МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ КІБЕРЗАГРОЗ В ПРОМИСЛОВИХ СИСТЕМАХ ТА РОЗРОБЛЕННЯ СПОСОБІВ ЗАХИСТУ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ігор ПОНОМАРЬОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ігор ПОНОМАРЬОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
Д.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:

Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пономарьову Ігорю Володимировичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аналіз кіберзагроз в промислових системах та розроблення способів захисту”, керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н.,доцент.
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби забезпечення інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати теоретичні основи кіберзагроз в промислових системах.
   4.2. Дослідити сучасні методи захисту від кіберзагроз в промислових системах.
   4.3. Розробити рекомендації щодо розроблення та впровадження ефективних методів захисту промислових систем.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ кіберзагроз в промислових системах.	08.04.2024	
4.	Дослідження сучасних методів захисту від кіберзагроз в промислових системах.	22.04.2024	
5.	Розробка рекомендацій щодо розроблення та впровадження ефективних методів захисту промислових систем.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Ігор ПОНОМАРЬОВ

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувач Пономарьов І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Аналіз кіберзагроз в промислових системах та розроблення способів захисту"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ПОНОМАРЬОВ Ігор у кваліфікаційній роботі проаналізував особливості управління інформаційною безпекою підприємства, дослідив основні засоби та методи захисту інформації на підприємств, вивчив засоби підвищення ефективності захисту інформації на підприємстві, розробив практичні рекомендації за темою дослідження.

ПОНОМАРЬОВ Ігор показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ПОНОМАРЬОВА Ігоря на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Пономарьов І.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ПОНОМАРЬОВА Ігоря
на тему “Аналіз кіберзагроз в промислових системах та розроблення способів захисту”

Актуальність.

Швидкий розвиток промислових систем, збільшення кількості підключених пристроїв та обсягів оброблюваних даних створюють серйозні виклики для забезпечення кібербезпеки в промисловому секторі. Однією з ключових причин актуальності цієї теми є постійне зростання кількості та складності кіберзагроз. Зловмисники прагнуть використовувати вразливості в системах безпеки для несанкціонованого доступу до критичних інфраструктур, крадіжки даних або впливу на нормальне функціонування виробничих процесів. Організація захисту від кіберзагроз стає стратегічно важливою для забезпечення стабільності та надійності промислових систем. Клієнти, партнери та регулятори вимагають від компаній доказів того, що їхні системи належним чином захищені від можливих загроз. Важливо, щоб промислові підприємства постійно контролювали та оцінювали свої методи захисту, щоб забезпечити їхню актуальність та ефективність у протидії новітнім загрозам. Значення вимірювання показників управління ризиками та оцінки ефективності заходів безпеки постійно зростає. Комплексний аналіз і оцінка ефективності захисту від кіберзагроз є критичними аспектами для постійного вдосконалення систем управління ризиками та адаптації до змін у загрозах. Регулярне тестування і аудит захисних процесів допомагають виявити слабкі місця та впровадити необхідні покращення для підвищення рівня кібербезпеки в промислових системах.

Позитивні сторони.

Кваліфікаційна робота охоплює важливу та актуальну тему, пов'язану з аналізом кіберзагроз в промислових системах та розробленням способів захисту, що відображає значущість цієї проблеми у сучасному цифровому світі. Кваліфікаційна робота вражає глибиною аналізу застосовуваних методик та підходів до аналізу кіберзагроз. Чітко структуровані вступ та висновки роблять роботу добре організованою та логічно зв'язаною. Акцент на рекомендаціях щодо розроблення та впровадження ефективних методів захисту промислових систем є важливим аспектом роботи, що відображає сучасні тенденції у галузі інформаційної безпеки.

Недоліки.

