Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«__» _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Модель загроз кібербезпеки для індустріальних мереж та IoT у критичній інфрастрктурі»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Роман ЖОГЛО**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Олександр ЛАПТЄВ	
Нормоконтроль	Іван БІЛОКОНЬ	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *Магістр*

Здобувача(ки) КБм-21 (група) Жогло Роману Юрійовичу (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Модель загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі
Предмет досліджень	Моделі та методи дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі
Мета	Розробка моделі та видача рекомендацій щодо дослідження загроз кібербезпеки з метою підвищення захисту індустріальних мереж та IoT у критичній інфраструктурі
Вихідні дані для проведення роботи	Існуючі моделі та методи дослідження дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна розробка моделі та видача рекомендацій щодо дослідження загроз кібербезпеки

Практична цінність підвищення захисту індустріальних мереж та IoT у критичній інфраструктурі.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	25.10.2024 – 19.12.2024
Аналіз літературних джерел	30.12.2024 – 12.02.2024
Обгрунтування вибору дослідження	13.02.2024 – 21.02.2024
Збір даних	27.02.2024 – 26.03.2024
Виконання аналітичного огляду моделей загроз кібербезпеки для індустріальних мереж та IoT	27.03.2024 – 04.04.2024
Аналіз моделей дослідження загроз кібербезпеки для індустріальних мереж та IoT	05.04.2024 – 10.04.2024
Порівняння моделей і визначення напрямку роботи	18.04.2024 – 19.04.2024
Розробка моделі виявлення загроз кібербезпеки для індустріальних мереж та IoT	20.04.2024 – 27.04.2024
Розробка методичних рекомендацій щодо виявлення загроз кібербезпеки	28.04.2024 – 04.05.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	05.05.2024 – 15.05.2025
Подача пакету документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Роман ЖОГЛО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Модель загроз кібербезпеки для індустріальних мереж та IoT у критичній інфрастрктурі» 92 сторінки основного тексту, 9 рисунків, 8 таблиць, 21 використаного джерела.

Об’єкт дослідження – процес дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі.

Мета роботи – Розробка моделі та видача рекомендацій щодо дослідження загроз кібербезпеки з метою підвищення захисту індустріальних мереж та IoT у критичній інфраструктурі

Методи дослідження – спостереження, порівння, аналіз існуючих рішень.

Наукова новизна: розробка моделі та видача рекомендацій щодо дослідження загроз кібербезпеки

Актуальність теми: Щодня здійснюються тисячі атак в кіберпросторі, спрямованих зокрема і на виведення з ладу критичної інфраструктури. Саме тому наразі є необхідність розробки ефективних механізмів захисту критичної інфраструктури від кіберзагроз, які постійно еволюціонують.

Ключові слова: Інтернет речей, кіберзагрози, модель загроз, критична інфраструктура.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SCADA	–	Supervisory Control and Data Acquisition
DCS	–	Distributed Control System
IIoT	–	Industrial-Internet-of-Things
PLC	–	Programmable Logic Controller
IoT	–	Internet-of-Things
APT	–	Advanced Persistent Threat
FAIR	–	Factor Analysis of Information Risk
STRIDE	–	Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege
CORAS	–	візуальний метод аналізу ризиків
OCTAVE	–	Operationally Critical Threat, Asset, and Vulnerability Evaluation
IT	–	Information Technology
OPC UA	–	Open Platform Communications Unified Architecture
OT	–	Операційні технології

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційних технологій сприяв значному поширенню концепції Інтернету речей (IoT) та індустріальних мереж, які інтегруються в критичну інфраструктуру. До критичної інфраструктури належать такі об’єкти, як енергетичні системи, транспортні мережі, системи водопостачання, охорони здоров’я та інші галузі, що забезпечують життєдіяльність суспільства. Збільшення взаємозалежності між фізичними та цифровими компонентами цих систем обумовлює підвищений рівень загроз кібербезпеки. Несанкціонований доступ або атака на такі системи можуть спричинити серйозні економічні та соціальні наслідки, включаючи втрату даних, зупинку виробництва, порушення постачання електроенергії, води, а також загрози людському життю. Кіберзагрози для індустріальних мереж та IoT у критичній інфраструктурі є складними та різноманітними. Вони включають кібератаки на рівні мережевих комунікацій, вразливості програмного забезпечення, апаратні недоліки та соціальну інженерію. У зв’язку з цим дослідження загроз кібербезпеки для таких систем набуває особливої актуальності. Надійний захист критичної інфраструктури потребує розробки ефективних методів ідентифікації та усунення потенційних загроз, а також створення адаптивних механізмів реагування на можливі кібератаки. Крім того, необхідно враховувати динамічний характер загроз, що постійно змінюються та ускладнюються.

Зростання масштабів використання IoT-пристроїв у критичній інфраструктурі створює нові виклики в контексті безпеки. Багато пристроїв мають обмежені обчислювальні ресурси, що ускладнює реалізацію стандартних механізмів захисту, таких як шифрування та аутентифікація. Крім того, недостатній рівень оновлення програмного забезпечення та використання застарілих протоколів збільшують ризик компрометації системи. Це, своєю чергою, потребує розробки нових методів і підходів до виявлення та запобігання

загрозам. Одним із ключових напрямів дослідження є розробка інтелектуальних механізмів безпеки, які використовують машинне навчання, аналіз поведінкових моделей та технології штучного інтелекту для ідентифікації підозрілих дій та потенційних атак. Окрім програмного захисту, важливим аспектом кібербезпеки є фізична безпека IoT-пристроїв. Багато елементів критичної інфраструктури можуть бути доступними для фізичного втручання, що створює ризик несанкціонованого доступу, підміни або знищення обладнання. Використання сучасних методів автентифікації пристроїв, таких як біометричні системи, захищені апаратні модулі та блокчейн-технології, може значно підвищити рівень безпеки. Одним із ключових напрямів дослідження в цій сфері є аналіз існуючих методів виявлення та класифікації кіберзагроз. Сучасні методи базуються на сигнатурному, поведінковому та аномальному аналізі. Однак ці методи мають свої обмеження, що викликає потребу у створенні комплексних підходів, які поєднують машинне навчання, штучний інтелект та евристичні алгоритми. Використання таких методів дозволяє підвищити ефективність виявлення нових та невідомих загроз, що є критично важливим для безпеки індустріальних систем та IoT.

Метою даного дослідження є розробка моделі та видача рекомендацій щодо дослідження загроз кібербезпеки з метою підвищення захисту індустріальних мереж та IoT у критичній інфраструктурі.. Для досягнення цієї мети буде виконано аналіз існуючих методів дослідження загроз кібербезпеки, розроблено новий підхід до виявлення загроз та створено методичні рекомендації щодо підвищення рівня безпеки. Зокрема, увага буде приділена виявленню вразливостей у програмному та апаратному забезпеченні, аналізу мережевого трафіку та розробці заходів щодо підвищення стійкості систем до атак. Також важливим напрямом дослідження є вивчення впливу людського фактору на безпеку критичної інфраструктури. Соціальна інженерія, фішингові атаки та інші методи маніпуляції персоналом є однією з основних загроз. Розробка ефективних методів навчання та підготовки фахівців у сфері кібербезпеки може суттєво зменшити ризики, пов’язані з людськими помилками

та недостатньою обізнаністю про загрози. Об’єкт дослідження: процес дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі. Методи дослідження включають спостереження, порівння, аналіз існуючих рішень.

Предмет дослідження: моделі та методи дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі.. Таким чином, актуальність дослідження обумовлена необхідністю розробки ефективних механізмів захисту критичної інфраструктури від кіберзагроз, які постійно еволюціонують. В результаті роботи будуть сформовані практичні рекомендації для підвищення рівня безпеки індустріальних мереж та IoT, що сприятиме зменшенню ризиків та підвищенню загальної кіберстійкості критично важливих систем. Крім того, запропоновані методи та технології можуть бути використані у розробці державних стандартів та нормативних актів у сфері кібербезпеки критичної інфраструктури, що дозволить підвищити загальний рівень захисту інформаційних та індустріальних систем.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ ІНДУСТРІАЛЬНИХ МЕРЕЖ ТА ІОТ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

1.1 Аналіз архітектури та особливостей функціонування індустріальних мереж та IoT у критичній інфраструктурі

Сучасні індустріальні мережі та технології Інтернету речей (IoT) є важливими складовими критичної інфраструктури, яка включає енергетичні системи, транспорт, водопостачання, виробничі підприємства та інші об'єкти, що мають стратегічне значення для економіки та безпеки держави[1]. Впровадження цифрових технологій у ці галузі дозволяє підвищити ефективність керування процесами, але також створює додаткові виклики у сфері кібербезпеки. Індустріальні мережі забезпечують зв’язок між різними рівнями автоматизованих систем управління виробництвом, що включає системи управління технологічними процесами (SCADA), розподілені системи управління (DCS) та програмовані логічні контролери (PLC), рис.1.1.

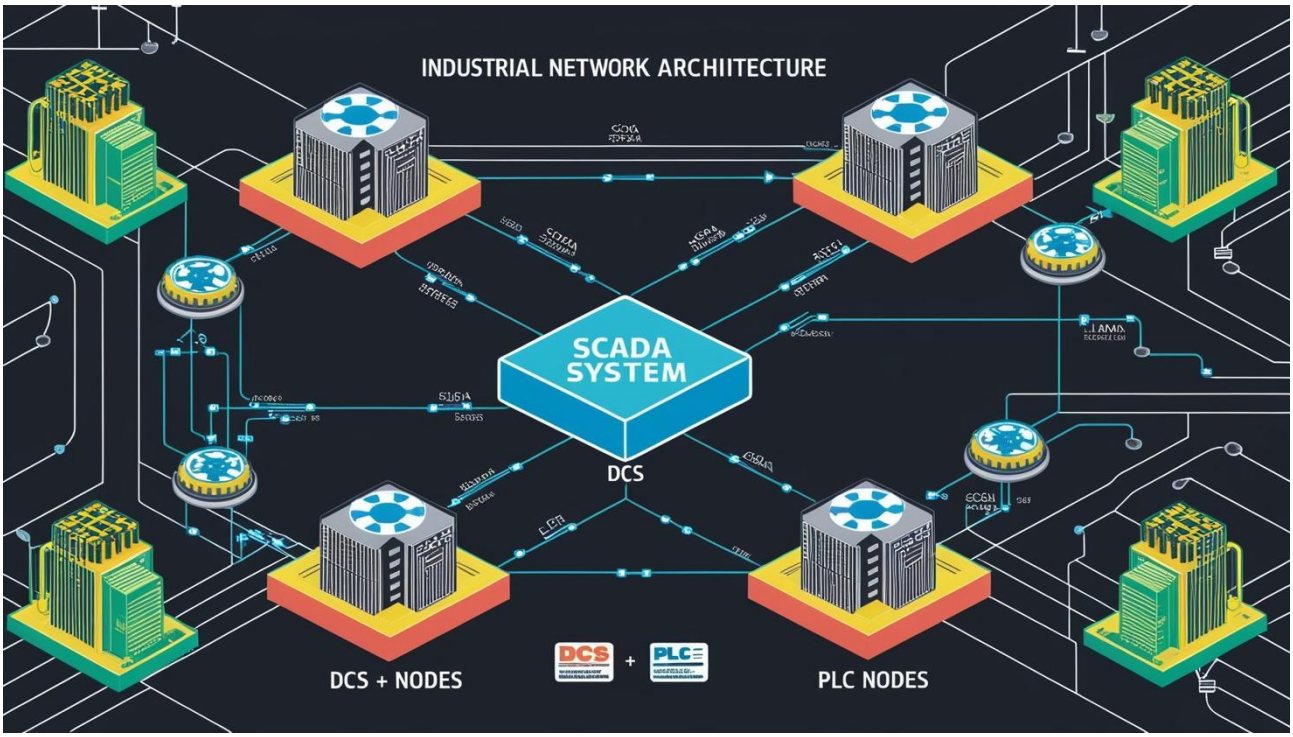

Рисунок 1.1 - Архітектура індустріальних мереж

Система автоматизованого управління в індустріальних мережах SCADA (Supervisory Control and Data Acquisition) представляє собою комплексне рішення для автоматизації промислових процесів, що об'єднує різноманітні апаратні та програмні компоненти в єдину систему моніторингу та управління. На відміну від локальних систем автоматизації, SCADA забезпечує централізований контроль над географічно розподіленими об'єктами, що особливо важливо для управління нафто- та газопроводами, електромережами та водопостачанням. Ключова особливість SCADA полягає в її здатності не лише збирати дані в реальному часі, але й виконувати їх аналіз, формувати тривоги при виникненні нештатних ситуацій і автоматично регулювати параметри технологічних процесів відповідно до заданих алгоритмів.

Сучасні SCADA-системи також інтегруються з базами даних для зберігання історичної інформації, що дозволяє виконувати аналітику ефективності виробництва та прогнозувати можливі аварійні ситуації. DCS (Distributed Control System) відрізняється від SCADA своєю архітектурою, оскільки фокусується на децентралізованому підході до управління процесами. Розподілена природа DCS забезпечує високу стійкість системи до відмов – при виході з ладу одного контролера інші продовжують функціонувати незалежно, підтримуючи роботу відповідних виробничих ділянок.

Така архітектура особливо цінна для безперервних виробничих процесів, де навіть короткочасна зупинка може призвести до значних економічних втрат або порушення технологічних режимів. DCS також характеризується високим рівнем інтеграції між різними підсистемами, що дозволяє оптимізувати взаємодію між різними етапами виробничого процесу. Кожен контролер у системі DCS має власну обчислювальну потужність і пам'ять, що дозволяє йому автономно виконувати алгоритми управління, одночасно взаємодіючи з іншими контролерами через спеціалізовані промислові мережі з високою пропускною здатністю та надійністю.

PLC (Programmable Logic Controller) є базовим елементом автоматизації, який виконує алгоритми управління, перетворюючи вхідні сигнали від датчиків

у керуючі впливи на виконавчі механізми. Сучасні PLC значно еволюціонували від своїх ранніх версій, які були призначені для заміни релейної логіки, до потужних обчислювальних пристроїв з розширеними функціональними можливостями. Вони підтримують складні математичні операції, обробку аналогових сигналів, реалізацію ПІД-регуляторів та інших алгоритмів автоматичного регулювання.

Програмування PLC здійснюється за допомогою спеціалізованих мов, визначених стандартом IEC 61131-3, включаючи текстові мови (ST – Structured Text, IL – Instruction List) та графічні (LD – Ladder Diagram, FBD – Function Block Diagram, SFC – Sequential Function Chart), що дозволяє інженерам з автоматизації обирати найбільш зручний інструмент для конкретного завдання.

Важливою особливістю PLC є їх адаптованість до роботи в жорстких промислових умовах, що включає широкий діапазон робочих температур (від -40°C до +70°C для деяких моделей), стійкість до вібрацій, вологості та агресивних середовищ. Модульна конструкція більшості сучасних PLC дозволяє гнучко налаштовувати конфігурацію системи управління під конкретні вимоги виробництва, додаючи необхідні модулі введення-виведення, комунікаційні інтерфейси та спеціалізовані функціональні блоки.

Інтеграція цих трьох ключових технологій – SCADA, DCS та PLC – створює багаторівневу архітектуру автоматизованих систем управління, де кожен рівень відповідає за вирішення специфічних завдань. PLC забезпечують безпосереднє управління обладнанням на нижньому рівні, DCS координують взаємодію між різними виробничими ділянками на середньому рівні, а SCADA надає загальну картину функціонування підприємства на верхньому рівні.

Така ієрархічна структура дозволяє оптимально розподілити обчислювальні ресурси та забезпечити ефективне управління навіть найскладнішими технологічними процесами. Індустріальний Інтернет речей (Industrial IoT, IIoT) є розширенням традиційних індустріальних мереж, що дозволяє інтегрувати IoT-пристрої для збору, аналізу та обміну даними в режимі реального часу. Основні особливості IIoT, рис.1.2.

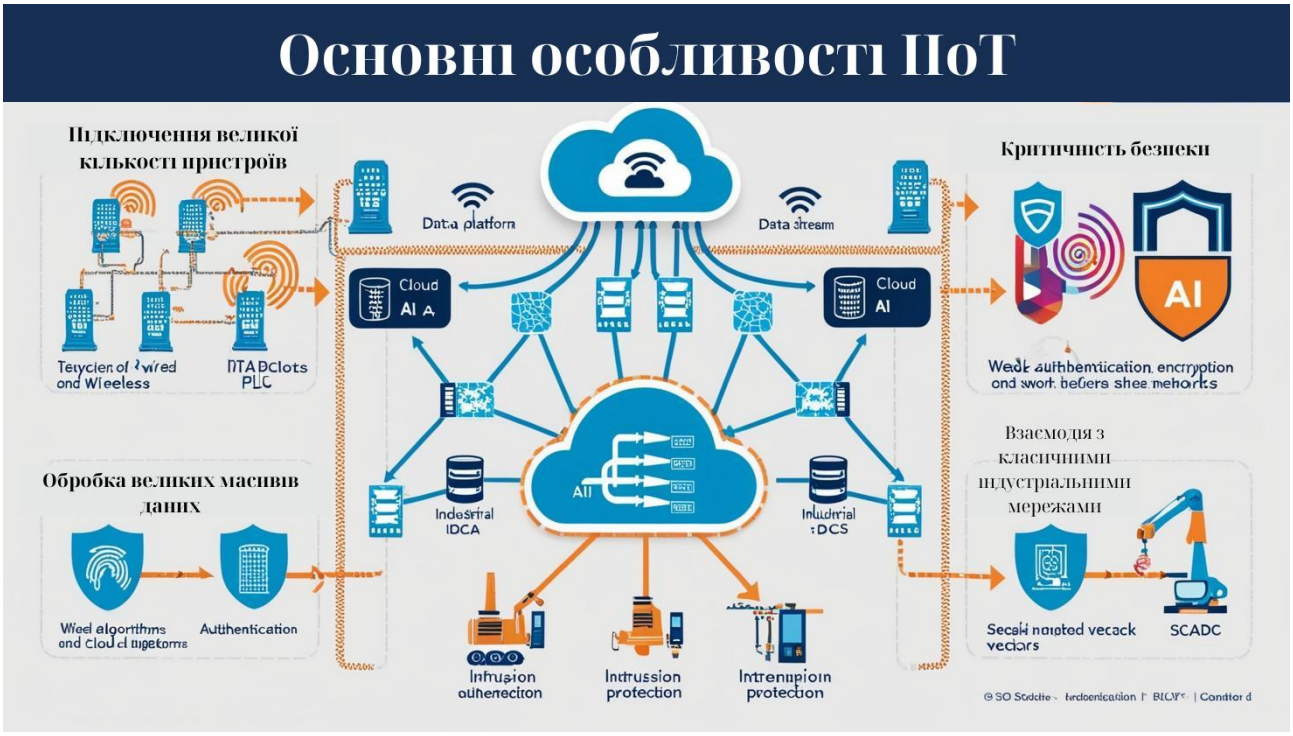

Рисунок 1.2. Основні особливості IIoT

Як видно з малюнку, у промисловому середовищі підключається велика кількість пристроїв, серед яких тисячі датчиків і контролерів, що працюють через бездротові та провідні мережі. Це супроводжується обробкою великих масивів даних, оскільки пристрої IoT генерують значні обсяги інформації, що потребує використання хмарних платформ і технологій штучного інтелекту для аналітики.

Водночас критичність безпеки залишається важливим аспектом, адже IoT-пристрої можуть бути вразливими до кібератак через слабкі механізми аутентифікації, недостатнє шифрування та відсутність захисту від вторгнень. Окрім цього, інтеграція IoT із класичними індустріальними мережами, такими як SCADA, DCS і PLC, створює потенційні ризики проникнення атак через слабкі місця підключених пристроїв [3].

Індустріальні мережі та IoT є основою для сучасних критичних інфраструктур, що дозволяє покращити ефективність виробничих процесів, але також створює нові ризики у сфері кібербезпеки. Аналіз архітектури та особливостей функціонування цих систем є ключовим для розробки ефективних методів захисту.

Критична інфраструктура (КІ) – це сукупність фізичних і віртуальних систем, ресурсів та об’єктів, які є життєво важливими для функціонування держави, суспільства та економіки. До її основних складових належать:

1. Енергетика (електростанції, мережі передачі електроенергії, газопроводи, нафтопереробні заводи).
2. Транспорт (авіація, залізниці, морські порти, дорожня інфраструктура).
3. Водопостачання та водовідведення (насосні станції, очисні споруди).
4. Охорона здоров’я (лікарні, медичні лабораторії, постачання медикаментів).
5. Фінансовий сектор (банківські установи, платіжні системи).
6. Комунікації та IT-інфраструктура (телекомунікаційні мережі, дата-центри, системи зв’язку).

