоне
Частота	868-868.6 МГц. Період опитування датчиків: 10 – 300 секунд
Зв'язок	2-х сторонній зв'язок
Дальність	1700 м на відкритому просторі

Характеристики бездротового smart замка ATIS SL-01	
Спосіб встановлення	накладний
Робоча частота	433 МГц
Дальність зв'язку	30 м
Живлення	замок 2 батареї AA, кнопка виходу 1 літієва батарея 2032, пульт 1 літієва батарея 2032
Споживання в режимі очікування	до 10 мкА
Споживання у робочому режимі	замок до 42 мА, кнопка виходу до 3 мА, пульт до 3 мА
Робоча температура замка	-20°C~+60°C

Характеристики реле Ajax Relay	
Дальність зв'язку з Ajax Hub	до 1000 м за умови прямої видимості
Діапазон робочої напруги	DC 7—24 В
Захист по напрузі	min — 6.5 В, max — 36.5 В
Максимальний струм навантаження	5A@24В DC, 13A@230В AC
Вихідна потужність	до 3 кВт
Частота	868—868.6 МГц
Клас захисту	IP20

Характеристики роз'єму-power ATIS під затискач (мама)	
Тип роз'єму	DC
Тип з'єднання	сухий контакт
Матеріал корпусу	пластик
Максимальна напруга	250 В
Граничний струм	2
Ізоляційний опір	не менше 50 мОм
Опір на контактах	до 0.02 Ом
Робоча температура	-35°C~+85°C

Блок живлення обраний BGW-122, роз'єм живлення, з виходом +12 В/2 А, вхід ~220 В, клемник.

На Рис. 4.10 представлений обраний комплект сигналізації із замком.

Рис. 4.10 Комплект сигналізації із замком

4.1.4 Вибір протипожежної системи

Системи протипожежного захисту включають в себе:

- Пожежні сигналізації: автоматичне виявлення диму або тепла.
- Вогнегасники та системи спринклерів: для гасіння пожеж.

В якості протипожежної охорони було обрано ППК Артон 08П (Рис. 4.11). ППК "АРТОН-08П" призначений для організації централізованої та автономної охорони різних об'єктів від пожеж, шляхом цілодобового контролю стану до 8-ми шлейфів пожежної сигналізації. Середнє напрацювання на відмову приладу не менше 40000 годин. Кожен з ШС приладів може бути налаштований споживачем як пожежний ШС без верифікації, з верифікацією, або зі спрацюванням двох сповіщувачів, а також можуть бути встановлені залежності типів А, В, С (згідно з вимогами ДСТУ EN-54-2:2003/Зміна №1).

Прилади визначають і відображають наступні стани ШС: «Черговий режим», «Увага» (спрацювання першого сповіщувача в ШС), «Пожежа», «Несправність - коротке замикання», «Несправність - обрив», «ШС відключений», «Несправність одного з інтелектуальних сповіщувачів в ШС».

Рис. 4.11 ППК "АРТОН-08П"

4.2. Фізичні засоби захисту критично важливих об’єктів

Фізичні засоби захисту є першою лінією оборони для критично важливих об'єктів, таких як енергетичні станції, транспортні інфраструктури, фінансові установи та державні об'єкти. Вони спрямовані на запобігання несанкціонованому доступу, захист територій та об'єктів, а також на забезпечення безпеки персоналу.

В якості фізичних засобів зазвичай застосовуються паркани, стіни, загородження, бар’єри і т.д. Все ці є ненадійними методами. Для розробки технології інтелектуального захисту критично важливих об’єктів пропонується використання безпілотних літальних апаратів (БПЛА) для захисту периметру критичних об’єктів.

Безпілотні літальні апарати (БПЛА) надають ряд переваг у порівнянні з традиційними системами безпеки, таких як розширене покриття, швидший час реагування та зменшення витрат [28]. Для фахівців у сфері фізичної безпеки впровадження дронів у їх стратегії може забезпечити суттєву конкурентну перевагу та створити нові можливості.

Нижче розглянемо 5 основних переваг використання дронів для охорони периметра.

1. Поліпшене покриття

Однією з найбільш істотних переваг використання дронів для охорони периметра є можливість забезпечити ширше охоплення контрольованої території. Дрони можуть літати на різній висоті та під різними кутами, що дозволяє їм робити кадри з місць, куди важко чи неможливо дістатися за допомогою традиційних засобів безпеки. В результаті дрони можуть забезпечити більш повний огляд периметра та більш ефективно виявляти потенційні загрози безпеці.

2. Швидший час відгуку

Дрони можуть реагувати на інциденти безпеки набагато швидше, ніж працівники охоронної служби. Щойно потенційну загрозу виявлено, дрон може швидко переміститися на місце та оцінити ситуацію, надаючи інформацію в режимі реального часу командам безпеки. Це дозволяє персоналу служби безпеки реагувати швидше та ефективніше, потенційно запобігаючи порушенням безпеки або зводячи до мінімуму збитки, спричинені такими інцидентами.

Зниження витрат

Дрони можуть стати економічно ефективною альтернативою традиційним заходам безпеки. Використовуючи дрони, фахівці фізичної безпеки можуть скоротити потребу в дорогих людських ресурсах, таких як охоронці. Крім того, дрони можуть забезпечувати цілодобове спостереження, зменшуючи потребу в кількох змінах служби безпеки та знижуючи загальні експлуатаційні витрати.

4. Гнучкість

Дрони можна швидко і легко розгорнути, що робить їх ідеальними для забезпечення безпеки у різних сценаріях. Їх можна використовувати для безпеки різних заходів, охорони будівельних майданчиків, захисту критичної інфраструктури та багатьох інших об’єктів. Крім того, дрони можна запрограмувати на виконання певних траєкторій польоту або патрулювання певних територій, що забезпечує підвищену гнучкість та налаштування.

5. Підвищена безпека

Дрони можуть використовуватися для забезпечення безпеки в небезпечних або важкодоступних місцях, знижуючи ризик для працівників служби безпеки. Наприклад, дрони можуть контролювати райони, схильні до стихійних лих, такі як області, схильні до повеней або землетрусів. Це може допомогти забезпечити безпеку працівникам служб надзвичайних ситуацій та знизити ризик травм або загибелі людей [25].

Використання дронів для охорони периметра має свої плюси і мінуси. Дрони забезпечують покращене покриття, швидший час реагування, зменшення вит-

рат, більшу гнучкість і підвищену безпеку, але водночас мають обмеження, такі як короткий час польоту, залежність від технологій, погодні умови, питання конфіденційності та нормативні обмеження.

Що стосується технології, важливо враховувати тип дрона, який використовується. Наприклад, хоча дистанційно керовані дрони є популярними, деякі провідні компанії також пропонують автономні моделі.