Хоча робота добре структурована, варто розглянути можливість більш детального аналізу окремих методик захисту та їхнього порівняння, щоб надати читачеві глибше розуміння вибору конкретних підходів. Це дозволить визначити найбільш ефективні та відповідні методи реагування на кіберзагрози для різних типів промислових систем. Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування обраних методик управління ризиками на конкретних прикладах чи в реальних умовах промислової діяльності. Такий підхід дозволить оцінити практичну ефективність методів та адаптувати їх до специфічних потреб і умов різних промислових підприємств, забезпечуючи максимальну ефективність реагування на кіберзагрози.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач ПОНОМАРЬОВ Ігор заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

к.т.н., доцент _____ *підпис* _____ Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена оцінці ефективності засобів та методів захисту інформації на підприємстві. Робота складається зі вступу, трьох розділів, що містять 7 рисунків, висновків і списку використаних джерел із 43 найменувань. Загальний обсяг роботи становить 66 аркушів, з яких 6 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є організація реагування на кіберзагрози в промислових системах.

Об'єктом дослідження є кіберзагрози в промислових системах.

Предмет дослідження – особливості захисту та реагування на кіберзагрози в промислових системах.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до організації реагування на кіберзагрози в промислових системах.

Як результат у роботі проаналізовано теоретичні основи кіберзагроз в промислових системах, досліджено сучасні методи захисту від кіберзагроз в промислових системах, розроблено рекомендації щодо розроблення та впровадження ефективних методів захисту промислових систем.

Галузь застосування. Розроблені підходи можуть бути використані при організації реагування на кіберзагрози в промислових системах.

Ключові слова: ПРОМИСЛОВІ СИСТЕМИ, КІБЕРЗАГРОЗИ, ФУНКЦІОНУВАННЯ ПРОМИСЛОВИХ СИСТЕМ, КІБЕРАТАКИ, МЕТОДИ ТА СТРАТЕГІЇ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ, ВПРОВАДЖЕННЯ ЕФЕКТИВНИХ МЕТОДІВ, НОВІТНІ ТЕХНОЛОГІЇ.

ABSTRACT

The qualification work is devoted to the assessment of the effectiveness of information security tools and methods at an enterprise. The work consists of an introduction, three chapters containing 7 figures, conclusions and the list of references containing 43 items. The total volume of the work is 66 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to organize the response to cyber threats in industrial systems.

The object the study is cyber threats in industrial systems.

The subject of the study is the peculiarities of protection and response to cyber threats in industrial systems.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to organizing response to cyber threats in industrial systems were used.

As a result, the work analyzed the main theoretical foundations of cyber threats in industrial systems, investagated modern methods of protection against cyber threats in industrial systems; developed recommendations for the development and implementation of effective methods of protecting industrial systems.

Field of application. The developed approaches can be used in the organization of response to cyber threats in industrial systems.

Keywords: INDUSTRIAL SYSTEMS, CYBER THREATS, FUNCTIONING OF INDUSTRIAL SYSTEMS, CYBER ATTACKS, METHODS AND STRATEGIES OF PROTECTION AGAINST CYBER THREATS, IMPLEMENTATION OF EFFECTIVE METHODS, THE LATEST TECHNOLOGIES.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де кіберзагрози стають все більшим викликом для промислових підприємств, забезпечення ефективної організації захисту та реагування на ці загрози є важливим, як ніколи. Аналіз та оцінка ефективності засобів і методів реагування дозволяють визначити вразливості в системах безпеки та прийняти необхідні заходи для запобігання негативним наслідкам.

З огляду на зазначене, дослідження оцінки ефективності організації захисту та реагування на кіберзагрози в промислових системах є актуальним науковим завданням.

Мета роботи полягає у організації реагування на кіберзагрози в промислових системах.

Об'єкт дослідження – кіберзагрози в промислових системах.

Предмет дослідження – особливості захисту та реагування на кіберзагрози в промислових системах.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати теоретичні основи кіберзагроз в промислових системах.
2. Дослідити сучасні методи захисту від кіберзагроз в промислових системах.
3. Розробити рекомендації щодо розроблення та впровадження ефективних методів захисту промислових систем.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до організації реагування на кіберзагрози в промислових системах.