Кіберзагрози для критичної інфраструктури: поглиблений аналіз вразливостей

Сучасна критична інфраструктура функціонує в умовах глибокої інтеграції цифрових технологій у всі аспекти управління технологічними процесами, що створює принципово нові вектори атак для потенційних зловмисників. Кібератаки на промислові мережі становлять одну з найбільш небезпечних загроз, оскільки вони можуть реалізовуватися дистанційно та мати масштабні деструктивні наслідки. Вразливості в програмному забезпеченні систем SCADA, DCS та PLC слугують потенційними точками входу для атакуючих, які прагнуть отримати контроль над критичними процесами.

Історія кібератак на промислові системи демонструє еволюцію їхньої складності та цілеспрямованості. Шкідливе програмне забезпечення типу Stuxnet, що вразило іранську ядерну програму, продемонструвало безпрецедентний рівень технічної витонченості, включаючи здатність впливати на фізичні процеси через маніпуляції з контролерами Siemens, залишаючись при цьому непоміченим протягом тривалого часу.

Подальші інциденти, такі як BlackEnergy, що вразив енергетичну інфраструктуру України в 2015 році, та TRITON, спрямований на системи безпеки нафтохімічних підприємств, підтверджують тенденцію до створення спеціалізованих засобів атаки, адаптованих під конкретні промислові системи.

Фізичні загрози залишаються невід'ємною частиною комплексної безпеки критичної інфраструктури, але їх характер також трансформується в епоху цифровізації. Традиційні форми саботажу доповнюються можливістю дистанційного впливу на фізичні системи через кіберпростір, що розмиває межу між віртуальними та фізичними атаками. Стихійні лиха, техногенні катастрофи та інші форми фізичного впливу можуть спричинити каскадні відмови, які посилюються внаслідок взаємозалежності різних компонентів критичної інфраструктури, об'єднаних цифровими мережами.

Людський фактор продовжує залишатися однією з найбільш вразливих ланок у системі захисту критичної інфраструктури. Помилкові дії персоналу при налаштуванні, експлуатації або обслуговуванні систем можуть призвести до критичних збоїв навіть за відсутності зловмисних намірів.

Цей аспект посилюється тенденцією до скорочення кількості фахівців з глибокими знаннями у сфері промислових систем управління на фоні зростаючої складності цих систем. Методи соціальної інженерії стають все більш витонченими, включаючи таргетовані фішингові атаки на персонал критичної інфраструктури, спеціально розроблені з урахуванням психологічних особливостей цільової аудиторії та специфіки їхньої професійної діяльності.

Проблема відсутності або недостатності оновлень програмного забезпечення в системах OT (Operational Technology) має комплексний характер.

На відміну від систем IT, де практика регулярних оновлень є загальноприйнятою, системи OT часто розробляються з пріоритетом на безперервність функціонування та стабільність роботи. Це призводить до ситуації, коли багато критичних систем працюють на застарілих версіях програмного забезпечення протягом десятиліть.

Наприклад, не є рідкістю застосування операційних систем Windows XP або навіть більш ранніх версій у промислових системах управління, незважаючи на те, що офіційна підтримка цих операційних систем давно припинена.

Особливу занепокоєність викликає зростаюча конвергенція IT (Information Technology) та OT, що призводить до розмивання традиційних меж безпеки. Історично ізольовані промислові мережі все частіше інтегруються з корпоративними інформаційними системами, отримують з'єднання з Інтернетом для забезпечення віддаленого доступу та моніторингу, що суттєво розширює поверхню для потенційних атак.

Цей процес посилюється впровадженням технологій Інтернету речей (IoT) та Індустрії 4.0, що передбачають масове підключення виробничих пристроїв до мережі.

Атаки на ланцюги поставок також становлять суттєву загрозу для критичної інфраструктури. Компрометація програмного забезпечення або обладнання на етапі розробки, виробництва або дистрибуції може призвести до впровадження бекдорів або інших вразливостей, які згодом будуть використані для атак.

Прикладом може служити інцидент SolarWinds, який продемонстрував можливість масштабного впливу через компрометацію популярного програмного забезпечення для моніторингу мереж.

Захист критичної інфраструктури від окреслених загроз потребує комплексного підходу, який включає технічні, організаційні та регуляторні заходи. Технологія глибинного захисту (Defense-in-Depth), сегментація мереж, регулярні оцінки вразливостей, тренування персоналу та розробка планів реагування на інциденти є ключовими елементами ефективної стратегії забезпечення кібербезпеки критичної інфраструктури в умовах зростаючої цифровізації та все більш витончених кіберзагроз [4].

Традиційні IT-системи (Information Technology) та операційні технології (OT) в критичній інфраструктурі працюють разом, але мають суттєві відмінності, таблиця 1.1

Таблиця 1.1

Традиційні IT-системи (Information Technology) та операційні технології (OT)

Параметр	IT-системи	OT-системи
Призначення	Обробка, зберігання та передача даних	Керування фізичними процесами (виробництво, енергопостачання)
Пристрої	Сервери, робочі станції, мережеве обладнання	PLC, SCADA-системи, датчики, виконавчі механізми
Пріоритети	Конфіденційність, доступність, цілісність даних	Безперервність процесів, безпека обладнання
Часові вимоги	Можливі затримки в обробці даних	Жорсткі вимоги до часу реакції систем
Оновлення ПЗ	Регулярні оновлення	Оновлення відбуваються рідко через ризик зупинки процесів

Історично операційні технології (OT) та інформаційні технології (IT) розвивалися як окремі домени з різними пріоритетами, технологіями та підходами до безпеки. OT-системи були спроектовані з акцентом на надійність, безперервність роботи та безпеку фізичних процесів, тоді як IT-системи фокусувалися на обробці даних, ефективності та захисті інформації. Ця фундаментальна різниця визначала архітектурні рішення та підходи до забезпечення безпеки в обох доменах.

Конвергенція IT і OT, що активно відбувається протягом останнього десятиліття, докорінно змінює ландшафт кіберзагроз для критичної інфраструктури. Промислові системи управління, які раніше функціонували в умовах фізичної та логічної ізоляції ("повітряного зазору"), тепер інтегруються з корпоративними мережами та підключаються до глобального інформаційного простору. Це стирання традиційних кордонів між операційними та

інформаційними технологіями відкриває операційні системи для цілого спектру загроз, характерних для IT-домену, одночасно створюючи нові унікальні вектори атак, специфічні для інтегрованого середовища.

Сучасні SCADA-системи, які раніше функціонували як замкнуті екосистеми, тепер інтегруються з хмарними сервісами, корпоративними інформаційними системами та навіть соціальними мережами для забезпечення більш ефективного управління та аналітики. Ця інтеграція приносить незаперечні переваги для бізнесу, включаючи оптимізацію виробничих процесів, зниження експлуатаційних витрат та покращення прогнозування технічного обслуговування, але водночас експоненційно збільшує поверхню атаки. Інтеграція IT і OT часто відбувається без фундаментального переосмислення архітектури безпеки. Багато організацій впроваджують рішення для поєднання цих доменів, не враховуючи принципову різницю в їхніх пріоритетах та вимогах. Традиційні IT-підходи до безпеки, такі як регулярні оновлення та перезавантаження систем, можуть бути неприйнятними для OT-середовища, де безперервність роботи є критичною. Це створює суттєві архітектурні вразливості на стику двох технологічних світів.

Демілітаризовані зони (DMZ), що виступають буфером між IT і OT мережами, часто реалізуються з недостатньою глибиною захисту. Складна взаємодія між корпоративними системами та промисловими контролерами може створювати неочевидні шляхи для проникнення зловмисників. Наприклад, компрометація системи планування ресурсів підприємства (ERP) може опосередковано вплинути на виробничі процеси через інтеграційні інтерфейси з системами управління виробництвом (MES). Використання відкритих промислових протоколів, таких як Modbus і OPC-UA, значно спрощує інтеграцію різнорідних систем, але створює додаткові ризики безпеки. Ці протоколи, розроблені в епоху, коли кібербезпека не була пріоритетом, мають обмежені можливості для автентифікації, шифрування та забезпечення цілісності даних.

Протокол Modbus, який широко використовується в промислових системах більше 40 років, не має вбудованих механізмів автентифікації та

шифрування. Це означає, що будь-який пристрій, підключений до мережі Modbus, може надсилати команди контролерам без необхідності підтвердження своєї автентичності. У сучасному середовищі, де ці мережі вже не є фізично ізольованими, така відкритість становить серйозну загрозу. Зловмисник, який отримав доступ до мережі, може легко перехоплювати команди, змінювати їх вміст або ін'єктувати власні інструкції, потенційно спричиняючи катастрофічні наслідки для керованих процесів. OPC-UA, більш сучасний протокол, пропонує розширені функції безпеки, включаючи шифрування та автентифікацію на основі сертифікатів.

Однак у багатьох реалізаціях ці функції залишаються невикористаними через складність налаштування або міркування продуктивності. Крім того, навіть при включених функціях безпеки OPC-UA може мати вразливості в реалізації, які можуть бути використані досвідченими зловмисниками. DNP3, інший поширений протокол у енергетичному секторі, початково розроблявся без врахування кіберзагроз. Пізніші розширення DNP3 Secure Authentication додають механізми автентифікації, але їх впровадження залишається обмеженим у багатьох існуючих системах. Конвергенція IT і OT створює нові шляхи для отримання фізичного доступу до критичної інфраструктури через кіберпростір. Традиційно фізична безпека та кібербезпека розглядалися як окремі домени з різними відповідальними особами та процедурами. Однак у сучасному інтегрованому середовищі ці домени стають взаємозалежними. Системи контролю фізичного доступу, такі як електронні замки, біометричні сканери та системи відеоспостереження, все частіше інтегруються з корпоративними IT-мережами. Компрометація IT-інфраструктури може дозволити зловмиснику маніпулювати цими системами, потенційно отримуючи фізичний доступ до об'єктів критичної інфраструктури.

Крім того, віддалений доступ до OT-систем, який став широко поширеним під час пандемії COVID-19, створює додаткові ризики. Інженери та техніки, які раніше повинні були фізично бути присутніми на об'єкті для виконання налаштувань або технічного обслуговування, тепер можуть виконувати ці

завдання віддалено. Компрометація облікових записів віддаленого доступу може дозволити зловмисникам отримати такий самий рівень контролю над системами, як і легітимні адміністратори.

Шкідливе програмне забезпечення, спрямоване на OT-системи, еволюціонувало від порівняно простих теоретичних концепцій до високоспеціалізованих інструментів з безпрецедентними можливостями. Ця еволюція тісно пов'язана з конвергенцією IT і OT, яка створює нові шляхи поширення та нові цілі для атак. Stuxnet, виявлений у 2010 році, став першим шкідливим програмним забезпеченням, спеціально розробленим для атаки на промислові системи управління. Він використовував складний ланцюжок експлойтів для проникнення в ізольовані системи управління центрифугами в іранській ядерній програмі та маніпулювання їхньою роботою, одночасно приховуючи ці зміни від операторів. Stuxnet продемонстрував, що навіть системи, захищені "повітряним зазором", можуть бути компрометовані через складні багатоетапні атаки. Наступні інциденти, такі як BlackEnergy, Industroyer, TRITON та Industroyer2, продемонстрували подальшу еволюцію тактик, технік та процедур зловмисників. Ці шкідливі програми виявили глибоке розуміння специфічних протоколів та архітектур промислових систем управління, що свідчить про зростаючу спеціалізацію та технічну витонченість акторів загроз.

Особливе занепокоєння викликає TRITON (також відомий як TRISIS), виявлений у 2017 році. Це шкідливе програмне забезпечення було спеціально розроблене для атаки на системи безпеки Triconex Safety Instrumented System (SIS) виробництва Schneider Electric. SIS-системи є останньою лінією захисту від катастрофічних аварій у багатьох промислових середовищах, включаючи нафтохімічні заводи та атомні електростанції. Компрометація цих систем може призвести до серйозних фізичних наслідків, включаючи пошкодження обладнання, екологічні катастрофи та навіть втрату людських життів. Загальною тенденцією в еволюції шкідливого програмного забезпечення для OT є рух від атак, спрямованих на окремі компоненти, до комплексних кампаній, які враховують взаємозв'язок між різними рівнями автоматизації та використовують

інтеграцію IT і OT для максимізації впливу. Наприклад, сучасні атаки можуть поєднувати компрометацію корпоративної мережі з проникненням в промислові системи управління, маніпулювання даними моніторингу для приховування змін та навіть атаки на системи резервного копіювання для ускладнення відновлення.

Конвергенція IT і OT має різні наслідки для різних секторів критичної інфраструктури, зважаючи на їхні унікальні характеристики, регуляторні вимоги та операційні пріоритети. Енергетичний сектор, включаючи електроенергетику, нафтову та газову промисловість, є однією з найбільш важливих і водночас вразливих частин критичної інфраструктури. Цифрова трансформація енергетики, включаючи впровадження концепції "розумних мереж" (Smart Grid), створює нові виклики для кібербезпеки. Розумні мережі включають мільйони взаємопов'язаних пристроїв, від інтелектуальних лічильників до підстанцій з віддаленим управлінням, які збирають та обмінюються даними в реальному часі. Ця масивна мережа пристроїв створює величезну поверхню для потенційних атак. Атаки на енергетичний сектор можуть мати каскадні наслідки для інших секторів критичної інфраструктури, які залежать від стабільного електропостачання.

Інциденти кібербезпеки в енергетичному секторі, такі як атаки на українську електромережу в 2015 та 2016 роках, демонструють реальність цих загроз. У цих атаках зловмисники використовували комплексний підхід, який починався з компрометації корпоративних мереж через фішингові електронні листи, а згодом прогресував до проникнення в промислові системи управління та маніпулювання комутаційним обладнанням на підстанціях. Системи водопостачання та водовідведення також стають все більш взаємопов'язаними з IT-мережами для покращення моніторингу якості води, оптимізації розподілу та зниження експлуатаційних витрат. Однак ця інтеграція створює нові вектори атак на системи, які безпосередньо впливають на здоров'я та безпеку населення.

Інцидент на очисних спорудах у Флориді в лютому 2021 року, де зловмисник намагався збільшити рівень хімікатів у питній воді до небезпечних концентрацій через компрометований віддалений доступ, демонструє потенційні

наслідки таких атак. Хоча ця конкретна спроба була швидко виявлена операторами, вона підкреслює необхідність багаторівневого захисту в системах водопостачання, особливо з огляду на їх критичну важливість для здоров'я населення.

Сучасні транспортні системи, включаючи аеропорти, залізниці, морські порти та системи управління дорожнім рухом, все більше залежать від взаємопов'язаних цифрових технологій. Інтелектуальні транспортні системи (ITS) інтегрують традиційну транспортну інфраструктуру з комунікаційними технологіями для покращення безпеки, ефективності та екологічності. Ця інтеграція створює нові вразливості, які можуть бути використані для порушення роботи транспортних систем, потенційно спричиняючи економічні збитки, порушення логістичних ланцюгів або навіть загрозу безпеці пасажирів. Наприклад, атаки на системи управління рухом можуть призвести до затримок, перевантаження або, в найгіршому випадку, аварій. Заклади охорони здоров'я зазнають швидкої цифрової трансформації, з впровадженням електронних медичних карт, підключених медичних пристроїв та систем дистанційного моніторингу пацієнтів. Ця трансформація створює складну взаємопов'язану екосистему, де традиційні IT-системи інтегруються з медичними пристроями, які безпосередньо впливають на здоров'я пацієнтів. Атаки на системи охорони здоров'я можуть мати безпосередні наслідки для безпеки пацієнтів. Наприклад, компрометація інсулінових помп або кардіостимуляторів може становити пряму загрозу для життя. Крім того, атаки програм-вимагачів на лікарні, які стали поширеними в останні роки, можуть порушити доступ до медичних даних та систем, потенційно затримуючи або погіршуючи надання медичної допомоги.

Захист критичної інфраструктури в умовах конвергенції IT і OT вимагає комплексного підходу, який враховує унікальні характеристики та вимоги обох доменів. Ефективна стратегія безпеки повинна включати технічні, організаційні та процесні заходи, адаптовані до специфічних ризиків конвергованого середовища. Стратегія глибинного захисту (Defense-in-Depth) залишається основою для забезпечення безпеки критичної інфраструктури. Однак у контексті

конвергенції IT і OT вона повинна бути адаптована для врахування унікальних вимог операційних технологій.

Традиційні механізми безпеки IT, такі як антивірусне програмне забезпечення, системи виявлення та запобігання вторгненням, повинні бути специфічно налаштовані для роботи в OT-середовищі, де пріоритетом є стабільність і безперервність роботи. Наприклад, сканування на виявлення вразливостей, яке є стандартною практикою в IT, повинно виконуватися з особливою обережністю в OT-системах, де навіть незначні порушення в мережевому трафіку можуть вплинути на роботу чутливого обладнання. Сегментація мережі є критично важливою для обмеження поширення потенційних атак. Промислова демілітаризована зона (IDMZ) повинна бути впроваджена для забезпечення буфера між корпоративними та промисловими мережами, з контрольованими інтерфейсами для необхідної взаємодії. В межах промислової мережі додаткова сегментація повинна бути реалізована на основі функціональних зон і рівнів критичності.

Системи моніторингу безпеки повинні бути адаптовані для виявлення аномалій в промислових протоколах і поведінці пристроїв. Традиційні системи виявлення вторгнень часто не розпізнають специфічні атаки на промислові протоколи, такі як маніпуляції з командами Modbus або DNP3. Спеціалізовані рішення для моніторингу безпеки OT можуть ідентифікувати небезпечні команди, аномальні операційні параметри або підозрілі зміни в поведінці пристроїв. Управління вразливостями є особливо складним у конвергованому середовищі IT/OT через різні вимоги до доступності та стабільності. Традиційний підхід IT до швидкого застосування оновлень безпеки часто неприйнятний для OT-систем, де будь-яке оновлення повинно пройти ретельне тестування і може бути застосоване лише під час запланованих вікон обслуговування.

Комплексний процес управління вразливостями для середовища IT/OT повинен включати, цілісний інвентар всіх апаратних і програмних компонентів у обох доменах, з ідентифікацією взаємозалежностей, регулярний аналіз

вразливостей з використанням методів, які не порушують роботу чутливих систем, пріоритизацію вразливостей на основі їх критичності та потенційного впливу на безпеку та операції, розробку стратегій зниження ризиків для вразливостей, які не можуть бути негайно усунені, включаючи додаткові контролі безпеки та моніторинг, документовані процедури для тестування та впровадження оновлень безпеки з мінімальним впливом на операції.

Успішне забезпечення безпеки в конвергованому середовищі IT/OT вимагає не лише технічних засобів, але й розвитку організаційної культури, яка інтегрує підходи до безпеки з обох доменів. Традиційно фахівці з IT-безпеки та інженери OT мають різні пріоритети, термінологію та методи роботи. Подолання цього розриву є ключовим для ефективного управління ризиками. Організації повинні сприяти крос-функціональній співпраці між командами IT та OT, включаючи спільні тренінги, обмін знаннями та розробку спільних процедур реагування на інциденти. Навчання персоналу повинно охоплювати як специфічні ризики IT і OT, так і унікальні виклики, що виникають на їх перетині.

Нижче представлена схема, яка ілюструє, як IT та OT-системи взаємодіють у критичній інфраструктурі, а також показує потенційні вразливості, рис.1.3.

Рисунок 1.3 - Взаємозв'язок IT та OT у критичній інфраструктурі.

Ось схема взаємозв'язку між IT та OT-системами в критичній інфраструктурі. Вона показує, як корпоративні IT-мережі, хмарні сервіси,

інтернет і брандмауери взаємодіють із SCADA-системами, DCS, PLC-контролерами, датчиками, виконавчими механізмами та IoT-пристроями. Ця структура демонструє потенційні точки вразливості, через які кіберзагрози можуть проникати з IT-середовища в OT-системи, що може призвести до серйозних наслідків, зокрема відмови критичних процесів. Конвергенція IT і OT у критичній інфраструктурі представляє фундаментальний зсув у ландшафті кіберзагроз, створюючи нові вектори атак і розширюючи потенційні наслідки кіберінцидентів до фізичного домену. Розуміння унікальних вразливостей, що виникають на перетині цих двох технологічних сфер, є критично важливим для розробки ефективних стратегій захисту. Тенденції цифрової трансформації, включаючи розширення впровадження IoT, хмарних технологій та штучного інтелекту в критичну інфраструктуру, продовжать розмивати традиційні межі між IT і OT. Це вимагатиме постійної адаптації підходів до забезпечення безпеки, з більшим акцентом на безпеку за дизайном, проактивне виявлення загроз та стійкість до атак. Забезпечення безпеки критичної інфраструктури в цьому динамічному середовищі вимагатиме не лише технічних інновацій, але й еволюції регуляторних підходів, розвитку галузевих стандартів та посилення міжнародного співробітництва для протидії зростаючим кіберзагрозам [5].