Інтегратори фізичної безпеки повинні ретельно проаналізувати ці аспекти перед тим, як включати дрони у свої системи. Правильне планування та впровадження можуть дати значну конкурентну перевагу та підвищити ефективність безпекових рішень. На Рис. 4.12. представлено зображення з БПЛА та сам квадрокоптер дрон DJI Matrice 350 RTK Enterprise + DJI Zenmuse H20T (Рис. 4.13), який був обраний для інтелектуального захисту критично важливих об’єктів.

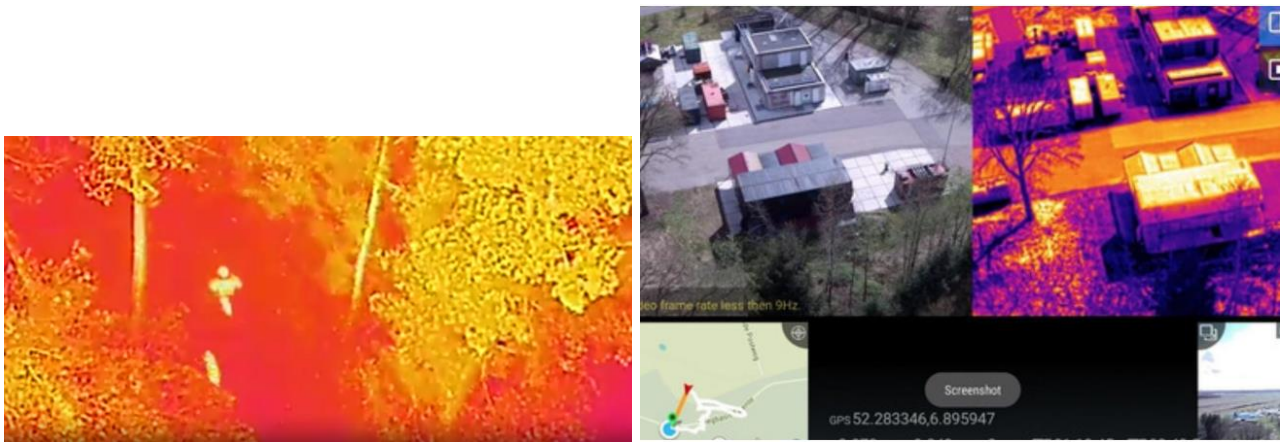


Рис. 4.12 Зображення з БПЛА для захисту периметру об’єкта

Рис. 4.13 Квадрокоптер дрон DJI Matrice 350 RTK Enterprise + DJI Zenmuse H20T

Дрон патрулює периметр об’єкта цілодобово та передає всю необхідну інформацію оператору, який аналізує її та приймає відповідні рішення [26].

4.3. Вибір фреймворків та механізмів для захисту об'єкта

Вибір оптимального фреймворку для захисту критичного об'єкта енергетичної системи залежить від кількох ключових факторів:

- Складність інфраструктури: Критичні об'єкти в енергетичних системах часто мають складну інфраструктуру, що включає різноманітні системи та компоненти, такі як системи управління, системи безпеки, підстанції, центри керування енергосистемою, комунікаційні системи тощо.
- Рівень загроз: Оскільки критичні об'єкти є привабливою мішенню для кіберзлочинців, важливо вибрати фреймворк, здатний ефективно протистояти сучасним кіберзагрозам.
- Фінансові та людські ресурси: Впровадження та підтримка фреймворку потребують відповідних фінансових і людських ресурсів [29]. Цей аспект також слід враховувати при виборі найбільш підходящого фреймворку.

Враховуючи ці фактори найкращим фреймворком для захисту критичного об’єкту енергосистеми можна обрати Mitre ATT&CK [30]. Це фреймворк, який описує різні етапи атаки на IT-інфраструктуру, починаючи від розвідки та закінчуючи діями після компрометації. Кожен етап атаки відповідає певній тактиці, а кожна тактика включає кілька технік, які використовуються для досягнення мети. Наприклад, тактика Initial Access (Початковий Доступ) може включати техніки Spearphishing Attachment (цільовий фішинг), Drive-by Compromise або Exploit Public-Facing Application (Експлуатація Публічного Додатка). MITRE ATT&CK надає детальну інформацію про кожну тактику та техніку, включаючи опис, приклади використання, засоби виявлення та запобігання [].

Принцип роботи MITRE ATT&CK заснований на тому, що зловмисники зазвичай використовують ті самі тактики і техніки для атаки на різні IT-інфраструктури. Це дозволяє фахівцям з кібербезпеки аналізувати поведінку противника, визначати його вразливість та слабкі місця, а також розробляти ефективні заходи захисту. MITRE ATT&CK допомагає фахівцям з кібербезпеки розуміти логіку та мотивацію супротивника, а також передбачати його наступні кроки [27].

Матриці MITRE ATT&CK складені для трьох сегментів: інформаційних інфраструктур підприємств (Enterprise), мобільних пристроїв на базі операційних систем Android та iOS, а також промислових систем керування (ICS). У свою чергу, матриця для сегменту Enterprise містить інформацію про тактики та техніки, які застосовуються при розвідці та атаках проти інфраструктур на базі Windows, Linux та macOS, а також хмарних, контейнерних та мережевих.

На Рис. 4.14. наведена сегментація матриць MITRE ATT&CK залежно від сфери застосування.

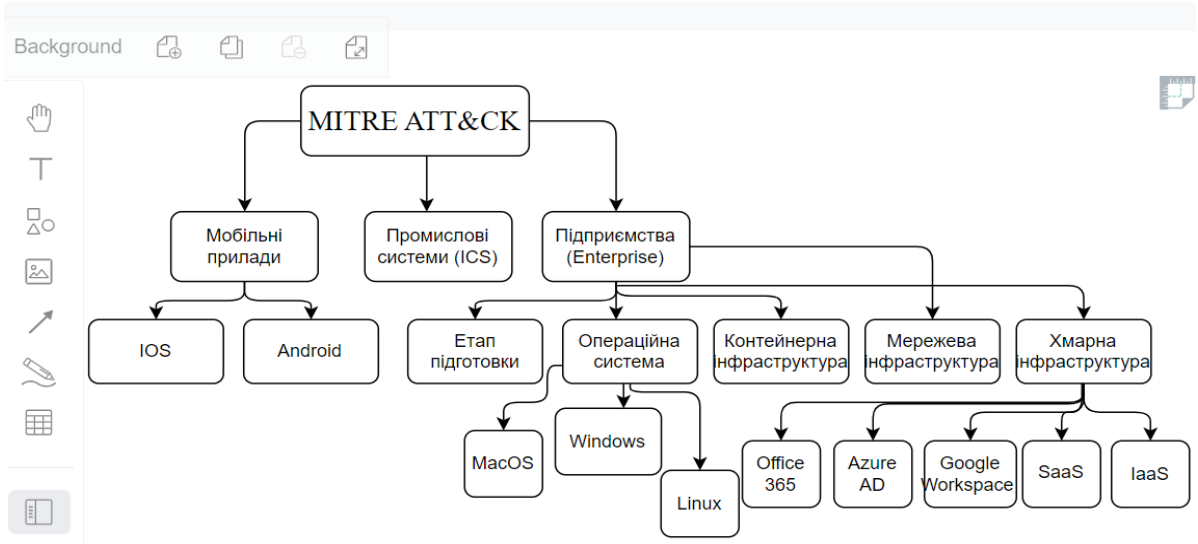


Рис. 4.14. Сегментація матриць MITRE ATT&CK залежно від сфери застосування

Якщо розглядати MITRE ATT&CK комплексно, то це не тільки матриці тактик і технік, але також інформація про джерела даних, що застосовуються для виявлення дій кіберзлочинців, про способи зниження ризиків в інформаційній безпеці, про злочинні угруповання, шкідливі програми, що ними використовуються, і хакерські кампанії.