Як результат у роботі проаналізовано теоретичні основи кіберзагроз в промислових системах, досліджено сучасні методи захисту від кіберзагроз в промислових системах, розроблено рекомендації щодо розроблення та

впровадження ефективних методів захисту промислових систем.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити правильну оцінку забезпечення безпеки інформації на підприємстві. Результати дослідження можуть допомогти оптимізувати систему реагування на кіберзагрози, спираючись на оцінку наявних методів та рекомендації щодо їх покращення. Це дозволить підприємствам швидше і ефективніше виявляти, реагувати на та усувати інциденти, мінімізуючи потенційні збитки та підвищуючи загальний рівень інформаційної безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАГРОЗ В ПРОМИСЛОВИХ СИСТЕМАХ

У сучасному інформаційному суспільстві, де віртуальна реальність переплітається з фізичною, питання кібербезпеки стає найбільш актуальним та нагальним. В контексті промислових систем, які є основою економіки та життєво важливими для нормального функціонування суспільства, кіберзагрози набувають особливого значення та стають об'єктом глибокого дослідження. Неабияку увагу привертають теоретичні аспекти цього явища, що дозволяють краще зрозуміти природу, причини та наслідки кіберзагроз у промислових системах.

Аналіз теоретичних основ кіберзагроз в промислових системах спрямований на виявлення ключових аспектів цього явища та визначення шляхів його подолання. Однією з основних складових теорії кібербезпеки є розуміння потенційних загроз та уразливостей, які притаманні промисловим системам. Це означає вивчення методів та засобів, які використовуються зловмисниками для проникнення в інформаційні системи, а також визначення можливих точок вразливості в промислових процесах.

Розуміння механізмів формування кіберзагроз у промислових системах передбачає аналіз взаємодії людей, технологій та процесів. Сучасні промислові системи все більше стають об'єктом автоматизації та віртуалізації, що відкриває нові можливості для кіберзлочинців, а також підвищує ризики виникнення серйозних кібератак. Тому вивчення теоретичних аспектів кіберзагроз у промислових системах є критично важливим для розробки ефективних стратегій захисту та протидії цим загрозам.

1.1. Поняття та класифікація кіберзагроз в промислових системах

Поняття кіберзагрози в промислових системах відображає складну ситуацію, коли цифрові технології, що контролюють та управляють

промисловими процесами, стають об'єктом потенційних атак з боку зловмисників. Кіберзагрози можуть виникати з різних джерел і мати різні наслідки для промислових систем, від порушення нормального функціонування до серйозних матеріальних та екологічних збитків. Для розуміння та класифікації кіберзагроз в промислових системах можна використовувати різні підходи та критерії, включаючи джерело загроз, спосіб атаки, наслідки для системи та інші.

Рис. 1 Основні категорії кіберзагроз в промислових системах

1. **Шкідливе програмне забезпечення (Malware):**

це тип загрози, який включає в себе різноманітні види шкідливого програмного забезпечення, такі як віруси, черви, троянські коні, шпигунське програмне забезпечення тощо. Шкідливе програмне забезпечення може використовуватися для порушення промислових систем, викрадення конфіденційної інформації, а також для завдання матеріальних збитків [1].

Шкідливе програмне забезпечення (Malware) є одним з найбільш поширених та небезпечних видів кіберзагроз в промислових системах. Цей тип загрози включає в себе різноманітні шкідливі програми, створені з метою завдання шкоди, крадіжки інформації або викрадення контролю над системою.

Існують такі види шкідливого програмного забезпечення:

- *віруси* є програмними кодами, які вбудовуються в інші файли або програми та розповсюджуються шляхом виконання забраженого коду. Вони можуть поширювати інфекцію, завдавати шкоди файлам та системі в цілому, а також виконувати різноманітні завдання, включаючи крадіжку інформації або виклик атак з відмовою в обслуговуванні.
- *черви* є самореплікуючими програмами, які поширюються через мережу без необхідності вбудовування в інші файли. Вони можуть використовувати вразливості мережевого протоколу для автоматичного розповсюдження та завдання шкоди промисловим системам;
- *троянські коні* виглядають як корисне програмне забезпечення, але фактично містять шкідливий код, який може виконувати різноманітні атаки, такі як крадіжка паролів, руйнування файлів або створення «задніх дверей» для отримання несанкціонованого доступу до системи;
- *шпигунське програмне забезпечення* призначене для збору конфіденційної інформації про користувача без його відома. Це може включати історію перегляду веб-сторінок, особисті дані, паролі та іншу приватну інформацію;
- *програми-вимагачі (Ransomware)*, які блокують доступ до системи або зашифровують файли з метою вимагання викупу для їх розблокування. Ці програми можуть завдати серйозних фінансових збитків та перерв у роботі промислових систем.