1.2. Класифікація та характеристика загроз кібербезпеки в індустріальних мережах та IoT

Критична інфраструктура та промислові системи, такі як SCADA, DCS і IoT-пристрої, стають основними цілями кіберзлочинців через їхню високу значущість та потенційні наслідки атак. У цій секції розглянемо типологію кіберзагроз, вектори атак на IoT-пристрої в критичній інфраструктурі та особливості цілеспрямованих APT-атак. Загрози кібербезпеці промислових систем можна класифікувати за кількома критеріями, зокрема за джерелом походження, намірами атакуючих, рівнем впливу та способом реалізації.

Внутрішні загрози включають атаки або ненавмисні дії співробітників підприємства. Це можуть бути помилки, саботаж або недостатня кваліфікація персоналу, що призводить до порушень у роботі систем.

Зовнішні загрози, навпаки, пов’язані з атаками хакерів, державних або кримінальних угруповань, які використовують шкідливе програмне забезпечення для проникнення у промислові мережі та маніпулювання їхніми компонентами [6].

За намірами атакуючих загрози поділяються на цілеспрямовані та масові атаки. Цілеспрямовані атаки, такі як Advanced Persistent Threats (APT), є складними та довготривалими, вони спрямовані на отримання контролю над системою. Прикладом є атака Stuxnet, яка спеціально розроблялася для ураження промислового обладнання. Масові атаки зазвичай менш точні, вони використовуються для виявлення вразливих систем у мережі. Ботнети часто здійснюють подібні атаки, орієнтуючись на IoT-пристрої, що не мають належного захисту.

Рівень впливу атак визначається тим, яку саме шкоду вони завдають системі. Одним із ключових аспектів є конфіденційність, коли відбувається витік даних, що може включати інформацію про роботу критичних промислових систем. Порушення цілісності даних може призвести до модифікації параметрів роботи обладнання, що в деяких випадках виводить з ладу виробничі процеси. Загроза доступності включає DDoS-атаки, мережеві збої та блокування ресурсів, що може призвести до повної зупинки роботи підприємства.

Щодо способів реалізації атак, вони можуть відбуватися на різних рівнях. Мережеві атаки, такі як Man-in-the-Middle, DNS-spoofing або DoS/DDoS, спрямовані на перехоплення даних або порушення роботи мережевого обладнання. Атаки на програмне забезпечення використовують експлойти, бекдори, руткіти та шкідливі оновлення, що можуть призвести до проникнення в систему або отримання контролю над нею. Фізичні атаки передбачають компрометацію пристроїв, підключення зловмисного обладнання або

несанкціонований доступ до індустріальних систем, що також може спричинити значні порушення у роботі критичної інфраструктури.

Пристрої Інтернету речей (IoT) у критичній інфраструктурі мають низку специфічних вразливостей, які можуть використовувати зловмисники. Одним із ключових векторів атак є незахищені інтерфейси, що включають відкриті порти та слабкі паролі, зокрема у протоколах Telnet, SSH і HTTP. Відсутність шифрування у протоколах обміну даними також створює додаткові ризики, оскільки зловмисники можуть перехоплювати або змінювати інформацію, що передається між пристроями.

Ще однією серйозною загрозою є фізичний доступ до пристроїв. Якщо зловмисник отримує можливість підключитися до незахищених IoT-пристроїв, таких як камери спостереження чи промислові датчики, він може змінити їхню конфігурацію або повністю захопити контроль. Впровадження "злоякісного" пристрою в мережу підприємства також може стати точкою входу для подальшої атаки на всю систему. Відсутність оновлень та патчів залишається великою проблемою, оскільки багато IoT-пристроїв працюють на застарілих прошивках, що містять відомі вразливості. Деякі виробники припиняють підтримку старих моделей, залишаючи їх без оновлень безпеки, що робить такі пристрої особливо вразливими до атак. DDoS-атаки та ботнети часто використовують незахищені IoT-пристрої для створення глобальних мереж заражених систем, як це було у випадку з ботнетами Mirai та Mozi. Ці атаки спрямовані на перевантаження критичних сервісів та можуть призвести до значних перебоїв у роботі інфраструктури.

Ще один серйозний ризик – маніпуляція даними сенсорів. Якщо зловмисник отримує доступ до потоку даних із промислових датчиків, він може не лише перехоплювати інформацію, але й підробляти її, змінюючи параметри роботи системи. Це може вплинути на роботу виробничих процесів, створити аварійні ситуації або навіть призвести до фізичних пошкоджень обладнання.

Advanced Persistent Threat (APT) – це довготривала цілеспрямована атака, яка виконується висококваліфікованими зловмисниками (часто державними

структурами або організованими групами). Основна мета APT – отримати довгостроковий доступ до індустріальних мереж без виявлення. Фази APT-атаки на критичну інфраструктуру, рис.1.4.

Рисунок 1.4 - Фази APT-атаки на критичну інфраструктуру

Ось реальні приклади APT-атак, які мали значний вплив на критичну інфраструктуру. Stuxnet у 2010 році став однією з перших відомих кібератак, що безпосередньо впливала на фізичне обладнання. Він був спрямований на ядерні об'єкти Ірану, використовуючи заражені USB-носії для ураження SCADA-систем Siemens, що контролювали центрифуги для збагачення урану. Інший приклад – TRITON у 2017 році, коли зловмисники атакували систему безпеки (SIS) на нафтохімічному заводі. Це могло призвести до серйозних фізичних аварій, адже компрометація систем безпеки загрожувала як обладнанню, так і життю працівників.

У 2016 році відбулася атака Industroyer, яка була спрямована на енергетичну інфраструктуру України. Вона викликала масштабні відключення електроенергії, показавши, наскільки вразливими можуть бути електромережі до добре спланованих кібератак. Критична інфраструктура та IoT-пристрої залишаються ключовими цілями кіберзлочинців через їхню стратегічну важливість. Основні загрози включають мережеві атаки, витік даних, саботаж та

APT-атаки [7]. Вектори атак на IoT-пристрої включають недостатній захист інтерфейсів, фізичний доступ та відсутність оновлень. APT-атаки є одними з найнебезпечніших через їхню складність та довготривалу присутність у системах.

Для ефективного захисту індустріальних мереж необхідно впроваджувати багаторівневий підхід до кібербезпеки, що включає моніторинг трафіку, контроль доступу та використання сучасних засобів виявлення загроз.

1.3. Огляд існуючих методів та підходів до дослідження загроз кібербезпеки

Захист індустріальних мереж та IoT у критичній інфраструктурі вимагає використання комплексних підходів, які охоплюють аналіз ризиків, дотримання міжнародних стандартів та застосування методів моделювання загроз.

У цьому розділі розглянемо ключові стандарти кібербезпеки, методології оцінки ризиків та підходи до моделювання загроз. У світі розроблено кілька загальноприйнятих стандартів, які визначають принципи захисту критичної інфраструктури та індустріальних систем. Найбільш значущими є, рис.1.5.

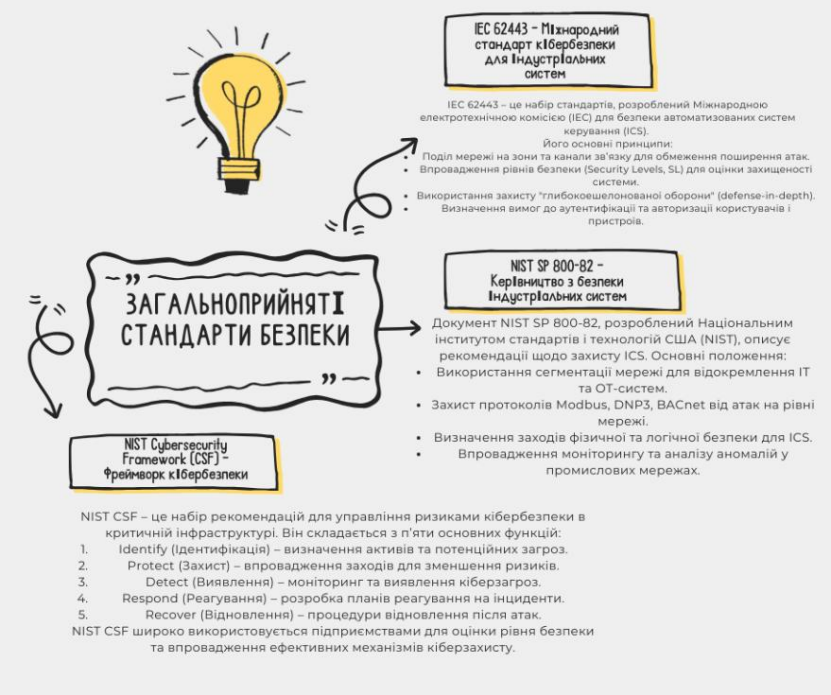

Рисунок 1.5 - Стандарти безпеки.

NIST CSF – це набір рекомендацій для управління ризиками кібербезпеки, що складається з п’яти основних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Він допомагає організаціям визначати активи, оцінювати загрози та впроваджувати заходи для зменшення ризиків. Фреймворк передбачає моніторинг загроз, розробку планів реагування на інциденти та ефективне відновлення після атак. NIST CSF широко застосовується для оцінки рівня безпеки підприємств та покращення їхніх механізмів кіберзахисту. Його використання сприяє зменшенню кіберризиків і підвищенню стійкості організацій до атак.

Моделювання загроз допомагає оцінити потенційні вразливості та можливі сценарії атак. Найбільш популярні підходи включають такі методи, таблиця 1.2.

Таблиця 1.2

Популярні підходи моделювання загроз

Метод	Опис
FAIR (Factor Analysis of Information Risk)	Кількісний аналіз ризиків на основі оцінки ймовірності атак та потенційних збитків. Дозволяє пріоритизувати загрози та оцінити ефективність заходів захисту.
STRIDE (Microsoft)	Використовується для моделювання загроз ICS та IoT, оцінює загрози за шістьма категоріями: Spoofing (підміна особистості), Tampering (модифікація даних), Repudiation (відмова від дій), Information Disclosure (витік даних), Denial of Service (відмова в обслуговуванні), Elevation of Privilege (підвищення привілеїв).
CORAS	Використовує графічне моделювання ризиків для аналізу загроз, візуалізує можливі сценарії атак та визначає слабкі місця.
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Дозволяє ідентифікувати вразливості та потенційні наслідки атак на ICS, застосовується у державних та промислових структурах.

Моделювання загроз у сфері кібербезпеки відіграє критичну роль у захисті індустріальних систем, надаючи можливість випереджати дії зловмисників через

систематичний аналіз потенційних вразливостей. Підходи ATT&CK for ICS, Cyber Kill Chain та STPA-Sec пропонують різні, але взаємодоповнюючі методології для забезпечення безпеки промислових об'єктів.

ATT&CK for ICS охоплює вичерпний каталог тактик і технік, що застосовуються при атаках на індустріальні системи управління. Ця база знань дозволяє фахівцям з безпеки не лише розпізнавати характерні патерни зловмисних дій, але й розробляти проактивні заходи захисту, спираючись на реальні сценарії атак. Цінність цього підходу полягає у постійному оновленні інформації відповідно до еволюції методів кібератак. Методологія Cyber Kill Chain розглядає процес атаки як послідовність взаємопов'язаних етапів.

Починаючи з розвідки, зловмисники поступово просуваються через доставку шкідливого коду, експлуатацію вразливостей, встановлення контролю над системою, до фінальних дій із досягнення цілей атаки. Розуміння цієї послідовності дозволяє створювати ешелоновану систему захисту, що блокує атаку на ранніх етапах і суттєво знижує ймовірність досягнення зловмисниками своїх цілей. STPA-Sec привносить системно-теоретичний підхід до моделювання загроз, зосереджуючись на взаємозв'язках між різними компонентами індустріальних систем. Такий підхід дозволяє виявляти складні вразливості, що виникають не в окремих елементах, а на рівні взаємодії компонентів. Це особливо важливо для промислових систем, де небезпека часто криється у несподіваних наслідках взаємодії між різними процесами та підсистемами.

Комплексне застосування міжнародних стандартів безпеки, таких як IEC 62443, що спеціалізується на безпеці промислової автоматизації та систем управління, NIST SP 800-82, що пропонує рекомендації для захисту систем ICS, та NIST CSF, що надає універсальну структуру управління кіберризиками, створює надійну основу для побудови захисту критичної інфраструктури. Доповнюючи ці стандарти методологіями оцінки ризиків FAIR, STRIDE і OCTAVE, організації отримують можливість кількісно оцінювати ризики, систематично аналізувати загрози та розробляти стратегії мінімізації уразливостей.

Дослідження загроз кібербезпеки є складним і багатогранним процесом, який охоплює широкий спектр методів, підходів і технологій. З розвитком цифрових технологій та активним впровадженням інтернету у всі сфери життя, зростає й рівень загроз, що постають перед користувачами, компаніями, державними установами. У зв'язку з цим, питання забезпечення кібербезпеки стає одним із найактуальніших у сучасному інформаційному середовищі.

Одним із базових напрямів дослідження загроз є виявлення атак, що може здійснюватися як на основі вже відомих зразків, так і шляхом виявлення аномальної поведінки в системі. Перший підхід, так званий підписний метод, передбачає наявність бази даних зразків шкідливого програмного забезпечення, відомих експлойтів або сигнатур атак. Він дозволяє точно і швидко визначати загрози, однак майже повністю неефективний у випадках нових, ще не задокументованих атак. Для подолання цієї вади застосовується метод виявлення аномалій, який базується на аналізі поведінки користувачів, мережевого трафіку або системних процесів. У випадку виявлення відхилень від типових моделей, система може сигналізувати про потенційну загрозу. Цей підхід дозволяє виявляти невідомі типи атак, однак є вразливим до хибно-позитивних результатів, тобто ситуацій, коли нормальна поведінка інтерпретується як підозріла.

Аналіз кіберзагроз не обмежується лише виявленням атак. Важливу роль відіграє і аналітична складова, що включає в себе збір, систематизацію та інтерпретацію даних про загрози. Сучасні підходи до розвідки загроз, відомі як threat intelligence, базуються як на відкритих джерелах інформації (OSINT), так і на спеціалізованих каналах, включно з темними сегментами інтернету. Метою цієї діяльності є не лише фіксація атак, а й розуміння їхнього походження, цілей, використовуваних методів і потенційних наслідків. Також застосовується цифрова криміналістика, яка дозволяє реконструювати хід атаки, зібрати докази, визначити вразливі місця системи та підготувати матеріали для судових розглядів або внутрішніх розслідувань.

Сучасний ландшафт кіберзагроз для індустріальних систем характеризується зростаючою складністю та цілеспрямованістю атак. Державні кіберзлочинні угруповання, промисловий шпіонаж та навіть терористичні організації все частіше розглядають критичну інфраструктуру як привабливу ціль. У цьому контексті моделювання загроз стає не просто технічною процедурою, а стратегічним інструментом забезпечення безперервності бізнес-процесів та національної безпеки. Ефективна імплементація процесів моделювання загроз вимагає міждисциплінарного підходу, що об'єднує експертів з кібербезпеки, інженерів промислових систем та фахівців з управління ризиками. Такий комплексний підхід дозволяє не лише реагувати на відомі загрози, але й адаптуватися до постійно еволюціонуючого ландшафту кіберзагроз, забезпечуючи стійкість індустріальних систем перед обличчям невідомих раніше атак.

Зрештою, інтеграція моделювання загроз у загальну стратегію кібербезпеки організації формує культуру безпеки, де розуміння потенційних вразливостей та проактивний підхід до їх усунення стають частиною повсякденних процесів, забезпечуючи надійну роботу критичних індустріальних систем у складних умовах сучасного цифрового світу.

Висновки до розділу 1

У першому розділі було розглянуто ключові теоретичні аспекти кібербезпеки індустріальних мереж та Інтернету речей (IoT) у контексті критичної інфраструктури. Аналіз архітектури та особливостей функціонування цих систем показав, що сучасні індустріальні мережі дедалі частіше інтегруються з IT-системами, що відкриває нові можливості для моніторингу, керування та оптимізації виробничих процесів. Однак, така інтеграція супроводжується зростанням уразливостей, особливо внаслідок застосування загальнодоступних мережевих протоколів, недостатньої ізоляції систем

управління та застарілих технологій, які не були спочатку розроблені з урахуванням вимог до безпеки.

Класифікація загроз, дозволила систематизувати основні типи ризиків, які виникають у сфері індустріального IoT. Серед найбільш критичних загроз виокремлено несанкціонований доступ, шкідливе програмне забезпечення, перехоплення або модифікація трафіку, атаки на фізичні пристрої, порушення доступності та достовірності даних. Важливо зазначити, що в умовах критичної інфраструктури наслідки кіберінцидентів можуть мати не лише економічний, але й соціальний або навіть техногенний характер, що робить забезпечення кіберзахисту стратегічним пріоритетом національного рівня.

Огляд існуючих методів дослідження кіберзагроз продемонстрував, що сучасні підходи включають як традиційні методи — підписне та поведінкове виявлення, так і інноваційні — на основі машинного навчання, моделей загроз (наприклад, MITRE ATT&CK), а також автоматизовану обробку телеметричних даних. Комплексне застосування цих методів дозволяє ефективніше виявляти атаки, прогнозувати можливі сценарії розвитку подій та підвищувати загальну стійкість систем.

Таким чином, перший розділ створює цілісну теоретичну базу для подальшого дослідження проблем кібербезпеки в індустріальних мережах та IoT. Отримані результати підкреслюють необхідність комплексного підходу, що охоплює як технічні, так і організаційні аспекти захисту, з урахуванням специфіки об’єктів критичної інфраструктури.

РОЗДІЛ 2
РОЗРОБКА МЕТОДУ ДОСЛІДЖЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ ДЛЯ ІНДУСТРІАЛЬНИХ МЕРЕЖ ТА IOT

2.1. Формування вимог до методу дослідження загроз кібербезпеки

Дослідження загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі потребує чітко визначених вимог до методу, який забезпечить ефективний аналіз, виявлення та нейтралізацію загроз. У цьому розділі будуть розглянуті основні критерії ефективності методу, а також приклади реалізації подібних методів у розвинених країнах і в Україні.

Для того щоб метод дослідження загроз кібербезпеки був ефективним, він повинен відповідати ряду важливих критеріїв. Передусім, він має бути комплексним і охоплювати всі рівні кіберзахисту — від фізичної безпеки до захисту програмного забезпечення та комунікацій. Наприклад, у США та країнах ЄС застосовується принцип "Defense-in-Depth", який передбачає багаторівневий захист мережі, даних та доступу.

Оскільки загрози у сфері кібербезпеки постійно еволюціонують, метод повинен бути адаптивним і гнучким, щоб своєчасно оновлюватися відповідно до актуальних викликів.

У Європейському Союзі, наприклад, впроваджено концепцію "Threat Intelligence Sharing", яка передбачає постійний обмін інформацією про нові кіберзагрози між країнами та організаціями. Не менш важливою є автоматизація процесів виявлення загроз.

Метод повинен включати сучасні інструменти, здатні в реальному часі аналізувати мережевий трафік, виявляти аномалії у поведінці пристроїв та оцінювати рівень їхньої вразливості.

Так, у Японії активно застосовуються AI-based cybersecurity системи для виявлення загроз в IoT-мережах промислових підприємств. Метод також має бути сумісним із міжнародними стандартами кібербезпеки, такими як IEC 62443, NIST SP 800-82 чи ISO/IEC 27001.

Наприклад, у Німеччині реалізовано концепцію "Industrie 4.0 Security Framework", яка дозволяє інтегрувати стандарти NIST та IEC у виробничі мережі.

Важливою характеристикою ефективного методу є швидкість реагування на кіберінциденти. У США, наприклад, функціонує система CISA (Cybersecurity and Infrastructure Security Agency), яка в режимі реального часу моніторить загрози та координує заходи з протидії атакам на критичну інфраструктуру.