Матриці MITRE ATT&CK складаються із двох сутностей: тактик та технік. Тактики визначають мету, якої атакуючі хочуть досягти шляхом використання певних технік та процедур, які також називають підтехніками [31].

Графічне представлення матриці тактик и технік MITRE ATT&CK для сегмента Enterprise наведено на Рис. 4.15.

Матриця ATT&CK організована у вигляді таблиці, де:

- Рядки представляють тактики.
- Стовпці представляють техніки і, в деяких версіях, підтехніки.

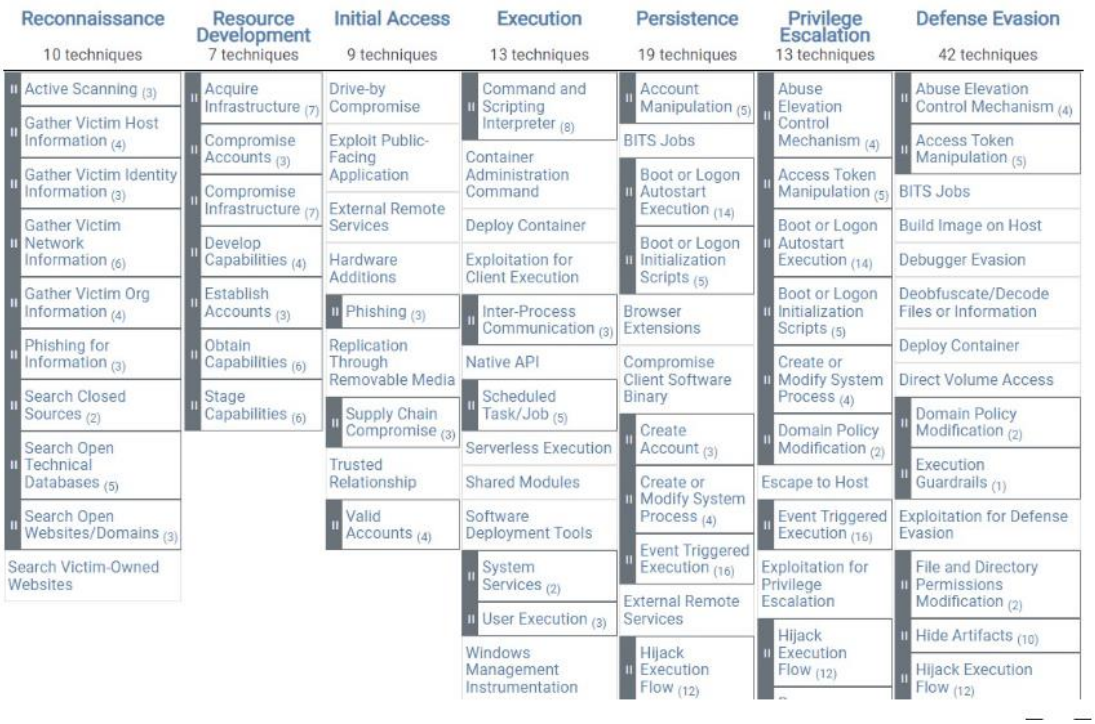


Рис. 4.15 Матриця тактик і технік MITRE ATT&CK для сегмента Enterprise

На рис. 4.16 представлено процес моделювання векторів атак на компанію за допомогою ATT&CK Navigator. MITRE ATT&CK Navigator — це інтерактивний інструмент, який допомагає в моделюванні, аналізі та візуалізації векторів атак, використовуючи базу знань MITRE ATT&CK [32].

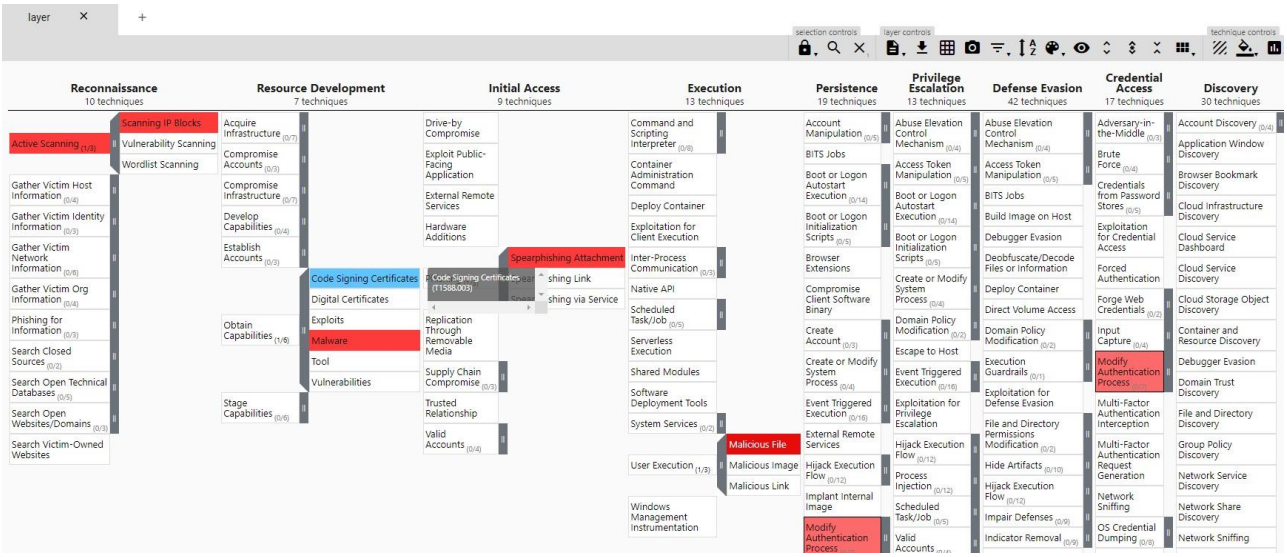


Рис. 4.16 Процес моделювання векторів атак на компанію за допомогою ATT&CK

Цей інструмент дозволяє здійснити аналіз векторів атак [33]. Це включає в себе перевірку взаємозв'язків між техніками, виявлення потенційних шляхів атаки і оцінку ймовірності використання певних технік.