Шкідливе програмне забезпечення може використовуватися для різних цілей, включаючи крадіжку конфіденційної інформації, виклик відмови в обслуговуванні, руйнування файлів та завдання інших видів шкоди. Для захисту від шкідливого програмного забезпечення необхідно використовувати ефективні антивірусні програми, вести регулярне оновлення програмного забезпечення та

виконувати проактивні заходи з кібербезпеки, щоб уникнути вразливостей та атак [2].

2. **Атаки на мережеві протоколи і протоколи безпеки:**

зловмисники можуть використовувати різноманітні методи для атак на мережеві протоколи та протоколи безпеки, такі як відмова в обслуговуванні (DDoS) атаки, перехоплення трафіку, використання вразливостей в протоколах безпеки.

Атаки на мережеві протоколи і протоколи безпеки є серйозною загрозою для сучасних інформаційних систем, зокрема промислових систем. Ці атаки спрямовані на експлуатацію вразливостей у протоколах мережевого зв'язку та протоколах безпеки, що використовуються для передачі даних і забезпечення конфіденційності, цілісності та доступності інформації[3].

Атаки на мережеві протоколи можуть включати в себе такі методи, як перехоплення пакетів даних, зміна чи відхилення потоків даних, а також переповнення буфера. Ці атаки можуть бути спрямовані на здобуття конфіденційної інформації, модифікацію переданих даних або навіть відмову в обслуговуванні, що може призвести до припинення роботи мережі або зниження її продуктивності.

Протоколи безпеки, такі як SSL/TLS, IPsec, SSH тощо, призначені для захисту конфіденційності, цілісності та аутентифікації даних, переданих через мережу. Атаки на протоколи безпеки можуть включати в себе злам аутентифікації, використання вразливостей в реалізації протоколів, а також атаки типу «людина-посередник» (man-in-the-middle), коли зловмисник перехоплює та модифікує передані дані.

Для захисту від атак на мережеві протоколи і протоколи безпеки важливо використовувати комплексний підхід, що включає в себе застосування криптографічних методів шифрування та аутентифікації, регулярне оновлення програмного забезпечення та відстеження вразливостей, а також моніторинг

мережевого трафіку для виявлення аномальних активностей. Також важливо забезпечити належне навчання та свідомість користувачів щодо потенційних загроз та захисних заходів.

3. **Соціальна інженерія:**

цей вид атаки використовує маніпулювання людьми з метою отримання несанкціонованого доступу до інформації або систем. Зловмисники можуть використовувати фішингові атаки, імітацію або здійснювати атаки через соціальні мережі для введення персоналу в оману та отримання доступу до промислових систем.

Соціальна інженерія є методом атаки, який базується на маніпуляції людьми з метою отримання несанкціонованого доступу до конфіденційної інформації або системних ресурсів. Цей підхід використовує психологічні та соціальні техніки для впливу на поведінку цільових осіб з метою виконання атакуючими зловмисниками задуманих дій або розкриття конфіденційної інформації.

Соціальна інженерія може приймати різноманітні форми, включаючи фішингові атаки, імітацію, інженерію дозволів, імперсонацію авторитетних осіб або атаки через соціальні мережі [4]. Ці атаки можуть бути спрямовані на виведення цільових осіб з радіусу дії або організації з метою отримання доступу до системи або конфіденційної інформації, використовуючи їх довіру, лояльність або необачність.

Однією з ключових складових соціальної інженерії є аналіз цільової аудиторії та використання психологічних та соціальних властивостей для досягнення поставленої мети. Це може включати в себе вивчення психології цільових осіб, встановлення довіри, створення вигідних сценаріїв, використання важливих подій або емоційних впливів.