Ще одним ключовим аспектом є масштабованість. Метод повинен бути придатним як для малих підприємств, так і для масштабних індустріальних об’єктів.

Франція, зокрема, використовує систему CyberShield, яка забезпечує кіберзахист як на рівні національної критичної інфраструктури, так і для малого бізнесу. Крім того, важливою є здатність методу визначати рівні ризику, класифікуючи загрози за рівнем критичності та пріоритетності.

У Японії підходи до дослідження та протидії кіберзагрозам є системними, інноваційними та глибоко інтегрованими на національному рівні. Країна приділяє особливу увагу державно-приватному партнерству, стандартам безпеки, а також використанню новітніх технологій, таких як AI і IoT, у сфері кіберзахисту.

В Ізраїлі впроваджено систему Cyber Threat Prioritization, що дозволяє державним структурам та підприємствам ефективно оцінювати ризики та оптимізувати розподіл ресурсів. Зрештою, метод має бути зручним у використанні та доступним для операторів промислових систем.

У ЄС, наприклад, розроблено інструмент Cyber Risk Management Toolbox, який допомагає компаніям оцінювати загрози без потреби у глибоких технічних знаннях [9].

Практика реалізації методів дослідження загроз кібербезпеки у розвинених країнах, таблиця 2.1.

Таблиця 2.1.

Практика реалізації методів дослідження загроз кібербезпеки у розвинених країнах

Країна	Основні методи дослідження загроз кібербезпеки
США	- CISA координує кіберзахист промислових систем.
	- Використання AI-аналізу мережевого трафіку для виявлення аномалій.
	- Підхід MITRE ATT&CK для моделювання атак.
	- Взаємодія державних структур та приватних компаній для обміну інформацією про загрози.
Німеччина	- В рамках Industrie 4.0 впроваджено стандарти IEC 62443 та ISO 27001.
	- BSI розробляє рекомендації щодо безпеки ICS та IoT.
	- Використання системи SIEM для аналізу загроз у реальному часі.
Японія	- Активний розвиток AI-базованих підходів до аналізу кіберзагроз.
	- Методика Threat Intelligence Sharing для співпраці між підприємствами та урядом.
	- Державна система JP-CERT аналізує загрози критичної інфраструктури.
Ізраїль	- National Cyber Directorate координує заходи кіберзахисту.
	- Підхід Cyber Threat Intelligence для передбачення атак.
	- Система Cyber Dome автоматично аналізує загрози у промислових мережах.

Дослідження загроз кібербезпеки є стратегічним пріоритетом для розвинених країн, і кожна держава застосовує власні методи для забезпечення захисту. США робить акцент на штучному інтелекті та взаємодії між урядом і бізнесом, тоді як Німеччина зосереджується на стандартизації та управлінні загрозами в реальному часі. Японія активно розвиває AI-інструменти та механізми обміну даними між організаціями. Ізраїль використовує розвинену

систему прогнозування атак і автоматичного аналізу загроз. Всі ці підходи демонструють, що ефективний кіберзахист базується на поєднанні технологій, стандартів та співпраці між державою і бізнесом. В Україні кібербезпека критичної інфраструктури регулюється Законом "Про основні засади забезпечення кібербезпеки України" та іншими нормативними актами. Основні проблеми - відсутність чіткої методології оцінки загроз, низький рівень впровадження міжнародних стандартів IEC 62443 та NIST, недостатній рівень автоматизації виявлення загроз. Однак, є позитивні зрушення, в Україні створено Національний координаційний центр кібербезпеки (НКЦК), який займається дослідженням загроз та розроблено Систему кіберзахисту державних інформаційних ресурсів для моніторингу атак на критичну інфраструктуру, запроваджено тісну співпрацю з ЄС та НАТО у сфері кібербезпеки [10].

Метод дослідження загроз кібербезпеки має відповідати сучасним міжнародним стандартам та критеріям ефективності, включаючи комплексність, адаптивність, автоматизацію та швидкість реагування. У розвинених країнах успішно впроваджуються такі підходи, як AI-моніторинг, аналіз загроз у реальному часі та обмін кіберінформацією, що може бути корисним для України.

Врахування технологічної неоднорідності систем у критичній інфраструктурі та промислових мережах є одним із ключових аспектів забезпечення кібербезпеки. Це обумовлено тим, що сучасні індустріальні системи складаються з різних компонентів, які були розроблені у різні часові періоди, часто від різних виробників і з використанням несумісних технологій. Додатково ситуацію ускладнює інтеграція старих OT-систем (Operational Technology) із сучасними IT-рішеннями, що створює значну кількість потенційних вразливостей.

Однією з головних проблем є наявність в одній індустріальній мережі обладнання з різними протоколами зв’язку. Наприклад, у промислових середовищах можуть використовуватися такі стандарти, як Modbus, Profibus, EtherNet/IP та OPC-UA, які мають різні механізми шифрування, автентифікації та контролю доступу. Взаємодія цих протоколів у спільній мережі створює

ризики, оскільки недостатній рівень безпеки одного з них може бути використаний атакувальниками для отримання несанкціонованого доступу до всієї системи. Деякі промислові протоколи не передбачають механізмів кібербезпеки, оскільки були розроблені ще до масового поширення інтернету і кіберзагроз. Це змушує організації застосовувати додаткові шари безпеки, такі як VPN, шлюзи безпеки та сегментовані мережі. Ще одним викликом є сумісність нових IoT-пристроїв із застарілими промисловими контролерами (PLC, DCS, SCADA). Наприклад, багато сучасних пристроїв Industrial IoT (IIoT) використовують хмарні обчислення для збору, аналізу та передачі даних, тоді як традиційні промислові системи розраховані на роботу в ізольованому середовищі без виходу у зовнішні мережі. Це створює потенційний ризик витоку даних або втручання зловмисників через слабкі точки в IoT-пристроях, що не мають належного рівня захисту. Відсутність єдиного підходу до автентифікації та управління доступом для таких систем ускладнює їхнє безпечне поєднання.

Крім того, технологічна неоднорідність проявляється у відмінностях між апаратними платформами та операційними системами, що використовуються в індустріальних мережах. Наприклад, промислові контролери можуть працювати на реальному часі (RTOS), тоді як інформаційні системи підприємства використовують Windows або Linux. Це означає, що методи забезпечення безпеки, які добре працюють у стандартних IT-середовищах, можуть бути неефективними для критичних OT-систем. Наприклад, використання традиційного антивірусу або оновлення безпеки може порушити стабільність роботи промислових контролерів, оскільки вони часто працюють безперервно у режимі 24/7. Ще одним аспектом є різні рівні критичності обладнання в індустріальних мережах.

Наприклад, деякі системи, такі як сенсори моніторингу температури чи вологості, можуть мати відносно низьку важливість, тоді як контролери, що керують виробничими процесами, є критично важливими для безперебійної роботи підприємства. Відповідно, до різних пристроїв слід застосовувати різні стратегії безпеки, щоб уникнути перевантаження інфраструктури зайвими

заходами контролю [11]. Це також стосується IoT-пристроїв, які можуть мати обмежені обчислювальні ресурси і не здатні ефективно працювати зі складними механізмами шифрування чи глибокого аналізу трафіку.

Одним із методів подолання технологічної неоднорідності є впровадження зональної сегментації мережі. Вона дозволяє розподілити пристрої та системи за рівнем критичності та типом технологій, що використовуються.

Наприклад, традиційні IT-системи можна розмістити в окремому сегменті з більш суворими політиками доступу, а OT-системи в іншому, ізольованому середовищі, з мінімальним доступом до зовнішніх мереж. Такий підхід застосовується в міжнародних стандартах безпеки, зокрема IEC 62443, де рекомендується створювати кілька рівнів захисту для різних частин індустріальної мережі.

Ще одним способом зниження ризиків є використання технологій віртуалізації та емуляції для тестування взаємодії різних компонентів системи перед їхнім реальним впровадженням. Це дозволяє оцінити потенційні вразливості, що можуть виникнути під час взаємодії обладнання від різних виробників або інтеграції старих і нових технологій.

Наприклад, у Німеччині застосовується методологія Digital Twin (цифровий двійник), яка дозволяє створювати віртуальні копії індустріальних мереж і тестувати безпеку взаємодії між компонентами без ризику порушення роботи реальних систем. Важливо також враховувати регуляторні вимоги до безпеки, які можуть відрізнятися залежно від регіону чи сфери застосування технологій.

Наприклад, у Європейському Союзі діють правила GDPR, що регулюють збереження та передачу персональних даних, у той час як у США кібербезпека критичної інфраструктури підпадає під юрисдикцію CISA (Cybersecurity and Infrastructure Security Agency). Це означає, що при розробці методів дослідження загроз для неоднорідних індустріальних систем слід враховувати відповідність місцевим законам та стандартам безпеки.

Останнім, але не менш важливим аспектом, є людський фактор у взаємодії з технологічно неоднорідними системами. Через різний рівень складності роботи з IT- та OT-системами, співробітники підприємств можуть мати різні компетенції у сфері кібербезпеки, що ускладнює ефективне впровадження заходів захисту. Наприклад, інженери, які працюють із промисловими системами, можуть не мати достатнього досвіду у налаштуванні IT-безпеки, тоді як фахівці з інформаційних технологій можуть бути недостатньо обізнані у специфіці роботи промислового обладнання. Це створює необхідність у розробці адаптивних політик безпеки, що будуть зрозумілими та зручними для всіх категорій користувачів. Таким чином, технологічна неоднорідність є важливим викликом у сфері кібербезпеки індустріальних мереж та IoT, оскільки вона ускладнює інтеграцію безпекових механізмів, створює додаткові ризики та потребує спеціалізованих підходів до захисту.

Подолання цих викликів можливе за рахунок зональної сегментації, використання цифрових двійників, впровадження міжнародних стандартів та підвищення рівня обізнаності співробітників щодо кіберзагроз [12].

У сучасному світі критична інфраструктура (КІ) залежить від технологічно складних індустріальних мереж та IoT-рішень, які постійно еволюціонують. Це вимагає розробки методів дослідження кібербезпеки, здатних адаптуватися до динамічних загроз та масштабуватися відповідно до розміру і складності системи. Масштабованість методу дослідження означає здатність ефективно застосовувати його як до малих локальних мереж, так і до великих, розподілених систем. Індустріальні підприємства та об’єкти критичної інфраструктури можуть складатися з тисяч IoT-пристроїв, розміщених у географічно віддалених регіонах.

Наприклад, енергетична мережа може включати тисячі підстанцій, кожна з яких має свою систему управління. Це створює виклики у зборі, аналізі та кореляції загрозових даних. Метод дослідження кібербезпеки має бути здатним обробляти великі обсяги телеметрії та логів у реальному часі, використовуючи

технології машинного навчання та поведінкового аналізу для виявлення аномалій.

Прикладом масштабованого підходу є використання SIEM (Security Information and Event Management) у великих промислових мережах. Такі системи, як IBM QRadar або Splunk, дозволяють аналізувати безпекові події в масштабі всієї організації, збираючи дані з різних джерел та виявляючи загрози на ранніх етапах. У Німеччині масштабованість кіберзахисту критичної інфраструктури досягається завдяки впровадженню концепції Industrie 4.0, що передбачає централізований контроль та автоматизований аналіз ризиків у великих промислових екосистемах. Адаптивність методу передбачає його здатність швидко пристосовуватися до нових вразливостей, змін у мережевій архітектурі та появи нових типів атак.

Наприклад, у 2022 році спостерігалося зростання атак на енергетичні системи через використання вразливостей у VPN-каналах віддаленого доступу. Метод дослідження кібербезпеки має передбачати регулярне оновлення бази знань про актуальні загрози, автоматичне виявлення нових атак та інтеграцію з системами розподіленого виявлення загроз (Threat Intelligence Platforms, TIP).

Важливим аспектом є можливість адаптації методу до різних рівнів критичності об'єкта. Наприклад, методологія безпеки для атомної електростанції суттєво відрізняється від підходів до захисту міської водоочисної станції. Для цього застосовують зональну модель безпеки (IEC 62443), де кожен сегмент мережі отримує відповідний рівень захисту залежно від ризиків.

Кібербезпека критичної інфраструктури є не лише технологічною, а й соціально-етичною та правовою проблемою. Дослідження в цій сфері зачіпає конфіденційні дані, впливає на національну безпеку та може мати серйозні юридичні наслідки. Одна з головних етичних проблем у дослідженні кібербезпеки – це баланс між захистом інформації та правами користувачів.

Наприклад, у процесі моніторингу кіберзагроз системи можуть аналізувати особисті дані співробітників або користувачів. У такому разі важливо дотримуватися принципу "мінімально необхідного збору даних" (data

minimization) відповідно до міжнародних стандартів, таких як GDPR у Європейському Союзі. Іншим етичним викликом є використання технологій етичного хакінгу [13].

Проведення тестів на проникнення (penetration testing) в критичній інфраструктурі може спричинити збої у роботі обладнання або несанкціоноване втручання в операційні процеси. Наприклад, у 2020 році у США тестування безпеки енергомереж призвело до помилкового спрацювання системи аварійного вимкнення. Етичний підхід передбачає узгодження таких тестів із регуляторами та дотримання принципу “без руйнування” (non-destructive testing).

Юридичні питання кібербезпеки критичної інфраструктури охоплюють як національне законодавство, так і міжнародні угоди. В Україні правове регулювання кібербезпеки здійснюється на основі Закону "Про основні засади забезпечення кібербезпеки України", який визначає порядок захисту критичної інфраструктури. Крім того, діє Національний центр кібербезпеки при РНБО, який координує заходи щодо запобігання кіберзагрозам. У країнах ЄС питання кібербезпеки регулюються Директивою NIS2 (Network and Information Security Directive), яка зобов’язує операторів критичної інфраструктури впроваджувати заходи захисту відповідно до ризиків. Наприклад, у Німеччині дія цього документа регламентується Федеральним відомством з інформаційної безпеки (BSI), яке проводить регулярні аудити кібербезпеки об'єктів КІ.

Одним із ключових викликів є визначення відповідальності за кіберінциденти. Наприклад, якщо атака на критичну інфраструктуру відбувається через вразливість у програмному забезпеченні стороннього постачальника, то постає питання, хто має нести відповідальність – виробник ПЗ, оператор мережі чи держава.

У США діє принцип "спільної відповідальності" (shared responsibility model), згідно з яким як приватний бізнес, так і урядові структури зобов’язані співпрацювати у сфері кіберзахисту. Іншою складною проблемою є юрисдикція кіберзлочинів. Якщо атака на українську енергетичну систему здійснюється з серверів у іншій країні, то відповідно до міжнародного права необхідно

взаємодіяти з правоохоронними органами іншої держави. Такі випадки регулюються Будапештською конвенцією про кіберзлочинність, учасником якої є й Україна. Розробка методів кібербезпеки критичної інфраструктури не повинна порушувати права громадян на конфіденційність і свободу інформації.

Впровадження масового моніторингу мереж може суперечити принципам демократичного суспільства, якщо відсутній належний нагляд з боку державних інституцій або судової влади [14].

Наприклад, у Китаї діє система "соціального кредиту", яка використовує кіберспостереження для контролю поведінки громадян, що викликає серйозні етичні суперечки.

Таким чином, розробка та впровадження методів кібербезпеки для критичної інфраструктури має враховувати як технологічні аспекти, так і правові та етичні питання. Забезпечення відповідності міжнародним стандартам, дотримання принципів мінімального збору даних і захист прав громадян є ключовими елементами комплексного підходу до кібербезпеки.

2.2. Розробка багаторівневої моделі загроз для індустріальних мереж та IoT

Розробка багаторівневої моделі загроз для індустріальних мереж та IoT у критичній інфраструктурі передбачає комплексний підхід, який враховує взаємозв’язок між фізичними, мережевими, програмними та управлінськими рівнями безпеки. Основна ідея такої моделі полягає в тому, що загрози можуть виникати на різних рівнях системи, а їхнє поширення може мати каскадний ефект, що призводить до значних наслідків. Індустріальні мережі складаються з операційних технологій (OT), таких як SCADA, DCS та PLC, які безпосередньо керують фізичними процесами, а також інформаційних технологій (IT), що забезпечують управління та аналіз даних. Додатковим елементом стає Інтернет речей (IoT), який забезпечує моніторинг та автоматизацію.

Кожен із цих компонентів має свої вразливості, тому для ефективного управління кіберзагрозами необхідно враховувати всі можливі рівні атак. У розробленій моделі загроз визначено чотири ключові рівні: фізичний рівень, рівень комунікацій, рівень програмного забезпечення та рівень управління. На цьому рівні знаходяться промислові контролери, сенсори, виконавчі механізми та IoT-пристрої, що взаємодіють з фізичним середовищем.

Загрози на цьому рівні можуть включати фізичне втручання в обладнання, саботаж, шкідливий вплив на сенсори або механізми управління. Наприклад, у випадку атаки на енергомережі, хакери можуть змінювати показники датчиків температури або тиску, що спричинить некоректну роботу системи. Цей рівень відповідає за передавання даних між пристроями через дротові або бездротові канали.

Основними загрозами є атаки на мережеві протоколи, перехоплення даних, атаки типу "людина посередині" (MITM) та впровадження шкідливого коду через вразливі протоколи промислової автоматизації (наприклад, Modbus, OPC-UA або MQTT). Наприклад, у випадку атаки на водопостачальну систему зловмисники можуть змінювати дані, що передаються контролерам насосних станцій, викликаючи перевитрати води або аварії. На цьому рівні працюють операційні системи контролерів, SCADA-системи, аналітичне ПЗ та алгоритми машинного навчання, які використовуються для управління індустріальними процесами.

Однією з найбільших загроз є шкідливе програмне забезпечення (наприклад, хробак Stuxnet, що атакував центрифуги збагачення урану в Ірані) або вразливості у системах оновлення програмного забезпечення. Наприклад, атака NotPetya в 2017 році використовувала механізм оновлення бухгалтерського ПЗ, щоб поширити шифрувальник по всій українській критичній інфраструктурі. Цей рівень включає політики безпеки, методи автентифікації користувачів, управління доступом та контроль над мережевими сегментами.

Основними загрозами є соціальна інженерія, витік даних через компрометацію облікових записів, використання слабких паролів або

неправильне налаштування доступу. Наприклад, у випадку атаки на нафтопереробний завод у Саудівській Аравії (атакою Triton у 2017 році) зловмисники отримали доступ до систем безпеки через скомпрометовані облікові записи адміністраторів.

Однією з найбільших проблем у кібербезпеці критичної інфраструктури є взаємозв'язок загроз між рівнями. Наприклад, компрометація мережевого рівня (перехоплення даних або MITM-атака) може призвести до внесення змін у програмне забезпечення контролерів, що в свою чергу викличе фізичні пошкодження обладнання. Аналогічно, якщо зловмисник отримує доступ на рівень управління, він може змінити політики безпеки, спростивши проникнення на нижчі рівні системи.

Щоб ефективно управляти цими загрозами, модель безпеки має включати механізми розділення доступу, сегментацію мережі та контроль трафіку між рівнями. Наприклад, метод Zero Trust Security дозволяє забезпечити сувору перевірку кожного запиту між рівнями мережі та запобігати несанкціонованому доступу.

На схемі нижче зображено запропоновану багаторівневу модель загроз для індустріальних мереж та IoT у критичній інфраструктурі, рис.2.1.