4.4. Технологія інтелектуального захисту критично важливих об’єктів

Технологія інтелектуального захисту критично важливих об'єктів представляє собою передовий підхід до забезпечення безпеки стратегічних інфраструктур, таких як енергетичні станції, фінансові установи та транспортні системи. Вона об'єднує сучасні технології, включаючи штучний інтелект, машинне навчання, аналітику великих даних та інтеграцію інформаційних і операційних технологій, для створення комплексних і адаптивних систем захисту [34].

Основні переваги інтелектуального захисту включають проактивний підхід до виявлення і запобігання загрозам, автоматизацію процесів реагування, а також можливість глибокого аналізу загроз і вразливостей. Це дозволяє знижувати ризики, підвищувати ефективність захисних заходів і забезпечувати високу надійність критично важливих об'єктів. Інтеграція з інформаційними і операційними технологіями забезпечує комплексний підхід до захисту, що охоплює як цифрові, так і фізичні аспекти безпеки [35,36]. Технології виявлення та реагування на інциденти, а також системи оцінки ризиків і уразливостей, допомагають організаціям своєчасно і ефективно реагувати на нові загрози.

Однак, незважаючи на численні переваги, інтелектуальний захист також має свої виклики [37]. Складність інтеграції різних технологій, необхідність постійного оновлення і адаптації до нових загроз, а також вимоги до ресурсів для підтримки систем можуть становити серйозні труднощі.

Отже, впровадження технологій інтелектуального захисту є важливим кроком для забезпечення безпеки критично важливих об'єктів у сучасному світі. При належному плануванні, ресурсному забезпеченні і регулярному оновленні систем, ці технології можуть забезпечити значну перевагу в захисті від кіберзагроз і фізичних атак, сприяючи стабільності і безпеці [38,39].

На Рис. 4.17. представлено технологію інтелектуального захисту критично важливих об’єктів.

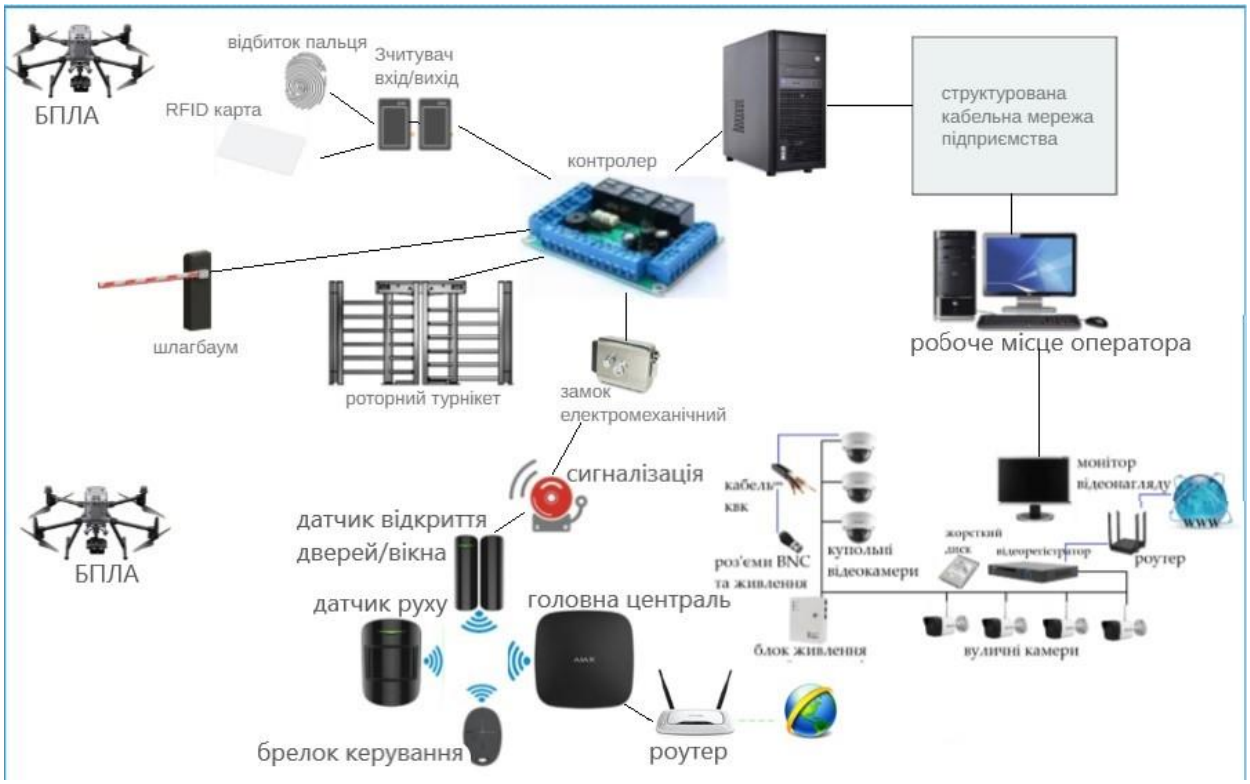


Рис. 4.17 Технологія інтелектуального захисту критично важливих об’єктів

Ця схема є загальним уявленням про те, як різні компоненти інтелектуального захисту критично важливих об'єктів можуть бути інтегровані для забезпечення комплексного захисту. Вона демонструє основні елементи системи і їх зв'язок, що дозволяє розробити ефективну стратегію безпеки для критичних інфраструктур. Ця схема може варіюватися в залежності від специфічних вимог, компонентів системи та самого об’єкта. Загалом, технологія інтелектуального захисту критично важливих об’єктів забезпечує всебічний підхід до управління безпекою і дозволяє ефективно протидіяти сучасним загрозам [40]. Правильне впровадження і постійне вдосконалення цієї технології можуть суттєво підвищити рівень безпеки і зменшити ризики для стратегічних інфраструктур.

Висновок

У сучасному світі, де технології розвиваються з неймовірною швидкістю, ми стикаємося як з безмежними можливостями, так і з новими викликами. Одним з найважливіших аспектів нашого часу є захист критично важливих об'єктів, які становлять основу інфраструктури будь-якої країни [41]. Це можуть бути енергетичні системи, транспортні мережі, фінансові установи та комунальні системи. Їх надійність і безперебійна робота мають вирішальне значення для стабільності національної економіки і безпеки суспільства.

Дослідження показали, що технології інтелектуального захисту є ключовими для впровадження ефективних рішень проти сучасних загроз. Вони постійно вдосконалюються у відповідь на нові виклики, включаючи як технічні, так і організаційні аспекти. Інтелектуальний захист охоплює широкий спектр методів, таких як моніторинг і виявлення загроз, управління ризиками, системи резервування і відновлення після аварій, а також навчання і підготовка персоналу [42].

Важливим є також інтеграція цих рішень у вже існуючу інфраструктуру, що дозволяє забезпечити їхню ефективність на всіх рівнях управління. Зокрема, стратегічний підхід до захисту критично важливих об'єктів не є просто технічною задачею; це питання національної безпеки та економічної стабільності.