Одним з основних методів захисту від соціальної інженерії є свідоме навчання персоналу та підвищення їх обізнаності про потенційні загрози. Крім того, важливо встановити строгі процедури перевірки та авторизації доступу до

системи, обмежити доступ до конфіденційної інформації та використовувати механізми автоматизованого виявлення аномальної активності. Також можуть бути використані технологічні засоби, такі як двофакторна аутентифікація, для підвищення рівня безпеки від соціально-інженерних атак.

4. **Використання вразливостей в програмному забезпеченні:**

цей тип загрози виникає внаслідок використання вразливостей або дефектів в програмному забезпеченні промислових систем для отримання несанкціонованого доступу або завдання шкоди.

Використання вразливостей в програмному забезпеченні є одним із ключових методів атак на інформаційні системи, що базується на експлуатації недоліків, помилок чи дефектів у програмному коді для отримання несанкціонованого доступу, виконання шкідливих дій або завдання шкоди. Цей вид атаки може включати в себе використання вразливостей в операційних системах, додатках, веб-додатках, базах даних та інших компонентах програмного забезпечення.

Уразливості в програмному забезпеченні можуть бути спричинені різноманітними факторами, такими як недостатня перевірка введених даних, недостатність або неправильна обробка виняткових ситуацій, недосконаліть алгоритмів або вразливості у використовуваних бібліотеках та компонентах. Атаки, що використовують ці вразливості, можуть призвести до розкриття конфіденційної інформації, втрати контролю над системою, внесення змін у функціонал або завдання матеріальних збитків [5].

Для захисту від атак, що використовують вразливості в програмному забезпеченні, необхідно приділяти увагу безпеці програмного забезпечення на кожному етапі життєвого циклу розробки програмного продукту. Це включає в себе проведення аудиту та аналізу вразливостей, використання практик безпеки програмування, таких як забезпечення правильного контролю вводу та виводу даних, відсутність використання застарілих алгоритмів або функцій, а також вдосконалення механізмів перевірки безпеки під час розробки та тестування програмного забезпечення.

Паралельно з цим, важливо проводити регулярне оновлення програмного забезпечення та використовувати механізми автоматичного виявлення та виправлення вразливостей. Також необхідно вдосконалювати механізми моніторингу та виявлення аномальних активностей, щоб вчасно виявляти та реагувати на потенційні загрози безпеки.

5. **Фізичні атаки:**

зловмисники можуть використовувати фізичний доступ до промислових систем для здійснення атак, таких як крадіжка обладнання, підключення пристроїв з метою вивчення або маніпулювання системою.

Фізичні атаки на інформаційні системи є одним із методів атак, які базуються на фізичному доступі до апаратного забезпечення, пристроїв чи інфраструктури системи з метою отримання несанкціонованого доступу до конфіденційної інформації, завдання шкоди або викрадення ресурсів. Ці атаки можуть бути спрямовані на об'єкти фізичної інфраструктури, такі як серверні кімнати, комутатори мережі, комп'ютери, а також на периферійні пристрої, такі як USB-пристрої, монітори, принтери тощо [6].

Одними з типових прикладів фізичних атак є крадіжки обладнання, підключення пристроїв для перехоплення даних або введення в систему шкідливого обладнання, фізичне пошкодження або руйнування обладнання, а також атаки на людський фактор, такі як використання соціальних інженерних методів для отримання доступу.

Для захисту від фізичних атак важливо приділяти увагу безпеці фізичного середовища, забезпечуючи контроль доступу до об'єктів, моніторинг зовнішньої периметральної зони, встановлення систем відеоспостереження та інших технічних засобів безпеки. Крім того, важливо використовувати шифрування даних, забезпечити фізичну безпеку пристроїв та периферійних пристроїв, а також регулярно проводити перевірки безпеки та аудит безпеки фізичної інфраструктури для виявлення потенційних загроз та вразливостей.

Розрізнення цих категорій допомагає розуміти різноманітність кіберзагроз, їх потенційні наслідки та різні методи захисту промислових систем від них.