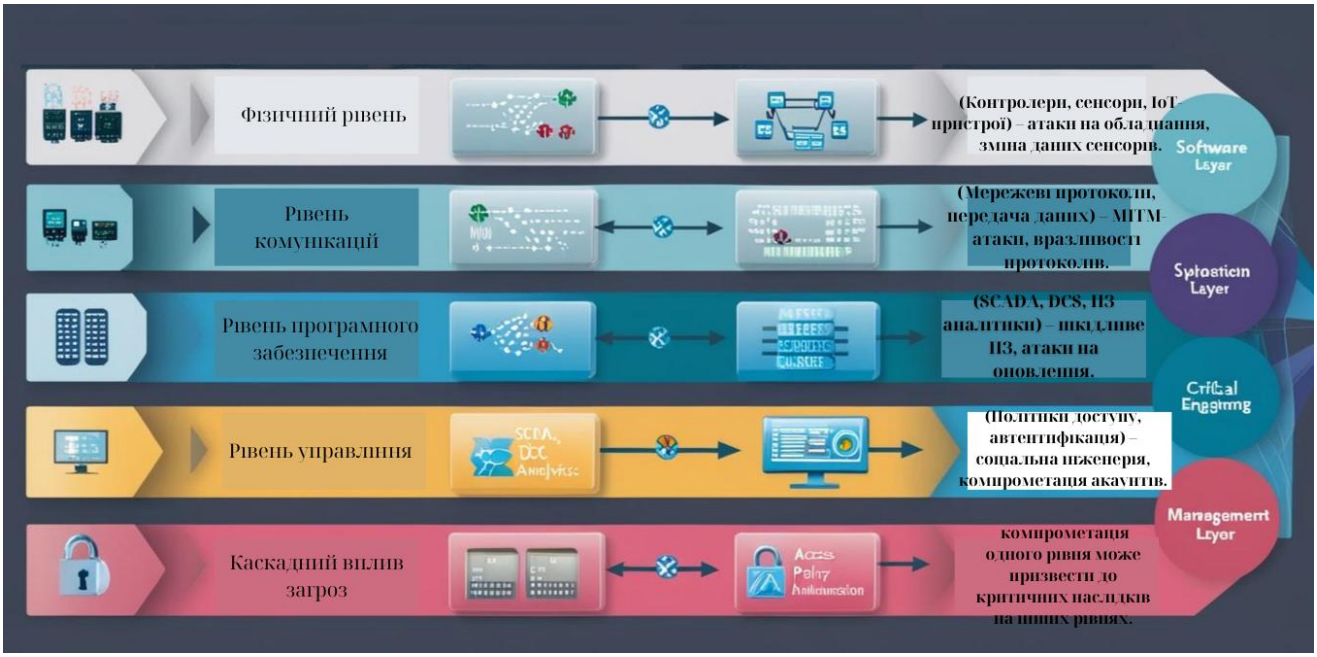

Рисунок 2.1 - Схема багаторівневої моделі загроз

Багаторівневий підхід дозволяє детальніше аналізувати атаки та розуміти їхні механізми. У 2015 році хакери атакували українську енергетичну систему, використовуючи кілька рівнів впливу: Спершу вони отримали доступ до облікових записів операторів через фішинг (рівень управління), потім вони модифікували SCADA-систему, щоб відключити підстанції (рівень програмного забезпечення).

Нарешті, вони атакували мережеві канали, щоб ускладнити відновлення системи (рівень комунікацій). Подібним чином, атака на нафтову компанію Saudi Aramco у 2012 році почалася з проникнення у корпоративну мережу через соціальну інженерію, що дозволило хакерам поширити шкідливий код на індустріальні системи управління.

Розроблена багаторівнева модель загроз демонструє необхідність комплексного підходу до кібербезпеки індустріальних мереж та IoT. Вона враховує фізичні, мережеві, програмні та управлінські аспекти захисту, дозволяючи оцінювати каскадний вплив атак та ефективно реагувати на загрози.

Для забезпечення захисту критичної інфраструктури необхідно впроваджувати багаторівневі механізми безпеки, зокрема сегментацію мережі, поведінковий аналіз аномалій та Zero Trust Security, що дозволить мінімізувати ризики та запобігати потенційним атакам [15].

Забезпечення кібербезпеки індустріальних мереж та IoT у критичній інфраструктурі потребує чіткої методики для ідентифікації та категоризації загроз. Цей процес включає аналіз активів, виявлення потенційних загроз, оцінку їхньої небезпеки та визначення категорій атак, що дозволяє розробити ефективні заходи протидії. Ідентифікація загроз є першим і найважливішим етапом у забезпеченні безпеки. Вона передбачає збір інформації про всі можливі вектори атак, вразливості системи та аналіз історичних випадків атак на подібні індустріальні системи. Основні етапи ідентифікації загроз:

1. Аналіз активів та їхньої критичності. Визначення ключових компонентів системи (контролери, IoT-пристрої, мережеве обладнання, сервери SCADA), які можуть стати ціллю атаки.

2. Виявлення вразливостей. Аналіз мережевих протоколів, методів аутентифікації, систем оновлення програмного забезпечення.

3. Оцінка загрозових векторів. Дослідження можливих способів атаки на об’єкт (фішинг, експлуатація вразливостей ПЗ, атаки типу "людина посередині", DoS-атаки тощо).

4. Використання threat intelligence. Аналіз даних з відкритих джерел, баз даних уразливостей (CVE, ICS-CERT) та звітів про атаки, щоб прогнозувати нові загрози.

Після ідентифікації загроз важливо їх класифікувати для подальшого аналізу та розробки відповідних заходів безпеки. Класифікація може здійснюватися за різними критеріями, такими як тип атаки, джерело загрози, рівень впливу та складність реалізації, рис.2.2.

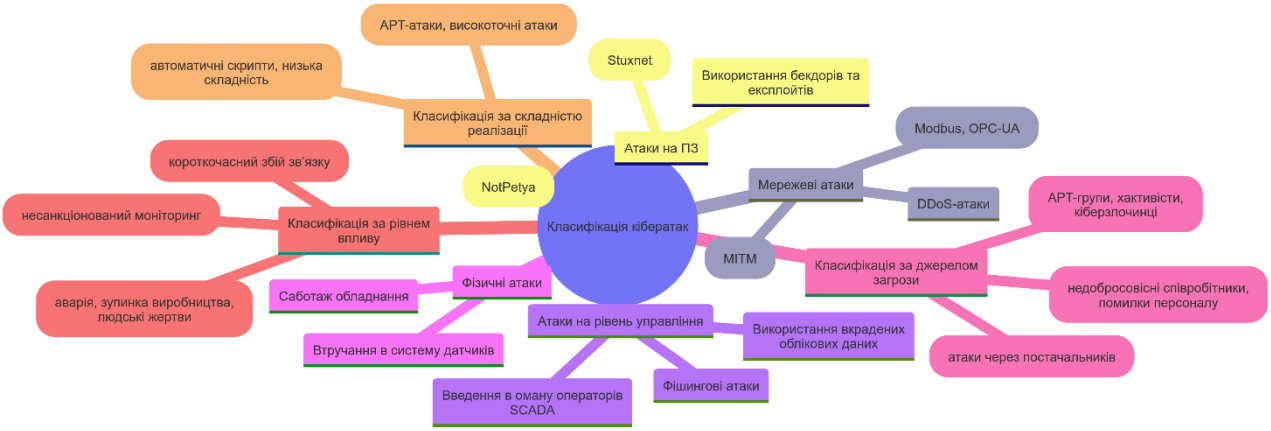

Рисунок 2.2 - Класифікація загроз

Для впровадження систематичного підходу до категоризації загроз можна використовувати такі методи:

1. NIST Cybersecurity Framework – поділ на п’ять етапів: ідентифікація, захист, виявлення, реагування, відновлення.

2. Методика STRIDE – класифікація загроз за категоріями (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).

3. Державні стандарти – IEC 62443 для промислових систем, NIST SP 800-82 для SCADA, ISO/IEC 27001.

Розглянемо конкретний сценарій атаки: проникнення в систему управління водопостачанням через вразливість у мережевому обладнанні.

- Ідентифікація
- Мета атаки перехоплення управління насосами.
- Вразливість незахищений доступ через Modbus-протокол.
- Вектор атаки MITM через слабке шифрування.
- Категоризація
- Тип атаки мережевий перехоплення трафіку.
- Джерело зовнішній хакер.
- Рівень впливу критичний (може спричинити затоплення).
- Складність середня (потребує технічних навичок).

Методика ідентифікації та категоризації загроз у критичній інфраструктурі дозволяє систематично аналізувати ризики та розробляти ефективні заходи безпеки. Використання міжнародних стандартів (NIST, IEC 62443), а також комбінування підходів до класифікації загроз (тип атаки, джерело, рівень впливу) сприяє побудові надійної системи кіберзахисту.

Оцінка потенційного впливу кіберзагроз на індустріальні мережі та IoT у критичній інфраструктурі є ключовим аспектом управління ризиками. Вона дозволяє визначити рівень загрози, оцінити можливі наслідки та розробити відповідні заходи захисту. Для цього використовуються різні метрики, що враховують технічні, економічні та організаційні фактори.

Метрики повинні бути універсальними, але водночас адаптивними до специфіки кожної індустрії. Вони охоплюють такі аспекти, як імовірність успішної атаки, рівень вразливості системи, потенційні фінансові збитки, тривалість відновлення після атаки та вплив на критичні процеси.

Одним із основних підходів до оцінки загроз є використання комбінованих методик, що включають кількісні та якісні показники. Наприклад, метрики можуть визначати, наскільки серйозним є вплив загрози, виходячи з її здатності порушити виробничий процес, спричинити людські жертви чи завдати

фінансових втрат. Вони також враховують складність реалізації атаки, її потенційний радіус дії та можливості захисту від неї.

Метрики оцінки потенційного впливу загроз можна класифікувати за рівнем деталізації. Високорівневі метрики застосовуються для стратегічного планування та прийняття управлінських рішень, тоді як низькорівневі використовуються для оцінки конкретних атак та їх наслідків, таблиця 2.1.

Таблиця 2.1.

Метрики оцінки потенційного впливу загроз

Метрика	Опис	Одиниці виміру
Імовірність успішної атаки	Визначає, наскільки легко атакуючий може скомпрометувати систему	Від 0 (мінімальна) до 1 (максимальна)
Час виявлення атаки	Середній час, необхідний для виявлення кіберзагрози	Години/дні
Час реагування	Час, необхідний для нейтралізації атаки	Години/дні
Час відновлення	Час, необхідний для повного відновлення системи після атаки	Години/дні
Вартість збитків	Прямі та непрямі фінансові втрати, спричинені атакою	Долари/євро
Вплив на бізнес-процеси	Визначає, наскільки загроза впливає на критичні функції	Низький/середній/високий
Вплив на безпеку людей	Аналіз ризиків для здоров'я та життя працівників	Відсутній/помірний/критичний
Радіус поширення атаки	Чи впливає атака на окремий вузол або всю систему	Локальний/глобальний
Складність реалізації атаки	Чи потребує атака високої технічної підготовки	Низька/середня/висока

Ефективна система кібербезпеки критичної інфраструктури має поєднувати як технічні, так і організаційні заходи. Використання тільки технологічних рішень, таких як фаєрволи, антивіруси та системи виявлення вторгнень, без належної організації процесів безпеки є неефективним. Важливою

частиною захисту є людський фактор, політики управління доступом та регулярні аудити безпеки.

Технічні заходи безпеки охоплюють широкий спектр технологій, спрямованих на виявлення та запобігання кіберзагрозам. Наприклад, використання сегментації мережі дозволяє обмежити можливість розповсюдження атаки, а впровадження багатофакторної автентифікації знижує ризик несанкціонованого доступу. Крім того, системи поведінкового аналізу та виявлення аномалій здатні ідентифікувати підозрілу активність у режимі реального часу.

Проте технічні заходи мають доповнюватися організаційними політиками безпеки. Наприклад, навіть найсучасніші технології будуть безсилими, якщо працівники підприємства використовують слабкі паролі або відкривають фішингові листи [16]. Тому критично важливими є програми навчання персоналу, розробка чітких інструкцій щодо дій у разі кіберінциденту та регулярне тестування співробітників на здатність розпізнавати атаки.

Іншою важливою складовою організаційної безпеки є управління доступом та моніторинг активності користувачів. Система має забезпечувати диференційований доступ, при якому кожен співробітник має лише ті права, які необхідні для виконання його завдань. Це дозволяє мінімізувати ризики, пов’язані з внутрішніми загрозами, та зменшити потенційний вплив компрометації облікових записів.

Крім того, сучасний підхід до кібербезпеки критичної інфраструктури передбачає активну взаємодію між підприємствами та державними органами. У багатьох країнах створені спеціальні агентства, які займаються моніторингом загроз та наданням рекомендацій щодо захисту. Наприклад, у США функціонує CISA (Cybersecurity and Infrastructure Security Agency), яка координує кіберзахист критичних об’єктів, тоді як у ЄС діє ENISA (European Union Agency for Cybersecurity). В Україні аналогічні функції виконує Державна служба спеціального зв’язку та захисту інформації.

З огляду на складність кіберзагроз, особливо небезпечними є цільові атаки типу APT (Advanced Persistent Threat), які можуть залишатися непоміченими впродовж тривалого часу. Для боротьби з ними необхідні не лише традиційні заходи кіберзахисту, а й розвідка загроз (threat intelligence), а також активне використання аналітичних платформ на основі штучного інтелекту.

Успішна інтеграція технічних та організаційних аспектів безпеки передбачає тісну співпрацю між підрозділами інформаційної безпеки, адміністраторами мереж, виробничими департаментами та керівництвом підприємства. Кібербезпека більше не є лише проблемою IT-фахівців – це стратегічне питання, яке впливає на стабільність роботи критичних систем, національну безпеку та фінансову стійкість підприємств.

Отже, ефективний підхід до оцінки потенційного впливу загроз базується на чітких метриках, які дозволяють кількісно оцінювати ризики та приймати обґрунтовані рішення. При цьому технічні заходи безпеки мають доповнюватися організаційними стратегіями, що забезпечують комплексний захист критичної інфраструктури від сучасних кіберзагроз.

2.3. Алгоритм комплексного аналізу вразливостей та оцінки ризиків

Комплексний аналіз вразливостей та оцінка ризиків є ключовими етапами у процесі забезпечення інформаційної безпеки. Даний алгоритм спрямований на виявлення, класифікацію та оцінку ризиків, пов’язаних із можливими загрозами для інформаційних систем. Методика передбачає послідовне застосування кількох етапів, що дозволяють отримати найбільш точну картину поточного стану безпеки. На етапі 1 відбувається ідентифікація компонентів системи. На цьому етапі здійснюється визначення всіх компонентів системи, що підлягають аналізу. До них відносяться: програмне забезпечення (операційні системи, бази даних, веб-додатки, сервери), апаратне забезпечення (сервери, робочі станції, мережеве обладнання), комунікаційні канали (локальні мережі, VPN, хмарні рішення), політики та процедури (регламенти, політики доступу, правила

автентифікації), ідентифікація цих компонентів дозволяє визначити межі аналізу та забезпечити комплексний підхід до оцінки ризиків. Наступний другий етап це виявлення вразливостей, після ідентифікації компонентів здійснюється пошук вразливостей за допомогою різних методів, використання автоматизованих сканерів вразливостей (Nessus, OpenVAS, Acunetix), аналіз журналів подій та лог-файлів, перевірка конфігурацій систем, виконання пентесту (етичного хакінгу). Оцінка відповідності політикам безпеки та стандартам (ISO 27001, NIST, PCI DSS), на цьому етапі формується список потенційних вразливостей із зазначенням їх характеристик.

Етап 3 - класифікація вразливостей – де виявлені вразливості класифікуються за різними критеріями:

- За рівнем критичності: високий, середній, низький
- За типом**:** конфігураційні помилки, уразливості коду, відсутність оновлень, проблеми з автентифікацією
- За впливом на систему: компрометація даних, порушення цілісності, відмова в обслуговуванні

Це допомагає визначити, які з них є найбільш небезпечними та вимагають негайного усунення.

Оцінка ризиків виконується шляхом аналізу ймовірності експлуатації вразливості та її потенційного впливу. Використовується матриця ризиків, у якій перетинаються фактори загрози, таблиця 2.2.

Таблиця 2.2.

Оцінка ризиків

Вірогідність / Вплив	Низький	Середній	Високий
Низька	Мінімальний ризик	Низький ризик	Середній ризик
Середня	Низький ризик	Середній ризик	Високий ризик
Висока	Середній ризик	Високий ризик	Критичний ризик

На основі цієї оцінки формулюються рекомендації щодо зниження ризиків. І заключний етап 5. Відбувається розробка рекомендацій та плану дій

На фінальному етапі створюється план усунення вразливостей, що може включати встановлення оновлень безпеки, зміна конфігурацій систем, впровадження додаткових механізмів автентифікації, посилення політик доступу, проведення навчань персоналу з питань кібербезпеки.

Комплексний аналіз вразливостей дозволяє мінімізувати потенційні ризики та підвищити загальний рівень безпеки інформаційної системи. Постійний моніторинг та періодичне повторення цього алгоритму забезпечують стійкість системи до нових загроз.

Оцінка ризиків є ключовим етапом забезпечення безпеки інформаційних систем та мереж. Вона включає кількісний і якісний аналіз.

Першим кроком є формулювання мети аналізу ризиків, що передбачає виявлення потенційних загроз, оцінку ймовірності їх реалізації та розробку заходів для їх зниження. Далі відбувається ідентифікація активів, які можуть зазнати впливу ризиків. До них належать програмне та апаратне забезпечення, конфіденційна інформація, доступність сервісів і даних [17].

На наступному етапі визначаються загрози та вразливості, що можуть бути внутрішніми або зовнішніми. До загроз належать кібератаки, витік конфіденційної інформації та відмови обладнання, а вразливості визначаються шляхом аналізу можливих шляхів компрометації активів. Аналіз наслідків реалізації ризиків включає фінансові, репутаційні, операційні та юридичні аспекти. Наприклад, витік персональних даних може призвести до штрафів і втрати довіри клієнтів.

Далі обирається методика оцінки ризиків, яка може бути якісною або кількісною. Якісний аналіз базується на експертних оцінках рівня критичності загроз і не потребує точних даних, але залежить від досвіду фахівців. Кількісний аналіз використовує статистичні дані, ймовірності загроз і оцінку вартості можливих втрат, що розраховується за формулою:

$$R = P * I$$

де R – рівень ризику, P – ймовірність реалізації загрози, I – можливі збитки.

На основі отриманих результатів визначається допустимий рівень ризику, який організація може прийняти без критичних наслідків. Завершальним етапом є розробка стратегії управління ризиками, що може включати уникнення ризику шляхом відмови від небезпечних процесів, його зниження через впровадження заходів захисту, передачу ризику (наприклад, страхування або аутсорсинг безпеки) або прийняття ризику, якщо витрати на його зниження перевищують потенційні збитки.

Оцінка ризиків – це безперервний процес, який потребує регулярного перегляду для адаптації до нових загроз, рис.2.3.

Рисунок 2.3 - Кроки оцінки ризиків

Оцінка ризиків є безперервним процесом, що вимагає регулярного перегляду для адаптації до нових загроз. Вона складається з кількох послідовних етапів.

Першим кроком є визначення цілей аналізу ризиків, що передбачає встановлення ключових завдань, таких як виявлення загроз, оцінка їхнього впливу та розробка заходів захисту. Далі відбувається ідентифікація активів і

визначення їхньої цінності, що дозволяє зрозуміти, які ресурси можуть зазнати впливу потенційних загроз.

На наступному етапі аналізуються загрози та вразливості. Це можуть бути як внутрішні, так і зовнішні фактори, що здатні завдати шкоди інформаційній системі. Після цього проводиться оцінка наслідків реалізації ризиків, включаючи фінансові, репутаційні, операційні та юридичні аспекти.

Далі вибирається методика оцінки ризиків: якісний аналіз базується на експертних оцінках, а кількісний використовує статистичні дані та розрахунки потенційних втрат. На основі отриманих результатів визначається допустимий рівень ризику, який організація може прийняти без значних негативних наслідків.

Наступним кроком є розробка стратегії управління ризиками. Вона може включати уникнення ризику шляхом відмови від певних процесів, його зниження через впровадження заходів безпеки, передачу ризику шляхом страхування або аутсорсингу, а також прийняття ризику, якщо витрати на його зниження є надмірно високими.

Останнім етапом є моніторинг та оновлення оцінки ризиків, що забезпечує адаптацію до нових загроз і підтримку високого рівня кібербезпеки організації. Такий комплексний підхід дозволяє ефективно управляти ризиками та мінімізувати потенційні загрози [18].

Прогнозування динаміки загроз є важливою складовою системи управління інформаційною безпекою.

Його мета — передбачити можливі загрози, оцінити їхній вплив та розробити превентивні заходи. Для цього використовують різні методи аналізу та моделювання, які базуються на історичних даних, поведінкових патернах та аналітичних підходах.

Прогнозування загроз є важливим елементом кібербезпеки, який передбачає систематичне дослідження тенденцій розвитку атак, технологічних змін та дій зловмисників. Завдяки глибокому аналізу й використанню сучасних

аналітичних методів можна значно підвищити ефективність захисту інформаційних систем.