Сьогоднішні зміни і зростання загроз вимагають постійного вдосконалення підходів до захисту. Ефективні рішення у сфері інтелектуального захисту є необхідними для забезпечення безпеки і стабільності в умовах постійних змін. Розглянуті методи, розроблені моделі, алгоритми і стратегії служать основою для подальшого розвитку і вдосконалення систем захисту, забезпечуючи не лише технологічну ефективність, але й загальну безпеку суспільства.

Таким чином, наше розуміння і впровадження технологій інтелектуального захисту стане ключем до стабільного і безпечного майбутнього, де критично важливі об'єкти будуть захищені від сучасних загроз і викликів.

Список використаних джерел

1. Закон України від 05.10.2017 № 2163-VIII Критично важливі об'єкти інфраструктури [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/TM059785

2. Хоружий О. С., Усачов Д. В. Визначення основних критеріїв захисту об’єктів критичної інфраструктури в умовах воєнного стану [Електронний ресурс] // Електронний репозитарій Національного університету цивільного захисту України (eNUCPUIR). – Режим доступу: http://repositsc.nuczu.edu.ua/bitstream/123456789/17402/1/Теза%20к-т%20Хоружий%20О.С.%20Секція%201.pdf

3. Інфраструктура (Infrastructure) [Електронний ресурс]. – Режим доступу: http://economicdefinition.com/Plants_and_soobruzheniya/Infrastruktura_Infrastructure_eto.html

4. Єрменчук О. П. Сутність та зміст поняття "інфраструктура" в контексті захисту критичної інфраструктури // Бюлетень Міністерства юстиції України. – 2017. – № 6. – С. 35–41.

5. Кодекс цивільного захисту України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/5403-17

6. UNISDR. (2009, May). 2009 UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction [Електронний ресурс]. – Режим доступу: http://www.unisdr.org/files/7817UNISDRTerminologyEnglish.pdf

7. Іваненко О. І. Підхід до національної оцінки ризиків для критичної інфраструктури // Вісник ХНТУ. – 2020. – № 2 (73). – С. 9–22.

8. Sendai Framework for Disaster Risk Reduction 2015–2030 [Електронний ресурс]. – Режим доступу: http://www.unisdr.org

9. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні / Д. С. Бірюков, С. І. Конд-

ратов, О. І. Насвіт, О. М. Суходоля. – Київ : Національний інститут стратегічних досліджень, 2015. – 35 с.

10. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – Київ : НІСД, 2012. – 96 с.

11. Скіцько О. І. Використання ШІ для захисту об'єктів критичної інфраструктури : зб. матеріалів V Міжнар. наук.-практ. конф. «Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2024)», 18–19 квіт. 2024 р. – Черкаси : Черкаський національний університет імені Богдана Хмельницького, 2024. – С. 319.

12. Aggarwal C. C. Neural Networks and Deep Learning: A Textbook. – 1st ed. – Springer, 2018. – 520 p.

13. Ji S., Xu W., Yang M., Yu K. 3D Convolutional Neural Networks for Human Action Recognition // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2013. – Vol. 35, Issue 1. – P. 221–231.

14. Scikit-Learn. Supervised learning [Електронний ресурс]. – Режим доступу: https://scikitlearn.org/stable/supervised_learning.html#supervised-learning

15. Майба М. А., Єременко О. С. Розв’язання задачі класифікації мережних пристроїв на основі параметрів безпеки за допомогою машинного навчання // Проблеми телекомунікацій. – 2023. – № 2 (33). – С. 44–61.

16. Волос І. П. Алгоритми захисту даних в мережах Інтернет – речей : кваліфікац. робота на здобуття освіт. ступеня «магістр». – Тернопіль, 2023 [Електронний ресурс]. – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/50187/1/КР_Волос.pdf

17. Кібератаки російської федерації. Хронологія [Електронний ресурс] // Міністерство оборони України. – Режим доступу: https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federacziihronologiya.html (дата звернення: 31.09.2024).

18. Єрменчук О. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки // Jurnalul juridic national: teorie şi practică. – 2018. – № 6 (34). – С. 50–54.

19. Учасники проектів Вікімедіа. Фішинг [Електронний ресурс] // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Фішинг (дата звернення: 31.09.2024).

20. Учасники проектів Вікімедіа. Соціальна інженерія (безпека) [Електронний ресурс] // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека (дата звернення: 31.09.2024).

21. Інжиєвський О. О. Підвищення ефективності методів протидії кібератакам на об'єкти критичної інфраструктури : кваліфікац. робота на здобуття освіт. ступеня «магістр». – Житомир, 2023 [Електронний ресурс]. – Режим доступу: http://ir.polissiauniver.edu.ua/bitstream/123456789/15178/1/INZHYEVSKIY_OO_KR_125_2023.pdf (дата звернення: 31.09.2024).

22. Keenetic. Сегменти мережі [Електронний ресурс]. – Режим доступу: https://help.keenetic.com/hc/uk/articles/360005236300-Сегменти-мережі

23. bezpeka.club. Камери відеонагляду Reolink. 8 Мп PTZ IP-камера з PoE Reolink RLC-823A [Електронний ресурс]. – Режим доступу: https://bezpeka.club/reolink-rlc-823a

24. ZKTeco MA300-BT - Біометричний термінал зі скануванням відбитку пальця і зчитувачем EM карт [Електронний ресурс] // bezpeka-shop.com. – 2023. – Режим доступу: https://www.bezpeka-shop.com/ua/blog/videoobzor/zkteco-ma300-bt-biometricheskiy-terminal-so-skanirovaniem-otpechatka-paltsa-i-schityvatelem-em-kart/

25. Безконтактна RFID картка ATIS EF-08 EM-Marine 125 кГц + Mifare 13.56 МГц [Електронний ресурс] // bezpeka-shop.com. – 2023. – Режим доступу: https://www.bezpeka-shop.com/ua/product/ef-08/

26. Bezpeka.club. Переваги та недоліки застосування дронів для охорони периметра [Електронний ресурс]. – 2023. – Режим доступу:

https://bezpeka.club/perevagy-ta-nedoliky-zastosuvannya-droniv-dlya-ohorony-perymetra

27. Рішення для безпілотної охорони об'єктів [Електронний ресурс]. – Режим доступу: https://stantsiadroniv.com.ua/services/rishennia-dlia-bezpilotnoi-okhorony-ob-iektiv/

28. Як використовувати MITRE ATT&CK для побудови захищеної IT-інфраструктури: практичний посібник [Електронний ресурс] // SecurityLab. – 2023. – Режим доступу: https://www.securitylab.ru/analytics/538716.php

29. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (CSF 2.0) [Електронний ресурс]. – 2024. – Режим доступу: https://www.nist.gov/cyberframework

30. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations [Електронний ресурс]. – 2020. – Режим доступу: https://csrc.nist.gov

31. NIST Special Publication 800-82 Rev. 3. Guide to Industrial Control Systems (ICS) Security [Електронний ресурс]. – 2024. – Режим доступу: https://csrc.nist.gov

32. ENISA. Protecting Critical Infrastructure from Cyber Threats. – European Union Agency for Cybersecurity, 2023 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu

33. ENISA. AI Cybersecurity Challenges [Електронний ресурс]. – 2021. – Режим доступу: https://www.enisa.europa.eu

34. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. – ISO, 2022.