Розглянувши поняття та класифікацію кіберзагроз в промислових системах, можна зробити декілька важливих висновків. По-перше, різноманітність кіберзагроз свідчить про складність і масштабність проблеми кібербезпеки у сучасних промислових системах. Кожен вид загрози має свої особливості та потенційні наслідки, що вимагає ретельного аналізу та розробки відповідних стратегій захисту. По-друге, важливо враховувати постійну еволюцію технік та методів атак з боку зловмисників. Технологічний прогрес надає їм нові можливості, тоді як недоліки та вразливості в системах постійно використовуються для здійснення атак. Це підкреслює необхідність постійного удосконалення заходів з кібербезпеки та відповідного моніторингу промислових систем.

Розуміння класифікації кіберзагроз дозволяє розробити ефективні стратегії захисту, які враховують специфіку кожного виду загрози. Це включає в себе не лише впровадження технічних заходів захисту, але й навчання персоналу, вдосконалення процедур управління ризиками та забезпечення відповідності найвищим стандартам кібербезпеки.

Отже, для забезпечення безпеки та стійкості промислових систем необхідно поєднувати технологічні, організаційні та освітні заходи, щоб забезпечити комплексний підхід до проблеми кібербезпеки. Тільки такий підхід дозволить ефективно захищати промислові системи від сучасних кіберзагроз.

1.2 Особливості та принципи функціонування промислових систем

Промислові системи, порівняно з іншими інформаційними системами, мають свої унікальні особливості та принципи функціонування, які визначають їх ефективність, надійність та безпеку. Завдяки постійному розвитку технологій та цифровізації, промислові системи стають все більш складними та інтегрованими, втягуючи в себе сенсори, датчики, мережеве обладнання та програмне забезпечення.

Проте, разом зі зростанням функціональності та зв'язності промислових систем, зростає і рівень їх вразливості до різноманітних загроз, включаючи кібератаки, фізичні втручання та інші небезпечні події. Тому розуміння особливостей та принципів функціонування промислових систем має важливе значення для їх надійності, безпеки та стійкості [7].

На рис. 2 зображено одні з найважливіших аспектів промислових систем.

Рис.2 Найважливіші аспекти промислових систем:

Промислові системи часто працюють у вимогливих умовах, де надійність є критичною. Вони повинні бути здатні працювати безперебійно протягом тривалих періодів часу, навіть у навколишніх умовах, які можуть бути екстремальними, таких як великі температурні коливання, вологість, вібрації тощо.

Надійність та стійкість є ключовими характеристиками промислових систем, визначаючи їхню здатність функціонувати безперебійно та ефективно у вимогливих умовах. Надійність відображає ступінь, до якої система може забезпечити необхідну функціональність відповідно до заданих умов та протягом певного періоду часу без виникнення відмов. Стійкість, у свою чергу, визначається здатністю системи протистояти атакам, непередбаченим ситуаціям

та внутрішнім або зовнішнім збоям, зберігаючи при цьому свою продуктивність та функціональність.

Надійність та стійкість промислових систем побудовані на комплексному підході до проектування, реалізації та управління системою. Це включає в себе використання надійних компонентів та матеріалів, врахування факторів середовища та умов експлуатації, розробку систем резервування та відновлення, а також впровадження механізмів моніторингу та діагностики для виявлення та усунення відмов [8].

Стійкість промислових систем забезпечується за допомогою різноманітних заходів з кібербезпеки, таких як захист від вірусів та шкідливого програмного забезпечення, застосування механізмів автентифікації та авторизації, шифрування даних, сегментація мережі та інші методи захисту. Крім того, системи мають бути відповідно налаштовані та підтримувати високий рівень своєї стійкості в умовах змінного середовища та негативних впливів.

Такий підхід дозволяє забезпечити високу надійність та стійкість промислових систем, що є критичним для забезпечення безперебійної та ефективної роботи виробничих процесів та інфраструктури.

Багато промислових систем базуються на розподіленій архітектурі, де кілька компонентів працюють разом як єдине ціле. Це дозволяє розділити функціональність системи на незалежні модулі, що полегшує розвиток, масштабування та обслуговування.

Розподілена архітектура є концепцією проектування програмного забезпечення, в якій система складається з взаємопов'язаних компонентів, які функціонують незалежно один від одного, але спільно працюють для виконання певних завдань або функціональності. Ця архітектурна парадигма дозволяє розділити систему на логічні модулі, які можуть бути розгорнуті на різних фізичних пристроях або в різних мережевих середовищах.