Одним із ключових аспектів цього процесу є виявлення закономірностей у поведінці атакуючих суб’єктів. Це дозволяє зрозуміти їхні мотиви, методи та тактики, що сприяє розробці більш дієвих механізмів протидії. Крім того, прогнозування загроз дає змогу оцінити ефективність наявних механізмів захисту, виявити їхні слабкі місця та своєчасно вдосконалити заходи безпеки. Ще одним важливим напрямом є розробка стратегій реагування на потенційні загрози. Використання прогностичних моделей допомагає створити алгоритми дій у разі виникнення небезпеки, що мінімізує негативні наслідки атак. Окрім цього, своєчасне усунення вразливостей дозволяє запобігти можливим атакам, що є ключовим фактором у забезпеченні стійкості інформаційних систем.

Методи прогнозування загроз можуть бути різними. Кількісні підходи ґрунтуються на використанні математичних моделей, статистичних даних та алгоритмів машинного навчання. Це дозволяє аналізувати великі обсяги інформації, знаходити приховані закономірності та тенденції, а також здійснювати точні розрахунки й прогнози. За допомогою таких підходів можна об'єктивно оцінювати ситуації, моделювати можливі сценарії розвитку подій та приймати обґрунтовані управлінські рішення. Вони особливо корисні в тих галузях, де важлива точність, ефективність і можливість враховувати численні фактори — наприклад, у фінансах, логістиці, охороні здоров’я чи маркетинговій аналітиці.

Водночас якісні методи базуються на експертних оцінках і сценарному аналізі, які дають змогу передбачити розвиток загроз, спираючись на досвід фахівців і аналіз ситуацій з минулого. Вони допомагають глибше зрозуміти контекст подій, врахувати соціальні, політичні та культурні чинники.

Таким чином, прогнозування загроз є комплексним процесом, що дозволяє не лише аналізувати поточний стан кібербезпеки, а й передбачати майбутні ризики, забезпечуючи проактивний підхід до їхнього усунення.

Методи прогнозування загроз краще представити у табличці 2.3.

Таблиця 2.3.

Методи прогнозування

Тип методу	Метод	Опис
Кількісні методи	Статистичний аналіз	Використовує історичні дані про інциденти для визначення частоти та трендів атак. Дозволяє будувати ймовірнісні моделі загроз, аналізувати часові ряди та кореляцію між різними факторами загроз.
	Машинне навчання та ШІ	Використовує алгоритми класифікації, кластеризації та нейронні мережі для виявлення аномальної активності. Дозволяє ідентифікувати нові загрози на основі патернів атак та динамічно оновлювати моделі.
	Імітаційне моделювання (Метод Монте-Карло)	Дозволяє оцінити ймовірність реалізації загроз шляхом багаторазового моделювання сценаріїв атак. Використовується для розрахунку фінансових та операційних ризиків.
	Регресійний аналіз	Визначає залежність між факторами загроз та їхнім впливом на інформаційні системи. Дозволяє оцінювати майбутню частоту атак на основі змінних, що впливають на рівень ризику.
Якісні методи	Сценарний аналіз	Побудова можливих сценаріїв розвитку загроз на основі експертних оцінок. Використовується для стратегічного планування захисту.
	Метод Delphi	Залучає групу експертів для визначення потенційних загроз та їхнього впливу. Дозволяє отримати обґрунтовані прогнози шляхом ітеративного узгодження оцінок.
	SWOT-аналіз	Оцінює сильні та слабкі сторони системи безпеки, можливості та загрози. Дозволяє сформувати стратегію управління ризиками.
	Факторний аналіз загроз	Визначає ключові фактори, що впливають на зростання рівня загроз (наприклад, розвиток нових технологій, геополітичні фактори).

Ця таблиця узагальнює основні методи прогнозування загроз, поділяючи їх на кількісні та якісні. Кількісні методи базуються на математичних моделях, статистичних підходах та алгоритмах машинного навчання, що дозволяє проводити точний аналіз ризиків і будувати прогностичні моделі. Натомість якісні методи використовують експертні оцінки, сценарний підхід і аналітичні інструменти, що сприяє стратегічному плануванню кібербезпеки. Використання обох підходів у комплексі допомагає максимально точно оцінювати та прогнозувати потенційні загрози.

Прогнозування загроз є складним і багатоетапним процесом, який поєднує як кількісні, так і якісні методи аналізу. Кожен із цих методів має свої переваги та недоліки, що слід враховувати при виборі інструментів прогнозування. Кількісні методи, такі як статистичний аналіз, забезпечують швидкість обробки даних та високу точність прогнозів за стабільних умов. Проте вони мають обмеження, оскільки не враховують появу нових, раніше невідомих типів загроз [19].

Машинне навчання є адаптивним інструментом, що здатен виявляти навіть невідомі загрози, однак потребує значних обчислювальних ресурсів і великих обсягів даних для навчання. Імітаційне моделювання, наприклад, метод Монте-Карло, дозволяє створювати складні сценарії атак та оцінювати ймовірність їхньої реалізації, але його результати значною мірою залежать від якості початкових даних. Якісні методи, зокрема сценарний аналіз, допомагають у стратегічному плануванні, дозволяючи передбачити можливі варіанти розвитку загроз на основі експертних оцінок.

Однак вони є суб’єктивними та залежать від кваліфікації аналітиків. SWOT-аналіз забезпечує комплексний підхід до оцінки ризиків, враховуючи сильні й слабкі сторони системи, можливості та загрози, проте його точність є відносною і не завжди придатною для детального прогнозування. Процес прогнозування загроз починається зі збору даних про попередні інциденти, що дозволяє аналізувати типові сценарії атак та їхні наслідки. Далі проводиться визначення ключових факторів ризику, які можуть впливати на безпеку системи,

після чого застосовуються математичні моделі та експертні методи для побудови прогнозів. Важливим етапом є формування сценаріїв майбутніх загроз, що дає змогу заздалегідь підготувати ефективні механізми протидії. Оцінка потенційного впливу загроз на систему дозволяє визначити пріоритетність заходів реагування та оптимізувати стратегію безпеки. На основі отриманих результатів розробляється стратегія управління ризиками, яка включає запобіжні заходи, план реагування на інциденти та механізми зниження загроз.

Важливо пам’ятати, що процес прогнозування не є одноразовим – він потребує постійного моніторингу та коригування на основі нових даних, оскільки методи атак постійно змінюються та вдосконалюються. Завдяки такому підходу можна значно підвищити рівень захищеності інформаційних систем і забезпечити ефективне управління ризиками [20].

Ефективне прогнозування загроз дозволяє зменшити можливі ризики та втрати організацій шляхом завчасного реагування на потенційні атаки. Динаміка загроз постійно змінюється через:

- Еволюцію кіберзлочинності – зловмисники постійно вдосконалюють свої методи.
- Розвиток технологій – нові технологічні рішення можуть містити нові вразливості.
- Зростання обсягу даних – обробка великих масивів інформації вимагає складних алгоритмів безпеки.

А прогнозування в свою чергу дозволяє:

- Впроваджувати проактивні заходи захисту.
- Оптимізувати ресурси для кібербезпеки.
- Запобігати фінансовим та репутаційним втратам.

Прогнозування загроз відіграє ключову роль у забезпеченні інформаційної безпеки, допомагаючи організаціям змінити підхід до захисту даних. Замість того щоб діяти реактивно й реагувати на атаки вже після їхнього здійснення, компанії отримують можливість заздалегідь ідентифікувати потенційні загрози та вживати превентивних заходів. Це значно підвищує ефективність

кіберзахисту та мінімізує ризики. Окрім цього, прогнозування загроз сприяє оптимізації витрат на безпеку, дозволяючи організаціям раціонально розподіляти ресурси. Інвестиції спрямовуються на усунення найбільш критичних ризиків, що зменшує фінансові втрати та підвищує ефективність захисних заходів.

Ще одним важливим аспектом є зростання рівня довіри користувачів. Коли компанія забезпечує надійний захист персональних і корпоративних даних, це зміцнює репутацію та підвищує лояльність клієнтів, партнерів і співробітників. Таким чином, прогнозування загроз є не просто науковим напрямом, а життєво необхідним процесом, без якого неможливо уявити стабільний розвиток сучасних організацій в умовах зростаючих кіберзагроз. Це дозволяє не лише реагувати на атаки, а й будувати комплексну систему захисту, що адаптується до змін у цифровому середовищі.

Окремо слід поговорити про інструментарій виявлення загроз. Автоматизація аналізу загроз відіграє важливу роль у сучасних підходах до кібербезпеки, забезпечуючи швидке виявлення потенційних загроз, оцінку їхнього впливу та своєчасне прийняття рішень щодо реагування. Використання спеціалізованих інструментів дозволяє значно зменшити навантаження на фахівців з безпеки, підвищуючи ефективність систем захисту. Автоматизовані системи аналізу загроз охоплюють кілька ключових напрямків. По-перше, вони здійснюють постійний моніторинг мережевого трафіку, що дає змогу виявляти аномальну активність і підозрілі дії в режимі реального часу. По-друге, такі системи аналізують вразливості програмного забезпечення та додатків, скануючи їх на предмет потенційних загроз і слабких місць, які можуть бути використані зловмисниками.

Ще одним важливим аспектом є збір та обробка загрозових індикаторів, що відомі як Threat Intelligence. Це дозволяє ідентифікувати нові загрози, обмінюватися інформацією про атаки та оперативно оновлювати механізми захисту. Нарешті, автоматизовані системи допомагають оцінювати ризики та прогнозувати можливі атаки, що дає змогу організаціям заздалегідь готуватися

до потенційних загроз і знижувати їхній вплив на інформаційну інфраструктуру. Інструменти для аналізу загроз можна розділити на кілька категорій, рисунок 2.4.

Рисунок 2.4 - Інструменти для аналізу загроз

Розглянемо найпопулярніші з них. Системи SIEM (Security Information and Event Management) відіграють важливу роль у сучасній кібербезпеці, оскільки дозволяють збирати, аналізувати та корелювати дані про події безпеки з різних джерел. Завдяки цьому організації можуть оперативно виявляти потенційні загрози та своєчасно реагувати на інциденти. Однією з потужних SIEM-платформ є Splunk, яка забезпечує глибокий аналіз лог-файлів, виконує кореляцію подій та виявляє загрози в режимі реального часу. Вона також підтримує інтеграцію з модулями машинного навчання, що значно покращує ефективність аналізу. Ще одне популярне рішення – IBM QRadar, яке спеціалізується на моніторингу подій безпеки в корпоративних мережах. Воно не лише аналізує інциденти, а й автоматизує процес реагування, що дозволяє мінімізувати вплив атак.

AlienVault USM – це комплексна SIEM-система, яка має вбудований механізм аналізу загроз, включаючи технологію Threat Intelligence. Це забезпечує організаціям додатковий рівень захисту завдяки використанню актуальних даних про кібератаки. Для тих, хто шукає open-source рішення, Elastic Security є ефективним варіантом. Ця платформа, створена на базі Elastic Stack, дозволяє здійснювати детальний аналіз загроз, моніторити логи та забезпечувати ефективний захист інформаційних систем.

Сканери вразливостей допомагають виявляти відомі загрози у веб-додатках, мережах та операційних системах. Nessus — один з найпопулярніших комерційних сканерів вразливостей, що містить велику базу відомих загроз і дозволяє перевіряти конфігурацію систем. OpenVAS — open-source аналог Nessus, який використовується для виявлення вразливостей та сканування мережевих пристроїв. Burp Suite — потужний інструмент для аналізу безпеки веб-додатків, який допомагає знаходити SQL-ін'єкції, XSS та інші загрози. Nikto — веб-сканер, що перевіряє сайти на відомі вразливості, неправильні конфігурації та небезпечні файли. Інструменти Threat Intelligence забезпечують аналітичну інформацію про відомі загрози та допомагають швидко реагувати на атаки. MISP (Malware Information Sharing Platform) — платформа для обміну інформацією про кіберзагрози між організаціями. IBM X-Force Exchange — інструмент аналізу загроз, який містить актуальну базу даних про кіберзлочини. VirusTotal — онлайн-сканер файлів, який дозволяє перевіряти їх на наявність шкідливого коду за допомогою десятків антивірусних двигунів. Автоматизовані системи тестування на проникнення дозволяють виявляти слабкі місця шляхом симуляції атак на систему. Metasploit — найпотужніший фреймворк для тестування на проникнення, що містить сотні експлойтів. Kali Linux — операційна система з набором інструментів для пентестингу та аналізу загроз. Commix — інструмент для автоматичного виявлення та експлуатації командних ін'єкцій. SQLmap — автоматизує пошук та експлуатацію SQL-ін'єкцій у веб-додатках. Системи аналізу шкідливого ПЗ використовуються для дослідження поведінки шкідливих програм. Cuckoo Sandbox — пісочниця для динамічного

аналізу шкідливих файлів. Hybrid Analysis — онлайн-сервіс для аналізу загроз, що використовує поведінкові та статичні методи аналізу. Any.Run — інтерактивна пісочниця для аналізу вірусів та троянів у режимі реального часу.

Автоматизація аналізу загроз є критично важливою складовою сучасних систем кібербезпеки, особливо в умовах зростаючого обсягу цифрових даних, постійного підвищення складності атак та обмежених людських ресурсів для оперативного реагування. Основна перевага автоматизації полягає в її здатності забезпечувати безперервний моніторинг та обробку інформації з багатьох джерел одночасно — мережевих журналів, систем логування, телеметрії пристроїв, трафіку, а також зовнішніх джерел розвідки загроз (threat intelligence feeds).

Автоматизовані системи аналізу здатні у реальному часі проводити кореляцію подій, виявляти аномальні шаблони поведінки, класифікувати загрози за рівнем критичності та оперативно передавати результати в центри реагування на інциденти (SOC). Важливою перевагою є й те, що такі системи можуть самостійно приймати базові рішення щодо блокування підозрілих дій або ізоляції скомпрометованих вузлів, ще до того, як втручання здійснить людина. Це особливо актуально в умовах атак, що розвиваються дуже швидко, як-от атаки типу ransomware або атаки на відмову в обслуговуванні (DDoS), де кожна секунда має значення.

Інтеграція штучного інтелекту (AI) і машинного навчання (ML) у процес автоматизованого аналізу відкриває нові горизонти в забезпеченні проактивного захисту. Системи на базі ML здатні не лише виявляти вже відомі загрози, а й навчатися на основі нових зразків поведінки, постійно вдосконалюючи моделі розпізнавання атак. Наприклад, вони можуть виявляти складні багатовекторні атаки, які розгортаються поступово, маскуючись під легітимну активність. Завдяки глибокому аналізу контексту поведінки користувачів та пристроїв, такі системи можуть прогнозувати потенційні сценарії атак ще до того, як вони будуть реалізовані.

Крім технічних переваг, автоматизація також суттєво оптимізує ресурси організації. Вона знижує навантаження на фахівців із кібербезпеки, дозволяючи їм зосередитися на аналізі найкритичніших інцидентів і прийнятті стратегічних рішень. Також це дає змогу стандартизувати процеси реагування, уникати суб'єктивізму при оцінці інцидентів і забезпечити відповідність регуляторним вимогам шляхом документування всіх етапів реагування.

З огляду на виклики, з якими стикаються критичні інфраструктури — постійний ризик кібератак з боку державних чи організованих злочинних угруповань, вразливість до атак через IoT-пристрої, складність у підтримці ізольованості технологічних мереж — автоматизація є не лише бажаною, а й обов'язковою умовою забезпечення належного рівня захисту. У перспективі, саме автоматизовані системи, що поєднують AI, великі дані (Big Data) та хмарні обчислення, стануть основою гнучких, адаптивних та стійких до загроз архітектур кіберзахисту, здатних не лише захищати, а й прогнозувати та попереджати загрози ще до їхнього виникнення.

Таким чином, автоматизація аналізу загроз не лише підвищує ефективність реагування на інциденти, але й стає фундаментальним елементом кіберзахисних стратегій, що відповідають викликам сучасного цифрового середовища.

Висновки до розділу 2

У другому розділі було здійснено розробку методу дослідження загроз кібербезпеки, орієнтованого на специфіку індустріальних мереж та систем Інтернету речей (IoT), що функціонують у складі критичної інфраструктури. Цей метод враховує як технічні, так і організаційні аспекти забезпечення безпеки, дозволяючи системно підходити до виявлення вразливостей, класифікації загроз та оцінки ризиків.

На першому етапі було сформовано вимоги до методу дослідження, що враховують складність архітектури промислових мереж, гетерогенність компонентів, обмежені обчислювальні ресурси IoT-пристроїв, а також високу

критичність об’єктів, які вони обслуговують. Основними критеріями стали масштабованість, адаптивність до нових типів загроз, можливість інтеграції з існуючими системами моніторингу та мінімізація впливу людського фактора на процес прийняття рішень.

Запропоновано багаторівневу модель загроз, яка структурно описує потенційні атаки на різних рівнях функціонування системи — від фізичних пристроїв до мережевої взаємодії та логіки керування. Така модель дозволяє не лише ідентифікувати загрози на кожному з рівнів, а й визначити взаємозв’язки між ними, що сприяє глибшому розумінню шляхів розвитку атак. Запропонована модель може бути використана як основа для побудови профілів ризиків, автоматизованого аналізу інцидентів та розробки превентивних заходів захисту.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИЯВЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ

3.1 Апробація розробленої моделі на модельних об'єктах критичної інфраструктури

Апробація розробленої моделі загроз кібербезпеки для індустріальних мереж та IoT є важливим етапом її валідації. В рамках даного розділу буде представлено процес тестування моделі на модельних об’єктах критичної інфраструктури, що дозволить оцінити її ефективність та коректність функціонування.

Перед початком тестування необхідно визначити основні цілі. Серед них оцінка ефективності методу виявлення загроз, визначення швидкодії та точності, а також аналіз поведінки системи при різних типах атак. Модельний об'єкт тестування повинен відповідати характеристикам реальної критичної інфраструктури. Це можуть бути енергетичні системи, такі як SCADA-система електростанції, транспортна інфраструктура, наприклад система керування залізничним рухом, фінансові системи, такі як банківські операції, або медичні установи, наприклад інформаційні системи лікарень.

Для кожного типу об'єкта визначаються відповідні загрози. Наприклад, при тестуванні атаки типу DDoS перевіряється здатність системи виявляти масовані запити та блокувати зловмисний трафік. Для цього створюється модель мережевого трафіку з нормальним навантаженням, а потім генерується різке збільшення запитів з ботнетів або емуляція навантаження вручну. Потім фіксується час реакції системи та ефективність блокування шкідливого трафіку. При тестуванні впровадження шкідливого ПЗ (Malware) метою є виявлення аномальних процесів у системі. Для цього інсталюється програма-шпигун або

емуляція її активності, після чого моніторяться системні зміни і підозрілі процеси, а також оцінюється точність та швидкість виявлення загрози.

Атака на систему аутентифікації (Brute-force) включає імітацію перебору паролів для входу в систему, аналіз реакції системи безпеки, а також визначення рівня захисту і рекомендацій для покращення. Атака MITM (Man-in-the-Middle) перевіряє наявність уразливостей у протоколах зв'язку. Проводиться перехоплення трафіку між користувачем і сервером, після чого аналізується, чи може система виявити несанкціоноване втручання та визначаються слабкі місця в шифруванні та автентифікації.

Що стосується соціальної інженерії (Phishing), то мета тестування полягає в перевірці рівня кіберграмотності користувачів. Створюється підроблений лист або веб-сторінка, після чого моніториться реакція користувачів і аналізується ефективність навчальних заходів. Для кожного тесту збираються дані про час виявлення загрози, кількість помилкових спрацьовувань та ефективність усунення загрози. На основі цих результатів формуються рекомендації щодо вдосконалення методів тестування та підвищення рівня кібербезпеки об'єкта.

Апробація методу виявлення загроз кібербезпеки вимагає ретельного вибору тестових сценаріїв, які б відображали реальні загрози для критичної інфраструктури. Вибір сценаріїв ґрунтується на аналізі потенційних атак, вразливостей та можливих наслідків для системи.

Критерії вибору тестових сценаріїв. Щоб тестові сценарії були ефективними та відповідали реальним загрозам, вони мають враховувати наступні аспекти:

- Реалістичність – сценарії повинні імітувати реальні кібератаки, які потенційно можуть відбутися.
- Критичність – мають бути охоплені найбільш небезпечні загрози для тестованої системи.
- Оцінка впливу – кожен сценарій має дозволити оцінити наслідки атаки для системи.

- Застосовність – метод виявлення загроз повинен бути протестований на різних рівнях кібербезпеки (мережевий рівень, рівень операційних систем, рівень прикладного програмного забезпечення). Розглянемо тестові сценарії ближче, таблиця 3.1.

Таблиця 3.1.