35. ISO/IEC 27005:2022. Information Security Risk Management. – ISO, 2022.

36. MITRE Corporation. MITRE ATT&CK for Critical Infrastructure [Електронний ресурс]. – 2024. – Режим доступу: https://attack.mitre.org

37. MITRE Corporation. Zero Trust Architecture Framework [Електронний ресурс]. – 2023. – Режим доступу: https://www.mitre.org

38. Європейська Комісія. Directive (EU) 2022/2555 (NIS2 Directive) [Електронний ресурс]. – 2022. – Режим доступу: https://eur-lex.europa.eu

39. UK National Cyber Security Centre (NCSC). Securing Industrial Automation and Control Systems [Електронний ресурс]. – 2023. – Режим доступу: https://www.ncsc.gov.uk

40. IBM Security. AI-Powered Threat Detection for Critical Infrastructure [Електронний ресурс]. – 2024. – Режим доступу: https://www.ibm.com/security

41. Palo Alto Networks. AI and Machine Learning in Cybersecurity [Електронний ресурс]. – 2023. – Режим доступу: https://www.paloaltonetworks.com

42. Sarker I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions // SN Computer Science. – 2021.

ДОДАТОК А

Слайди презентації

Рис. А.1 Перший слайд

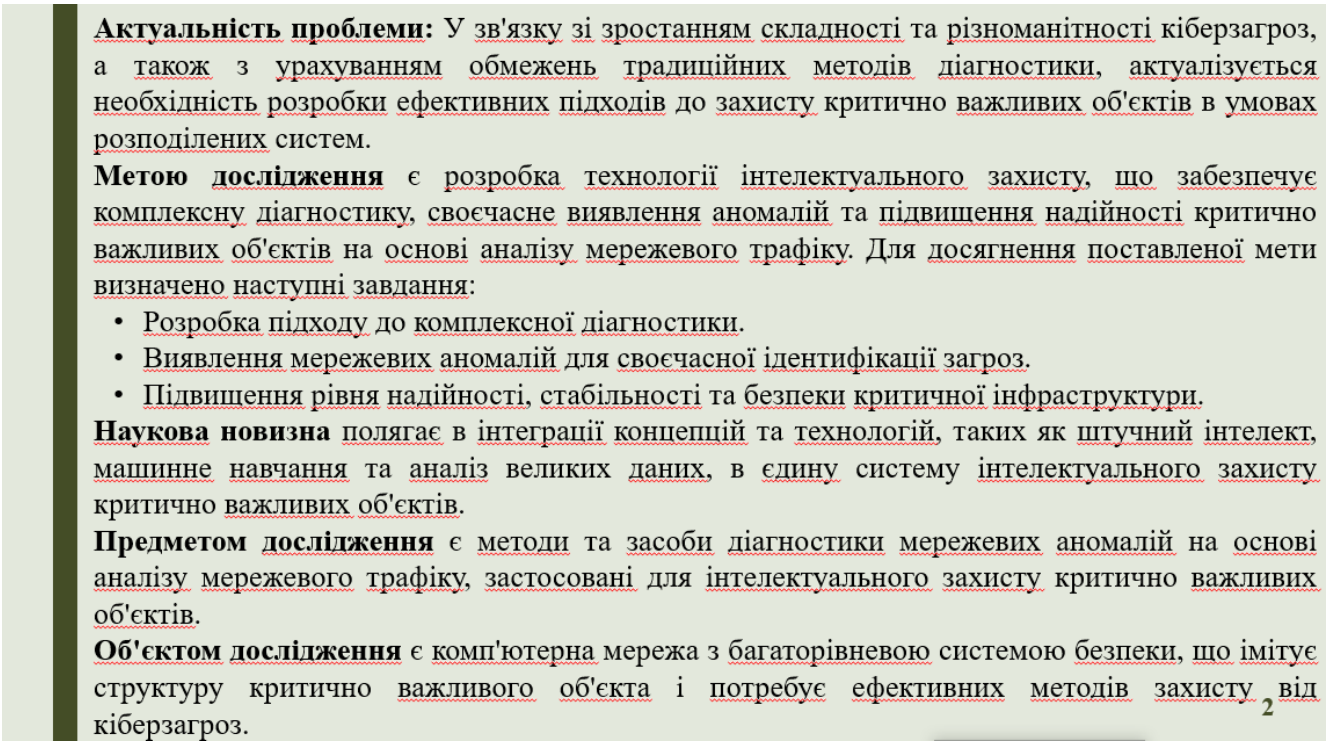


Рис. А.2 Другий слайд

Рис. А.3 Третій слайд

Рис. А.4 Четвертий слайд

Рис. А.5 П’ятий слайд

Рис. А.6 Шостий слайд

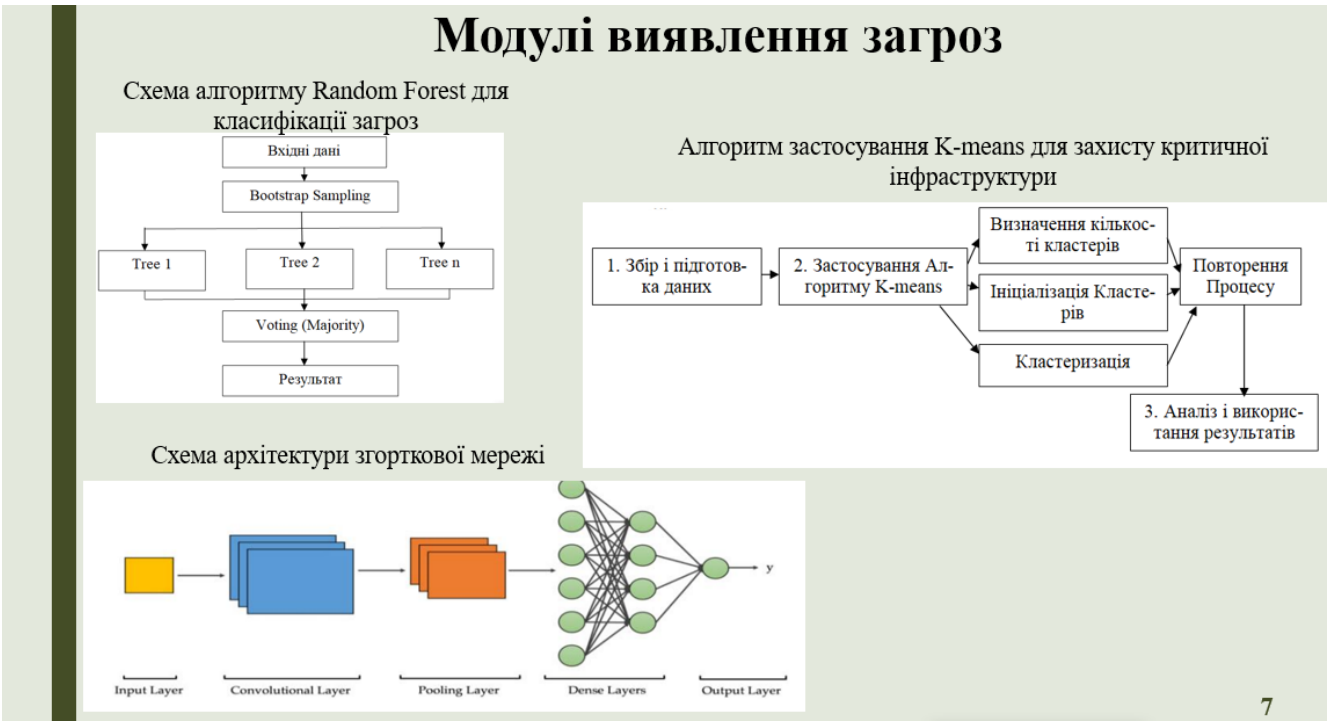


Рис. А.7 Сьомий слайд

Рис. А.8 Восьмий слайд

Рис. А.9 Дев’ятий слайд

Рис. А.10 Десятий слайд

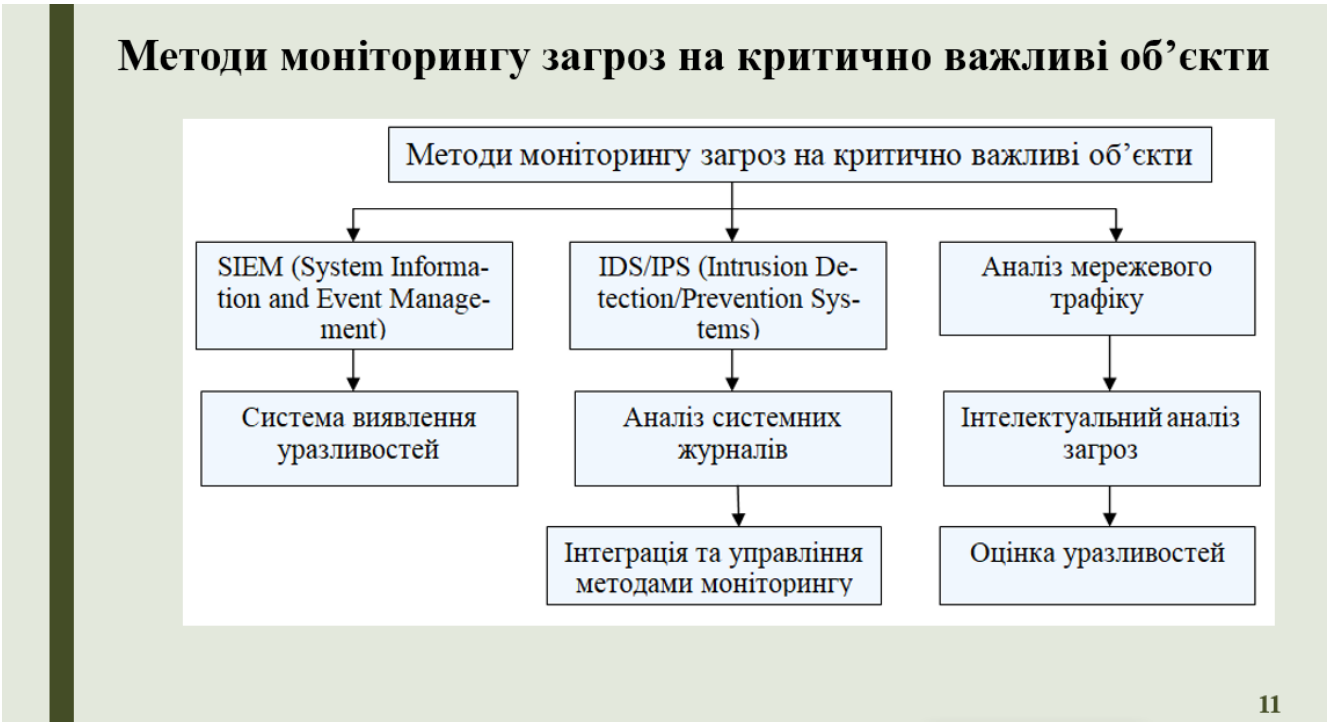


Рис. А.11 Одинадцятий слайд

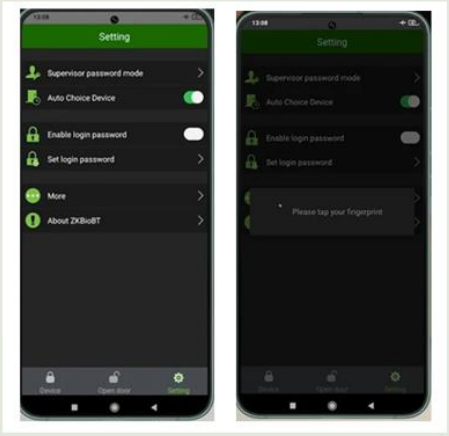
Рис. А.12 Дванадцятий слайд

Рис. А.13 Тринадцятий слайд

Рис. А.14 Чотирнадцятий слайд

Ідентифікація за відбитком пальця

застосунок ZKBioBT

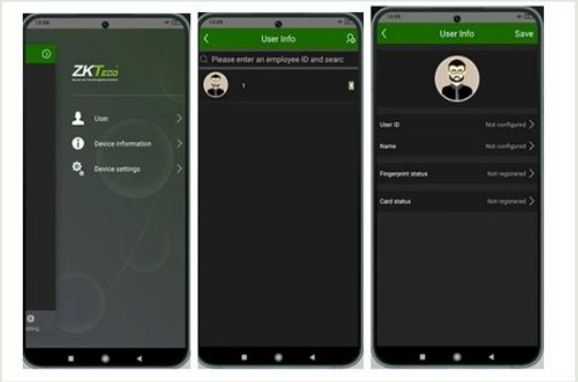


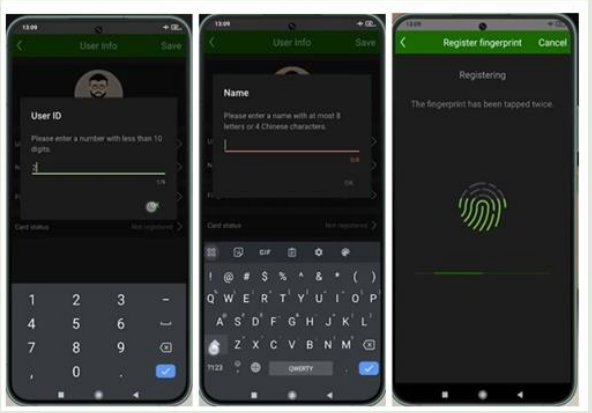
біометричний термінал з Bluetooth ZKTeco MA300-BT/ID