У розподіленій архітектурі кожен компонент системи може функціонувати автономно та взаємодіяти з іншими компонентами через мережу. Це дозволяє

розділити завдання та обробку даних між різними вузлами системи, що покращує масштабованість, надійність та продуктивність системи.

Система розбивається на окремі компоненти, кожен з яких відповідає за виконання певних функцій або послуг. Це дозволяє краще керувати складністю системи та полегшує розробку та супровід програмного забезпечення.

Компоненти системи можуть знаходитися на різних вузлах мережі та спілкуватися між собою за допомогою мережевого зв'язку. Це дозволяє розподілити навантаження та забезпечити більшу гнучкість та масштабованість системи.

Розподілена архітектура дозволяє ефективно використовувати ресурси, такі як обчислювальна потужність, пам'ять та сховища даних, шляхом їх спільного використання та координації між компонентами системи [9].

Завдяки розділенню функціональності та взаємодії через мережу, розподілена архітектура може бути більш стійкою до відмов та помилок, оскільки вона дозволяє локалізувати проблеми та забезпечити продовження роботи інших компонентів системи.

У цілому, розподілена архітектура є важливим інструментом для створення складних та масштабованих програмних систем, які забезпечують високу надійність, продуктивність та стійкість.

Деякі промислові системи вимагають обробки даних у реальному часі для забезпечення швидкої реакції на події або зміни у середовищі. Це особливо важливо в сферах, де затримки можуть призвести до серйозних наслідків, таких як автоматизоване виробництво або керування транспортними системами.

Реальний час (Real-Time) - це характеристика обчислювальних систем, що вказує на те, що результат обробки даних або виконання операцій має бути отриманий або здійснений протягом обмеженого часового інтервалу. Системи реального часу вимагають, щоб обробка даних була здійснена не тільки коректно, а й вчасно, щоб задовольнити поточні вимоги системи чи середовища.

Реальний час може бути класифікований на "жорсткий" (hard real-time) та "м'який" (soft real-time) в залежності від ступеня критичності часу виконання. У

жорстких системах реального часу будь-яка порушення у виконанні обчислень може призвести до серйозних негативних наслідків, тоді як у м'яких системах певна відставка в часі прийнятна, але забезпечується якомога найменшими [10].

Системи реального часу зазвичай використовуються у таких областях як автоматизація промислових процесів, медичне обладнання, автомобільні системи безпеки та керування, аерокосмічні системи та інші сфери, де необхідна надзвичайно точна та швидка реакція на події.

Основні виклики при розробці систем реального часу включають високу точність синхронізації, зменшення затримок у виконанні завдань, забезпечення достатньої потужності обчислювальних ресурсів та ефективне керування пріоритетами виконання завдань.

У загальному, системи реального часу є важливим елементом для забезпечення безпеки, ефективності та надійності у вимогливих та часочутливих додатках та середовищах.

Промислові системи зазвичай мають великі обсяги даних, які збираються з сенсорів, датчиків та інших джерел. Ці дані потрібно ефективно обробляти, аналізувати та зберігати для вивчення та прийняття рішень.

Великі обсяги даних (Big Data) представляють собою ситуацію, коли масштаби обсягу інформації перевищують звичайні методи обробки та аналізу даних, вимагаючи спеціальних підходів та інструментів для ефективного використання. Ця концепція виникла від необхідності вирішення проблем обробки та аналізу великих обсягів даних, які не можуть бути ефективно опрацьовані за допомогою традиційних методів.

Великі обсяги даних виникають у результаті накопичення великої кількості інформації з різних джерел, таких як датчики, додатки веб-послуг, соціальні медіа, медичні записи та інші. Ці дані можуть бути структурованими, наприклад, в базах даних, або неструктурованими, такими як тексти, зображення, аудіо- та відеофайли.

Основні виклики, пов'язані з великими обсягами даних, включають зберігання, обробку, аналіз та візуалізацію цих даних. Для ефективної роботи з

великими обсягами даних використовуються розподілені та паралельні обчислювальні системи, спеціалізовані бази даних та інструменти аналізу даних, такі як машинне навчання та інтелектуальний аналіз даних.