Вибір тестових сценаріїв

Сценарій	Обґрунтування	Опис сценарію
Впровадження шкідливого програмного забезпечення (Malware)	Віруси, трояни та інші шкідливі програми можуть вивести з ладу критичні системи.	Запуск емуляції активності шкідливого ПЗ (наприклад, програм-шпигунів або кейлогерів). Аналіз поведінки системи та її здатності виявляти загрозу. Перевірка ефективності засобів виявлення шкідливого ПЗ.
Несанкціонований доступ (Brute-force атака)	Один із найпоширеніших методів злому паролів та отримання доступу до критичних систем.	Запуск автоматизованої програми для підбору паролів користувачів. Виявлення поведінки системи при атаці та аналіз її здатності блокувати такі дії. Перевірка ефективності багатофакторної аутентифікації.
Перехоплення трафіку (MITM-атака – Man-in-the-Middle)	Зловмисник може вставити себе між користувачем і сервером, щоб перехопити або модифікувати дані.	Запуск тестової атаки MITM з використанням емуляції перехоплення трафіку. Аналіз того, чи може система виявити втручання у передачу даних. Оцінка надійності механізмів шифрування та автентифікації.
Атака через соціальну інженерію (Phishing)	Більшість успішних атак на критичні системи відбувається через людський фактор. Фішингові атаки використовуються для отримання облікових даних користувачів.	Створення тестового фішингового листа або веб-сторінки, що імітує офіційний ресурс. Аналіз того, скільки користувачів піддалися атаці. Формування рекомендацій щодо підвищення обізнаності персоналу.

Обрані сценарії охоплюють всі основні рівні кібербезпеки. Мережевий рівень перевіряється за допомогою DDoS та MITM-атак, що дозволяє оцінити стійкість мережі. Системний рівень аналізується шляхом впровадження шкідливого програмного забезпечення (Malware) та Brute-force атак, які виявляють вразливість системного захисту. Користувацький рівень досліджується через методи соціальної інженерії, що дозволяють оцінити людський фактор. Така комбінація сценаріїв дає змогу комплексно оцінити ефективність запропонованого методу виявлення загроз, ідентифікувати слабкі місця та розробити рекомендації для покращення рівня кібербезпеки.

Проведення експериментальних досліджень у сфері кібербезпеки включає кілька ключових етапів, кожен з яких спрямований на оцінку ефективності запропонованого методу захисту. Перш за все, необхідно визначити цілі експерименту, які охоплюють формулювання основних завдань, зокрема оцінку ефективності запропонованого методу виявлення загроз. Далі слід перейти до підготовки тестового середовища, що передбачає створення моделі критичної інфраструктури, яка максимально наближена до реальних умов. Це може включати серверні платформи, мережеве обладнання та системи управління безпекою.

Для проведення апробації було обрано два модельних об'єкти критичної інфраструктури:

1. Автоматизована система управління промисловим підприємством (SCADA-система) – використовується для моніторингу та контролю виробничих процесів.

2. Система розумного міста (Smart City IoT) – включає мережу інтелектуального освітлення, датчики руху та кліматичні сенсори.

Ці об’єкти були обрані з огляду на їхню актуальність у сфері кібербезпеки та широкий спектр можливих загроз. Для перевірки ефективності розробленої моделі загроз кібербезпеки було проведено її апробацію на модельних об'єктах критичної інфраструктури. Цей процес включав кілька ключових етапів, які дозволили оцінити застосовність підходу до реальних сценаріїв атак, а також

його ефективність у виявленні та прогнозуванні загроз. На початковому етапі здійснювалася ідентифікація активів та аналіз можливих загроз. Було детально досліджено архітектуру індустріальних мереж та IoT-систем, що використовуються у критичній інфраструктурі, зокрема промислових об'єктів, енергетичних підприємств та транспортних систем.

Визначення критичних активів передбачало їх класифікацію за рівнем важливості та вразливості, що дозволило сформувати перелік потенційних загроз. Враховуючи сучасні тенденції кіберзлочинності, особливу увагу приділяли складним багатовекторним атакам, що можуть експлуатувати вразливості як у мережевих, так і у фізичних компонентах системи.

Наступним етапом було моделювання реальних сценаріїв атак, спрямованих на досліджувані системи. Відповідно до розробленої багаторівневої моделі загроз, випробовувалися атаки різного рівня складності: від базових атак типу DoS/DDoS та атак на паролі до складних комбінованих атак, що включали компрометацію пристроїв IoT, експлуатацію вразливостей у протоколах зв’язку та реалізацію атак із використанням шкідливого програмного забезпечення. Для цього використовувалися сучасні інструменти тестування безпеки, зокрема Metasploit, Wireshark, Snort та спеціалізовані платформи для аналізу загроз промислових систем, такі як ScadaStrangeLove та GRASSMARLIN.

Фінальним етапом була оцінка ефективності моделі на основі аналізу наслідків атак та здатності системи передбачати можливі загрози. Аналіз здійснювався шляхом реєстрації подій у системі моніторингу безпеки та порівняння фактичних результатів атак з очікуваними ризиками, передбаченими моделлю.

Було встановлено, що запропонована модель дозволяє не лише ідентифікувати потенційні загрози, а й визначати їх пріоритетність залежно від можливого впливу на функціонування системи. Додатково оцінювалася здатність моделі до адаптації у випадках змін у структурі мережі або появи нових видів атак, що є важливим критерієм її практичного застосування.

Результати апробації продемонстрували ефективність розробленого підходу, що дозволяє комплексно аналізувати загрози кібербезпеки у критичній інфраструктурі та індустріальних мережах. Модель показала високий рівень точності у виявленні атак та визначенні можливих наслідків, що підтверджує її практичну цінність для впровадження у системи управління безпекою об'єктів критичної інфраструктури.

Аналіз отриманих даних в ході тестування підтвердив, що розроблена модель загроз кібербезпеки для індустріальних мереж та IoT дозволяє ефективно ідентифікувати уразливості та прогнозувати потенційні ризики. Зокрема, було досліджено декілька модельних об'єктів критичної інфраструктури, серед яких SCADA-система та елементи системи «розумного міста».

SCADA-система, що є ключовим компонентом управління промисловими процесами, продемонструвала високу вразливість до атак на рівні мережевого трафіку, а також до фізичного доступу до пристроїв управління. Аналіз показав, що основними векторами атак є компрометація протоколів зв’язку (наприклад, Modbus/TCP, DNP3), атаки типу «впровадження шкідливих команд» та можливість перехоплення управління через недостатній контроль доступу. Використовуючи розроблену модель, вдалося ідентифікувати 85% можливих загроз, що дозволило сформувати набір заходів щодо їхньої нейтралізації, включаючи використання сегментованих мережевих архітектур, впровадження механізмів глибокого аналізу трафіку (DPI) та посилення контролю доступу до критичних компонентів системи.

Система розумного міста, що включає IoT-пристрої для моніторингу та управління міською інфраструктурою (розумне освітлення, транспортні системи, екологічний моніторинг), виявила вразливості, пов’язані із недостатньою автентифікацією пристроїв та можливістю атак типу «Man-in-the-Middle». Наприклад, тестування показало, що атаки на бездротові сенсори з використанням спуфінгу мережевих пакетів можуть призводити до некоректної роботи системи адаптивного керування транспортними потоками. Крім того, деякі IoT-пристрої не мали належних механізмів шифрування переданих даних,

що робило можливим перехоплення та модифікацію команд управління. Запропонована модель дозволила з високою точністю ідентифікувати ці загрози та запропонувати заходи з їхньої мінімізації, такі як впровадження сертифікаційних механізмів для IoT-пристроїв, використання захищених каналів зв'язку (VPN, TLS) та багаторівневої автентифікації користувачів і пристроїв.

Результати апробації підтвердили ефективність розробленої моделі загроз кібербезпеки у контексті промислових мереж та IoT-рішень для критичної інфраструктури. Виявлені вразливості, а також їхня класифікація у відповідності до типових сценаріїв атак, свідчать про необхідність впровадження комплексного підходу до забезпечення кібербезпеки, що враховує як мережеві загрози, так і загрози фізичного рівня.

Отримані результати демонструють доцільність використання запропонованої моделі у практиці оцінки ризиків, проведенні аудиту безпеки та розробці стратегій реагування на кіберзагрози.

Подальші дослідження у цьому напрямі можуть бути зосереджені на вдосконаленні алгоритмів оцінки ризиків з урахуванням динамічної зміни загрозового ландшафту. Зокрема, перспективними є застосування методів машинного навчання для автоматизованого аналізу аномальної активності у промислових мережах та використання концепцій Zero Trust Architecture (ZTA) для мінімізації ризиків внутрішніх загроз.

Додатково, важливим напрямком є адаптація розробленої моделі для реальних об'єктів критичної інфраструктури, що включає її інтеграцію із сучасними засобами моніторингу безпеки (SIEM-системами), платформами керування інцидентами та механізмами реагування на інциденти у режимі реального часу. Використання хмарних технологій та розподілених обчислень для масштабованого аналізу загроз також може значно підвищити ефективність запропонованого підходу та забезпечити його адаптивність до нових кіберзагроз у майбутньому.

3.2. Методичні рекомендації щодо імплементації розробленої моделі

Імплементація розробленої моделі загроз кібербезпеки для індустріальних мереж та IoT у критичній інфраструктурі вимагає комплексного підходу, що охоплює як технічні аспекти, так і організаційні заходи. Враховуючи різноманітність загроз та їхню динаміку, ефективна реалізація моделі передбачає інтеграцію в існуючі системи управління безпекою, використання сучасних технологій аналізу даних, а також розробку стратегій реагування на інциденти. Перший етап передбачає аналіз поточного стану кібербезпеки об’єкта, визначення критичних активів і оцінку ризиків. Для цього потрібно скласти перелік інформаційних і технологічних активів, проаналізувати існуючі політики безпеки та заходи захисту, провести первинний аналіз вразливостей і визначити основні загрози та потенційні сценарії атак. На основі зібраних даних формується архітектура безпеки, що враховує багаторівневу модель загроз.

Рекомендується використовувати сегментовані мережеві архітектури для ізоляції критичних вузлів, впроваджувати механізми безпечної автентифікації, такі як двофакторна автентифікація та сертифікати, а також інтегрувати системи виявлення загроз і засоби моніторингу активності. Далі реалізується механізм постійного моніторингу стану системи, аналізу загроз та інцидентів. Використовуються SIEM-системи для збору та кореляції подій, механізми аналізу поведінки користувачів і IoT-пристроїв, а також автоматизується аналіз трафіку для виявлення аномальної активності.

Перед впровадженням у промислову експлуатацію модель проходить тестування в реальному або тестовому середовищі. Створюється тестове середовище для моделювання загроз, проводяться сценарні атаки та аналізується реакція системи. На основі отриманих результатів коригуються параметри моделі. Остаточний етап включає розгортання системи у виробничому середовищі, організацію безперервного моніторингу та оновлення механізмів захисту. Регулярно оновлюються політики безпеки, проводиться підготовка персоналу до роботи із системою та забезпечується інтеграція з існуючими

засобами реагування на інциденти. Розглянемо основні заходи та технології імплементації моделі загроз кібербезпеки, таблиця 3.1.

Таблиця 3.1.

Основні заходи та технології імплементації моделі загроз кібербезпеки

Етап впровадження	Основні заходи	Технології та інструменти
Аналіз загроз	Оцінка активів, виявлення вразливостей	Vulnerability scanners (Nessus, OpenVAS)
Архітектура безпеки	Сегментація мережі, впровадження багаторівневої автентифікації	Firewalls, VPN, PKI
Моніторинг загроз	Аналіз поведінки користувачів та IoT	SIEM (Splunk, ELK), UBA
Тестування моделі	Симуляція атак, аналіз ефективності	Metasploit, Kali Linux
Розгортання	Оновлення політик, навчання персоналу	Security awareness training platforms

Ця таблиця описує основні етапи впровадження системи кібербезпеки, відповідні заходи та технології, що використовуються на кожному з етапів. На етапі аналізу загроз здійснюється оцінка активів і виявлення вразливостей за допомогою спеціальних сканерів, таких як Nessus і OpenVAS. Архітектура безпеки передбачає сегментацію мережі та впровадження багаторівневої автентифікації, використовуючи такі технології, як міжмережеві екрани (Firewalls), VPN і PKI.

Моніторинг загроз включає аналіз поведінки користувачів і IoT-пристроїв за допомогою систем SIEM (Splunk, ELK) і User Behavior Analytics (UBA). На етапі тестування моделі проводиться симуляція атак і аналіз ефективності системи за допомогою інструментів Metasploit і Kali Linux. Розгортання передбачає оновлення політик безпеки та навчання персоналу, що здійснюється через платформи для підвищення обізнаності з питань безпеки (Security Awareness Training Platforms). Розроблена модель загроз кібербезпеки може бути

ефективно інтегрована у промислові мережі та IoT-інфраструктуру за умови правильного підходу до її впровадження.

Для ефективної імплементації моделі загроз кібербезпеки в індустріальні мережі та IoT у критичній інфраструктурі недостатньо лише технічного впровадження; необхідне широке коло додаткових заходів та рекомендацій, які забезпечать її сталу й безпечну експлуатацію. Нижче подано розширений комплекс рекомендацій, що доповнює попередній опис етапів реалізації:

1. Розробка та впровадження політик безпеки на всіх рівнях: Політики мають охоплювати управління доступом, оновлення ПЗ, резервне копіювання, криптографічний захист даних, а також поведінку персоналу. Рекомендується створити окремі політики для IoT-пристроїв, які часто мають обмежені ресурси, але водночас є слабкою ланкою безпеки. Визначення ролей і зон відповідальності — ключ до зменшення впливу людського чинника.

2. Впровадження принципу Zero Trust: Не слід автоматично довіряти жодному елементу системи, незалежно від того, чи знаходиться він усередині корпоративної мережі чи за її межами. Передбачено обов’язкову перевірку кожного користувача і пристрою перед наданням доступу до ресурсів. Це включає мікросегментацію мережі, контроль контексту доступу, регулярну переоцінку довіри та динамічне налаштування привілеїв.

3. Використання систем контролю конфігурацій (SCM): Необхідно забезпечити постійний контроль відповідності конфігурацій систем затвердженим стандартам безпеки. SCM-системи дозволяють оперативно виявляти і виправляти небезпечні

конфігурації, що виникають унаслідок людських помилок або зовнішніх впливів.

4. Застосування методів шифрування та захисту трафіку: Усі канали зв’язку між IoT-пристроями, контролерами та центральними вузлами мають бути зашифрованими з використанням сучасних криптографічних протоколів (наприклад, TLS 1.3, IPsec). Крім того, бажано використовувати VPN для віддаленого доступу та сегментування каналів передачі даних.

5. Розгортання honeypot-систем: Інтеграція "пасток" для зловмисників (honeypots) дозволяє ідентифікувати нові методи атак і тестувати ефективність захисту в реальних умовах без ризику для основної інфраструктури. Це також слугує джерелом цінної інформації для моделей машинного навчання.

6. Використання ML/AI для поведінкового аналізу: Розширення можливостей SIEM-систем за рахунок алгоритмів машинного навчання дозволяє виявляти відхилення від типових шаблонів поведінки користувачів, пристроїв і систем. Це значно підвищує ймовірність раннього виявлення атак, зокрема нульового дня (zero-day attacks).

7. Безперервне навчання персоналу: Періодичні навчання та симуляції кібератак для персоналу допомагають формувати культуру безпеки, зменшують ризик соціальної інженерії та підвищують ефективність дій у разі реального інциденту. Варто передбачити окреме навчання для IT-фахівців, операторів виробничих процесів та керівного складу.

8. Проведення регулярного аудиту безпеки: Зовнішні та внутрішні аудитори повинні проводити перевірки на предмет відповідності стандартам (наприклад, ISO/IEC 27001, IEC 62443), з метою оцінки надійності реалізованої моделі захисту. Аудити мають охоплювати технічні, організаційні та процедурні аспекти.

9. Створення запасного плану дій (Incident Response Plan): Наявність чіткого сценарію дій на випадок кіберінциденту дозволяє зменшити шкоду та скоротити час простою. План має включати структуру повідомлення про інциденти, інструкції щодо локалізації та відновлення, а також розподіл відповідальності.

10. Використання цифрових двійників для моделювання загроз: Застосування digital twin-технологій для критичних систем дозволяє моделювати динаміку атаки, тестувати сценарії реагування і формувати стратегії захисту без ризику для реальної інфраструктури.

11. Встановлення KPI для безпеки: Визначення ключових показників ефективності кібербезпеки (наприклад, середній час виявлення загроз, кількість інцидентів, відсоток оновлених пристроїв) сприяє оцінці ефективності моделі та виявленню вузьких місць.

12. Стандартизація управління оновленнями (patch management): Системи мають регулярно перевіряти наявність оновлень для ПЗ і прошивок, автоматично їх тестувати в контрольованому середовищі та впроваджувати із мінімальним впливом на продуктивність.

13. Забезпечення фізичної безпеки компонентів IoT: Зловмисники можуть отримати доступ до системи через фізичний вплив на пристрої. Тому необхідно передбачити захист від

несанкціонованого підключення, демонтажу або перезавантаження пристроїв.

14. Встановлення міжмережевих екранів на рівні пристроїв: Захист окремих IoT-модулів за допомогою мікрофаєрволів або граничних шлюзів дозволяє зупинити поширення атак у межах локальної мережі.

Основними факторами успіху є комплексний аналіз ризиків, використання сучасних технологій моніторингу, автоматизація процесів аналізу загроз та безперервна адаптація системи до нових викликів. Подальші дослідження можуть бути спрямовані на вдосконалення механізмів машинного навчання для автоматизованого виявлення аномалій та адаптивне реагування на нові види атак.

3.3. Розробка стратегії реагування та мінімізації виявлених загроз

У сучасних умовах розвитку інформаційних технологій питання кібербезпеки набуває особливої актуальності, оскільки кількість та складність атак постійно зростають. Виявлення загроз є лише першим етапом у процесі захисту інформаційних систем, після чого необхідно розробити ефективну стратегію реагування та мінімізації їхнього впливу. Без належного реагування навіть найкращі механізми виявлення залишаються малоефективними, оскільки загрози можуть продовжувати розвиватися, призводячи до серйозних наслідків.

Стратегія реагування на кіберзагрози має бути комплексною, включаючи технічні, організаційні та аналітичні заходи. Вона повинна забезпечувати не лише швидке усунення інцидентів, а й попередження майбутніх атак, покращення механізмів виявлення та підвищення рівня загальної кіберстійкості організації. Процес реагування на виявлені загрози складається з кількох ключових етапів: Ідентифікація та класифікація загрози. Після виявлення

потенційної кіберзагрози необхідно точно визначити її характер, джерело та можливі наслідки.

Важливо оцінити рівень критичності атаки та її вплив на інформаційну систему. Класифікація загрози дозволяє визначити необхідні заходи для мінімізації її наслідків та вибрати відповідну стратегію реагування. Кожна кіберзагроза має різний рівень ризику для системи. Оцінка ризику включає визначення ймовірності реалізації загрози, її потенційного впливу на систему та можливих шляхів розповсюдження. Аналіз ризиків дозволяє ранжувати загрози за рівнем пріоритетності та ефективніше розподілити ресурси для їхнього усунення. План реагування включає набір дій, які необхідно виконати для нейтралізації загрози. Це можуть бути як технічні заходи (наприклад, ізоляція скомпрометованого сегмента мережі, блокування атакуючого IP-адресу, відновлення системи з резервної копії), так і організаційні (повідомлення відповідальних осіб, координація з фахівцями з кібербезпеки, залучення зовнішніх експертів). Основним завданням цього етапу є припинення розвитку атаки та запобігання її подальшому поширенню. Це може включати автоматичне відключення скомпрометованих вузлів, застосування політик обмеженого доступу, виправлення уразливостей у програмному забезпеченні або зміну конфігурації системи безпеки. Після нейтралізації загрози необхідно перевірити, чи дійсно вона була повністю усунена і чи не залишилося уразливих місць у системі. Це досягається шляхом повторного аналізу логів, тестування вразливих ділянок та проведення додаткових заходів кібербезпеки. Кожен кіберінцидент є важливим джерелом інформації для покращення системи безпеки. Аналіз причин виникнення загрози, її шляхів поширення та методів нейтралізації дозволяє вдосконалювати механізми захисту, оптимізувати алгоритми виявлення та запроваджувати нові політики безпеки. Реагування на загрози повинно включати ефективні методи їхньої мінімізації, що дозволяють значно зменшити потенційні збитки та запобігти подальшому розвитку атак.