15

Рис. А.15 П’ятнадцятий слайд

Ідентифікація за відбитком пальця





16

Рис. А.16 Шістнадцятий слайд

Рис. А.17 Сімнадцятий слайд

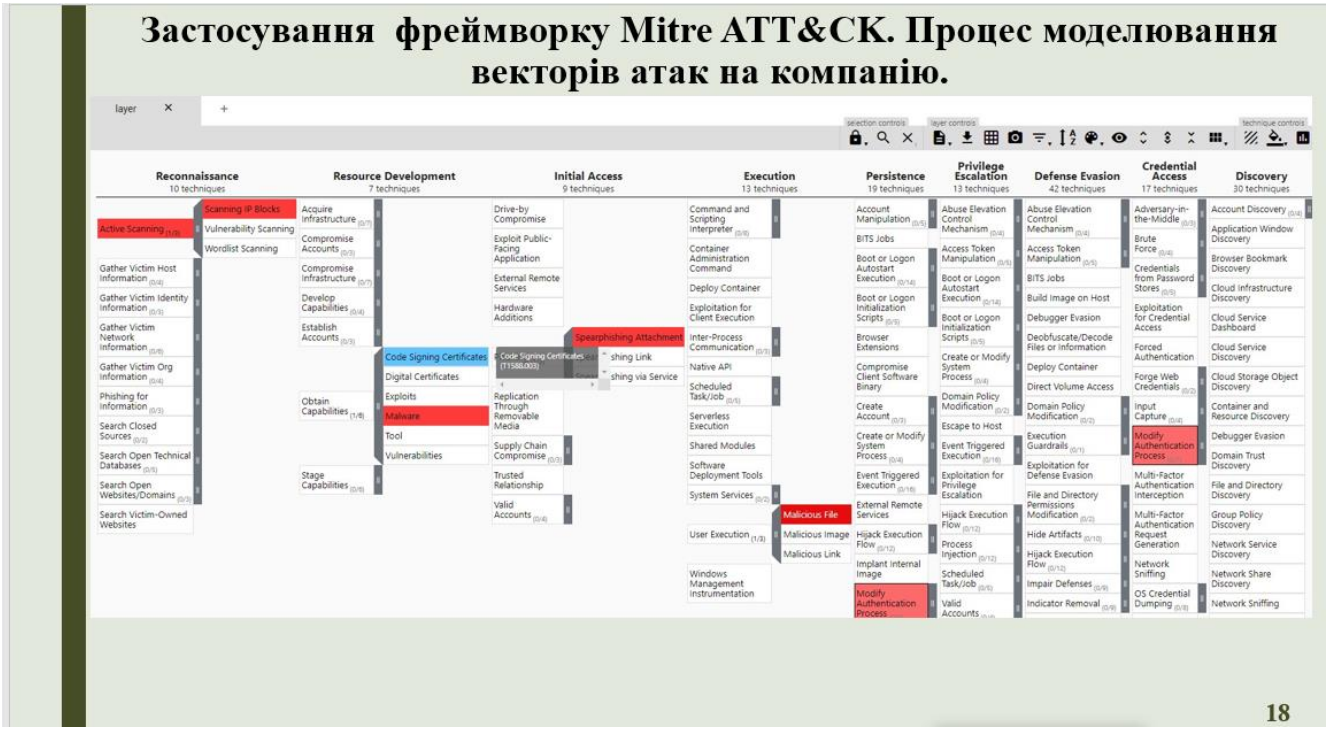
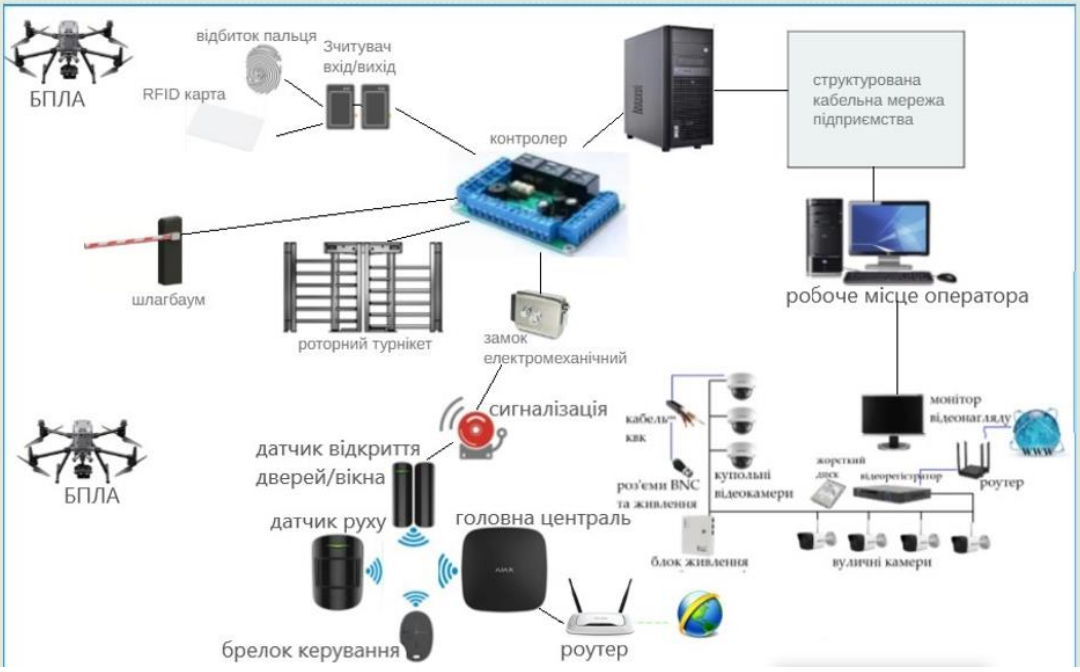


Рис. А.18 Вісімнадцятий слайд

Технологія інтелектуального захисту критично важливих об’єктів



19

Рис. А.19 Дев’ятнадцятий слайд

Висновки

-Проведено класифікацію критично важливих об’єктів (КВО)

- Визначені потенційні впливи на КВО.

-Розроблена схема архітектури системи інтелектуального захисту КВО.

-Представлена архітектура системи штучного інтелекту для захисту КВО.

- Описаний алгоритм K-means та Random Forest для класифікації загроз.

-Запропоновано застосування IOT в системах інтелектуального захисту КВО.

-Розроблені моделі атак та визначені методи моніторингу загроз.

-Розроблений алгоритм реагування на інциденти загроз на критичну інфраструктуру.

-Здійснено вибір технічних засобів (система відеоспостереження, система керування доступом, сигналізація та оповіщення, протипожежна система), фізичних засобів захисту КВО – застосування БПЛА для охорони периметру об’єкта,

-Вибір фреймворків та механізмів для захисту КВО (MITRE ATT&CK) та розроблена сама технологія інтелектуального захисту КВО.

Дякую за увагу!

Рис. А.20 Двадцятий слайд