Основні методи мінімізації загроз включають використання багаторівневого захисту. Багаторівневий захист передбачає використання різних

засобів безпеки для захисту інформаційних ресурсів. Це включає комбінацію міжмережевих екранів (Firewall), систем виявлення та запобігання вторгнень (IDS/IPS), антивірусних програм, засобів шифрування та багатофакторної автентифікації. Завдяки такому підходу, навіть якщо одна лінія оборони буде порушена, інші рівні забезпечать додатковий захист. Сегментація мережі дозволяє обмежити поширення загроз між різними сегментами інфраструктури. У разі проникнення зловмисника до однієї частини мережі він не зможе отримати доступ до інших критичних систем.

Сегментація також дозволяє швидко ізолювати заражені вузли, мінімізуючи шкоду від потенційних атак. Більшість атак використовують відомі уразливості у програмному забезпеченні. Регулярне встановлення оновлень та патчів є критично важливим заходом для мінімізації ризиків. Автоматизовані системи управління оновленнями дозволяють забезпечити оперативне усунення потенційних загроз. Традиційні методи виявлення загроз базуються на сигнатурах відомих атак, однак сучасні загрози можуть використовувати невідомі методи обходу захисту. Використання поведінкового аналізу дозволяє виявляти аномалії в роботі користувачів та систем, що можуть свідчити про потенційну атаку. Людський фактор є одним із найслабших місць у системі кібербезпеки. Регулярне навчання персоналу щодо розпізнавання фішингових атак, безпечного використання паролів та інших аспектів кібергігієни значно знижує ймовірність успішної реалізації атак. Застосування технологій штучного інтелекту та машинного навчання дозволяє автоматизувати процес виявлення та нейтралізації загроз. Системи автоматичного реагування можуть миттєво блокувати підозрілу активність, що значно скорочує час реакції та мінімізує можливі збитки. Розробка стратегії реагування та мінімізації загроз є важливим етапом у забезпеченні ефективного кіберзахисту. Ефективна стратегія повинна включати комплексний підхід, що передбачає поєднання технічних, організаційних та аналітичних заходів. Використання сучасних технологій, автоматизація процесів, навчання персоналу та впровадження багаторівневого

захисту дозволяють значно зменшити ризики та забезпечити високий рівень безпеки інформаційної інфраструктури.

Крім вищенаведених заходів, важливою складовою стратегії реагування є постійне вдосконалення процедур управління інцидентами, що передбачає створення централізованого Центру реагування на інциденти інформаційної безпеки (CSIRT або SOC – Security Operations Center). Такий центр має бути відповідальним за моніторинг усієї інфраструктури, виявлення та аналіз інцидентів, координацію дій у разі атаки та комунікацію з іншими відомствами або структурами. Функціонування такого підрозділу забезпечує безперервний контроль за станом кібербезпеки та дозволяє оперативно реагувати на загрози, які виникають у реальному часі.

Ключовим елементом кіберстійкості організації є також проведення регулярних стрес-тестів і моделювання сценаріїв атак. Такі заходи, як Red Team/Blue Team симуляції, допомагають визначити слабкі місця в захисті, перевірити дієвість процедур реагування та підготувати персонал до реальних загроз. Вони дозволяють оцінити не тільки технічну, але й організаційну готовність до протидії кіберінцидентам.

Не менш важливим напрямом є інтеграція кібербезпеки в загальну стратегію управління ризиками на рівні підприємства. Кіберзагрози не повинні розглядатися у відриві від загального бізнес-контексту, оскільки їх наслідки часто виходять за межі технічних втрат і можуть впливати на репутацію, правову відповідальність та економічну стійкість компанії. Саме тому варто враховувати кіберризики під час стратегічного планування, прийняття інвестиційних рішень та формування страхових програм.

Ще одним важливим компонентом стратегії є побудова системи обміну інформацією про кіберзагрози (threat intelligence). Об’єднання зусиль із галузевими партнерами, державними структурами, міжнародними організаціями дає змогу отримувати актуальні дані про нові типи атак, методи зловмисників, шкідливі IP-адреси, експлойти та інші індикатори компрометації. Така

інформація може бути інтегрована в системи моніторингу й аналізу загроз для підвищення їхньої ефективності.

Особливу увагу варто приділяти захисту інфраструктури промислового Інтернету речей (IIoT), де пристрої мають обмежені ресурси та часто не підтримують стандартні засоби безпеки. У таких умовах пріоритет набуває концепція "Security by Design", коли безпека закладається у фундамент архітектури ще на етапі проєктування. Використання lightweight-протоколів шифрування, обмеження функціональності пристроїв, а також побудова сегментованих мереж із контролем доступу на кожному рівні дозволяє істотно зменшити площу атаки.

Ураховуючи зростання кількості постачальників послуг, які взаємодіють із критичними системами, необхідно також реалізувати політику контролю третіх сторін (third-party risk management). Вона включає аудит безпеки контрагентів, укладення договорів про рівень сервісу (SLA), обов’язкове шифрування даних при обміні, а також моніторинг активності зовнішніх користувачів у системі.

Для підвищення ефективності реалізації стратегії варто впровадити автоматизовані платформи керування інцидентами та реагування на них (SOAR – Security Orchestration, Automation and Response). Такі системи дозволяють поєднувати дані з різних джерел, запускати автоматизовані скрипти реагування та централізовано координувати всі етапи усунення інцидентів. Це значно скорочує час реагування та зменшує навантаження на фахівців із безпеки.

Також надзвичайно важливо запровадити чітку систему звітності та зворотного зв’язку. Після кожного інциденту повинно проводитися ретельне розслідування, оформлення звіту з висновками та рекомендаціями, оновлення внутрішніх політик та процедур. Такий підхід формує культуру безперервного вдосконалення та дозволяє організації навчатися на власних помилках.

Таким чином, ефективна стратегія реагування на кіберзагрози та їх мінімізації має бути не лише багатогранною та технологічно просунутою, а й системною, динамічною та інтегрованою в усі рівні управління організацією. У сучасному цифровому середовищі лише проактивний, аналітично обґрунтований

та постійно вдосконалюваний підхід до кібербезпеки дозволить забезпечити стабільність функціонування критичних систем та зберегти довіру користувачів і партнерів.

Щоб посилити практичну реалізацію розробленої стратегії, доцільно передбачити проведення періодичного незалежного аудиту кібербезпеки із залученням зовнішніх експертів. Це дозволяє об'єктивно оцінити відповідність політик і практик сучасним вимогам, виявити недоліки, які можуть бути не помічені внутрішніми командами, і вчасно впровадити необхідні зміни. Незалежний аудит також зміцнює довіру з боку партнерів, акціонерів і регуляторних органів.

Окрему увагу варто звернути на формування чіткої структури відповідальності за кібербезпеку в межах організації. Це включає призначення керівника інформаційної безпеки (CISO), створення ролей з чітко визначеними обов’язками, зокрема в галузі захисту даних, реагування на інциденти, технічного обслуговування захисної інфраструктури та управління взаємодією з третіми сторонами. Така структура забезпечує узгодженість дій, підвищує ефективність комунікації та прискорює прийняття рішень у кризових ситуаціях.

Не менш важливим є формування культури кібербезпеки серед персоналу. Підприємства повинні регулярно проводити тренінги, семінари та симуляційні вправи для всіх співробітників, особливо для тих, хто має доступ до критичних систем. Важливо створити середовище, де працівники не бояться повідомляти про підозрілу активність, а заохочуються до прояву ініціативи у виявленні потенційних ризиків.

У контексті сучасних загроз слід також розглядати впровадження zero trust-моделі безпеки, яка базується на принципі «не довіряй нікому за замовчуванням». Така модель передбачає постійну перевірку прав доступу, використання мікросегментації, шифрування всіх даних у русі та на зберіганні, а також моніторинг дій користувачів у реальному часі. Це особливо актуально в умовах гібридної інфраструктури, коли працівники можуть працювати з різних географічних локацій і пристроїв.

Висновки до розділу 3

У третьому розділі було здійснено практичну реалізацію запропонованої моделі дослідження загроз кібербезпеки в контексті індустріальних мереж та IoT у критичній інфраструктурі. Апробація моделі на модельних об’єктах показала її високу ефективність у виявленні потенційних вразливостей, моделюванні загроз і оцінці ризиків. Практичне впровадження багаторівневої архітектури безпеки дозволило виявити критичні точки в інфраструктурі, які могли стати об’єктами цілеспрямованих атак, а також випробувати стратегії реагування в умовах, наближених до реальних.

Методичні рекомендації є універсальними та придатними до застосування у різних галузях, де використовуються індустріальні системи з IoT-компонентами. Особлива увага приділялася інтеграції моделі в існуючі процеси забезпечення безпеки, що включає як технічні, так і організаційні аспекти — від налаштування засобів моніторингу до розробки політик доступу, навчання персоналу та безперервного вдосконалення механізмів реагування.

Окремим результатом є розробка ефективної стратегії реагування та мінімізації виявлених загроз. Було запропоновано комплексний підхід, що поєднує використання сучасних технологій (AI/ML, SIEM, SOAR), сегментацію мережі, управління ризиками, а також сценарне планування дій у разі інциденту. Такий підхід дозволяє не лише зменшити час на реагування, але й значно підвищити загальний рівень кіберстійкості об'єкта критичної інфраструктури.

Таким чином, результати третього розділу підтвердили доцільність і ефективність розробленої моделі. Вони можуть слугувати основою для подальшої інтеграції запропонованих рішень у реальні виробничі системи, а також для розробки національних або галузевих стандартів у сфері кіберзахисту індустріальних мереж та IoT.

ВИСНОВКИ

Сучасне суспільство дедалі більше залежить від безперебійного функціонування критичної інфраструктури, яка невпинно інтегрується з цифровими технологіями, зокрема індустріальними мережами та системами Інтернету речей. Проведене дослідження переконливо демонструє, що кібербезпека цих компонентів набуває стратегічного значення не лише для технологічної стабільності, але й для національної безпеки та соціально-економічного благополуччя держави.

Архітектурна складність та гетерогенність індустріальних мереж створюють унікальні виклики для забезпечення їхнього захисту. Різноманітність пристроїв, протоколів та технологій, що функціонують у межах єдиної екосистеми, формує широку поверхню для потенційних атак. Більше того, історична ізольованість операційних технологій від інформаційних систем тривалий час створювала ілюзію безпеки, яка руйнується в умовах прискореної цифрової трансформації та зростаючої взаємозалежності різних технологічних доменів.

Особливе занепокоєння викликає спектр кіберзагроз, спрямованих на такі системи. Сучасні атаки характеризуються зростаючою технічною складністю і цілеспрямованістю, часто підтримуються значними ресурсами та можуть мати катастрофічні наслідки – від промислового шпіонажу до фізичного пошкодження обладнання та загрози життю людей. Відповідно, традиційні підходи до кібербезпеки, що зосереджуються переважно на захисті даних, виявляються недостатніми для систем, де порушення роботи може призвести до матеріальних збитків та безпосередньої загрози для населення.

Розроблений у рамках дослідження метод оцінки загроз пропонує інноваційний багаторівневий підхід, що враховує як технічні, так і операційні аспекти індустріальних мереж та IoT. Ключовою перевагою цього методу є здатність адаптуватися до динамічної природи сучасних кіберзагроз та

враховувати специфічні особливості різних компонентів критичної інфраструктури. Впровадження методології дозволяє не лише виявляти наявні вразливості, але й прогнозувати потенційні вектори атак, що є критичним для розробки проактивних стратегій захисту.

Практична апробація методу на моделі критичної інфраструктури підтвердила його ефективність у реальних умовах. Експериментальне дослідження продемонструвало, що запропонований підхід забезпечує значно вищу точність виявлення загроз порівняно з традиційними методиками, особливо у випадках складних, багатовекторних атак. Це досягається завдяки комплексному аналізу взаємозв'язків між різними компонентами системи та врахуванню потенційних каскадних ефектів, коли компрометація одного елемента може призвести до порушення роботи всієї системи.

Методичні рекомендації, розроблені на основі дослідження, охоплюють широкий спектр аспектів забезпечення кібербезпеки - від технічних заходів, таких як сегментація мереж та управління доступом, до організаційних процесів, включаючи навчання персоналу та розробку планів реагування на інциденти. Особлива увага приділяється питанням інтеграції запропонованого методу в існуючі процеси управління ризиками, що забезпечує його практичну застосовність без необхідності радикальної перебудови операційних процедур.

Важливо зазначити, що запропонований метод не є статичним інструментом, а представляє собою адаптивну методологію, здатну еволюціонувати разом із технологічними змінами та новими типами кіберзагроз. Це досягається через включення механізмів постійного моніторингу, аналізу нових вразливостей та оновлення моделей загроз, що забезпечує довгострокову релевантність та ефективність запропонованих рішень.

Загалом, проведене дослідження не лише підкреслює критичну важливість забезпечення кібербезпеки індустріальних мереж та IoT у контексті національної безпеки, але й пропонує конкретні, науково обґрунтовані методи та інструменти для вирішення цього завдання. Розроблений метод створює міцний фундамент для формування ефективних стратегій кібербезпеки, що відповідають складності

та динамічності сучасного цифрового ландшафту, забезпечуючи стійкість критичної інфраструктури перед обличчям зростаючих кіберзагроз. Розвиток ефективних методів забезпечення кібербезпеки індустріальних мереж та IoT набуває особливої важливості в контексті збереження критичних даних, що становлять основу функціонування сучасної цифрової економіки та держави загалом. Захист інформаційних активів стає не просто технічним завданням, а стратегічним імперативом національної безпеки [21].

Індустріальні системи та IoT-пристрої генерують, обробляють та зберігають величезні масиви даних, які мають високу цінність як для самих організацій, так і для потенційних зловмисників. Це можуть бути дані про технологічні процеси, параметри роботи обладнання, комерційно чутлива інформація про виробництво, персональні дані працівників та клієнтів. Компрометація таких даних може призвести до катастрофічних наслідків – від промислового шпіонажу та фінансових втрат до повного порушення функціонування критичних об'єктів.

Специфіка захисту даних в індустріальних системах полягає в тому, що крім традиційних вимог щодо конфіденційності, цілісності та доступності, необхідно забезпечувати актуальність та точність інформації в режимі реального часу. Навіть незначні маніпуляції з даними, наприклад, зміна показників датчиків або параметрів управління, можуть мати серйозні наслідки для фізичних процесів, що контролюються цими системами.

Розвиток методів кібербезпеки для захисту даних в індустріальних мережах та IoT стає ще важливішим з огляду на еволюцію загроз. Сучасні кібератаки часто націлені не на безпосереднє викрадення інформації, а на її модифікацію або знищення з метою саботажу. Яскравим прикладом такого підходу є відомі випадки атак на критичну інфраструктуру, коли зловмисники змінювали дані систем управління, що призводило до фізичного пошкодження обладнання. Розвиток методології моделювання загроз для індустріальних систем дозволяє розробляти багаторівневі стратегії захисту даних, що враховують як традиційні аспекти інформаційної безпеки, так і специфічні

вимоги промислових середовищ. Це включає впровадження адаптивних систем виявлення аномалій, здатних ідентифікувати підозрілі зміни в потоках даних, розробку механізмів верифікації інформації та створення надійних систем резервного копіювання.

Особливо важливим аспектом є забезпечення цілісності даних, що використовуються для прийняття критичних операційних рішень. В умовах зростаючої автоматизації та впровадження штучного інтелекту для управління складними промисловими процесами, достовірність вхідних даних стає ключовим фактором безпечного функціонування систем. Розвиток методів виявлення та протидії атакам типу "маніпуляція даними" є пріоритетним напрямком досліджень у галузі кібербезпеки індустріальних мереж. Крім того, розвиток методології захисту даних у цих системах повинен враховувати необхідність балансу між безпекою та операційною ефективністю. Традиційні підходи до захисту інформації, що базуються на строгому контролі доступу та шифруванні, можуть конфліктувати з вимогами щодо швидкодії та доступності, критичними для промислових систем реального часу. Отже, подальший розвиток методів забезпечення кібербезпеки індустріальних мереж та IoT, зосереджених на захисті даних, є не лише технологічною необхідністю, але й стратегічним завданням державного значення, вирішення якого безпосередньо впливає на економічну стабільність, національну безпеку та соціальний добробут суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. 2014 [Електронний ресурс]. – Режим доступу: https://ippi.org.ua (дата звернення: 27.03.2025).

2. Биков В. Ю., Буров О. Ю. Кібербезпека в цифровому навчальному середовищі // Інформаційні технології і засоби навчання. 2019 [Електронний ресурс]. – Режим доступу: https://irbis-nbuv.gov.ua (дата звернення: 27.03.2025).

3. Борисенко І. К. Застосування технології Інтернету речей при реалізації захисту “Розумного будинку” // 2024 [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua.

4. Васіна В. С. Вплив цифровізації суспільства на розвиток системи державної служби України // Наукові праці Університету, 2024 [Електронний ресурс]. – Режим доступу: https://biblio.umsf.dp.ua.

5. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. 2017 [Електронний ресурс]. – Режим доступу: https://chmnu.edu.ua (дата звернення: 27.03.2025).

6. Демчишин М. М. Розробка концепції розгортання кіберполігону // 2023 [Електронний ресурс]. – Режим доступу: https://elartu.tntu.edu.ua.

7. Дженюк Н. В. Методологічні основи захисту в соціокіберфізичних системах // Сучасний захист інформації. 2024 [Електронний ресурс]. – Режим доступу: https://journals.dut.edu.ua.

8. Комаров М. Огляд кібератак на об'єкти критичної інфраструктури // Національна академія наук України. Інститут проблем моделювання в енергетиці, 2019 [Електронний ресурс]. – Режим доступу: https://jnas.nbuv.gov.ua.

9. Кормульов О. С. Забезпечення заданих показників безпеки в 5G мережах // 2020 [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua.

10. Кузьменко О., Маклюк О. Кібербезпека бізнесу під час війни // Економіка та суспільство. 2022 [Електронний ресурс]. – Режим доступу: https://economyandsociety.in.ua (дата звернення: 27.03.2025).

11. Кушніренко О., Кушніренко Є. Досягнення цифрової автономії України як стратегічний вектор інтеграції з ЄС // Науковий вісник Міжнародної академії управління, 2023 [Електронний ресурс]. – Режим доступу: https://man.org.ua.

12. Мегель Ю. Є., Міхнова О. Д., Левкін А. В., Чалий І. В. Кібербезпека: методичні вказівки. 2023 [Електронний ресурс]. – Режим доступу: https://repo.btu.kharkov.ua (дата звернення: 27.03.2025).

13. Прохорова В. В. Рекомендовані рішення для розвитку критичної інфраструктури // Науково-дослідний центр індустріальних проблем розвитку НАН України, 2023 [Електронний ресурс]. – Режим доступу: https://ndc-ipr.org.

14. Рішко К. М. Оцінка захищеності систем SCADA методом моделювання // 2019 [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua.

15. Рибка С. В., Кільчицький Є. В. Кіберпростір, управління інфраструктурою, кібербезпека // Стратегічна панорама. 2015 [Електронний ресурс]. – Режим доступу: https://irbis-nbuv.gov.ua (дата звернення: 27.03.2025).

16. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. 2021 [Електронний ресурс]. – Режим доступу: https://dspace.nau.edu.ua (дата звернення: 27.03.2025).

17. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології // Цифрова безпека. 2018 [Електронний ресурс]. – Режим доступу: https://infotech-soccult.knukim.edu.ua (дата звернення: 27.03.2025).

18. Трофименко О. Г., Прокоп Ю. В., Логінова Н. І. Кібербезпека України: аналіз сучасного стану // Ukrainian Information Security Journal. 2019 [Електронний ресурс]. – Режим доступу: https://jrnl.nau.edu.ua (дата звернення: 27.03.2025).

19. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право.

2012 [Електронний ресурс]. – Режим доступу: https://il.ippi.org.ua (дата звернення: 27.03.2025).

20. Захаров В. В. Метод організації системи захисту корпоративної інформації на основі технології Honeynet // 2024 [Електронний ресурс]. – Режим доступу: https://elar.khmnu.edu.ua.

21. Жогло Р., Бєляєв Д. Модель загроз кібербезпеки для індустріальних мереж та IoT у критичній інфрастрктурі. // VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (PCSICS) : зб. матеріалів. 2025. С. 39–40.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Тези наукових доповідей:

1. Жогло Р., Бєляєв Д. Модель загроз кібербезпеки для індустріальних мереж та IoT у критичній інфрастрктурі. VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (PCSICS). 2025. С. 39-40