Застосування аналізу великих обсягів даних може приносити значні переваги у багатьох галузях, включаючи бізнес та маркетинг (аналіз клієнтських виборів, прогнозування попиту), медицину (діагностика захворювань, розробка нових ліків), науку (моделювання клімату, астрофізика) та інші. Однак, використання великих обсягів даних також може ставити питання щодо приватності, етики та безпеки, які вимагають уважного розгляду та вирішення.

З урахуванням підвищення кіберзагроз, безпека стає важливим аспектом промислових систем. Вони повинні мати вбудовані механізми захисту, такі як автентифікація, авторизація, шифрування даних та моніторинг безпеки, щоб захистити від несанкціонованого доступу та атак [11].

Безпека, особливо в контексті інформаційних технологій, є критично важливою складовою для забезпечення захисту від шкідливих загроз та збереження цілісності, конфіденційності та доступності даних та ресурсів. У світі, де обмін інформацією відбувається в мережі, а даними керують автоматизовані системи, безпека стає критичним аспектом для запобігання кіберзлочинності, несанкціонованого доступу та збереження приватності.

Безпека включає в себе широкий спектр заходів та методів, включаючи криптографічне захист, контроль доступу, мережеве обладнання, ідентифікацію та аутентифікацію користувачів, а також моніторинг та виявлення аномалій. Ці заходи призначені для запобігання, виявлення та вирішення загроз безпеці, включаючи злами, вразливості програмного забезпечення, фішинг, викиди, атаки з використанням вимоги викупу та інші види кіберзлочинності.

Основні принципи безпеки включають принцип обмеження доступу (принцип найменшого привілею), принцип захисту з перевіркою, принцип безпеки за замовчуванням та принцип безпеки в глибину. Для ефективного застосування цих принципів використовуються різні техніки та інструменти, такі

як використання вірусних програм, брандмауерів, інтрузійних виявлених систем (IDS), систем управління інформаційною безпекою (ISMS) та інші.

Оскільки загрози безпеці постійно змінюються та еволюціонують, безпека вимагає постійного вдосконалення та оновлення стратегій та заходів. Для цього необхідно активно вивчати нові технології та методи атак, проводити аудити безпеки та підтримувати свої системи на найвищому рівні захисту.

Принципи функціонування промислових систем базуються на поєднанні цих особливостей з використанням передових технологій та методів, що дозволяють забезпечити оптимальну продуктивність, надійність та безпеку. Для цього важливо ретельно проектувати, розробляти та управляти промисловими системами, враховуючи їх унікальні потреби та вимоги [12].

Розгляд особливостей та принципів функціонування промислових систем виявляє їхню складність, різноманітність та важливість для сучасного виробництва та інфраструктури. Надійність, розподілена архітектура, обробка даних у реальному часі, великі обсяги інформації та безпека є ключовими аспектами, що впливають на ефективність та стійкість промислових систем.

Розуміння цих особливостей дозволяє розробникам, інженерам та адміністраторам забезпечувати високий рівень надійності, безпеки та ефективності промислових систем. Вдосконалення технологій, розробка нових методів управління та забезпечення безпеки є важливими завданнями для подальшого розвитку промислових систем у виробничому середовищі.

1.3 Потенційні наслідки кібератак для промислових систем та виробничих процесів

З огляду на постійний розвиток технологій та зростання залежності виробничих підприємств від інформаційних систем, безпека промислових систем стає все більш актуальною та критичною проблемою. Кібератаки на промислові системи та виробничі процеси можуть мати серйозні наслідки як для ефективності виробництва, так і для безпеки працівників та довкілля. У цьому

контексті важливо ретельно дослідити потенційні наслідки кібератак для промислових систем та виробничих процесів з метою розуміння їхнього впливу та розроблення ефективних стратегій захисту та відновлення [13].

Потенційні наслідки кібератак для промислових систем та виробничих процесів є серйозними та можуть мати значний вплив на виробничі підприємства та інфраструктуру в цілому.

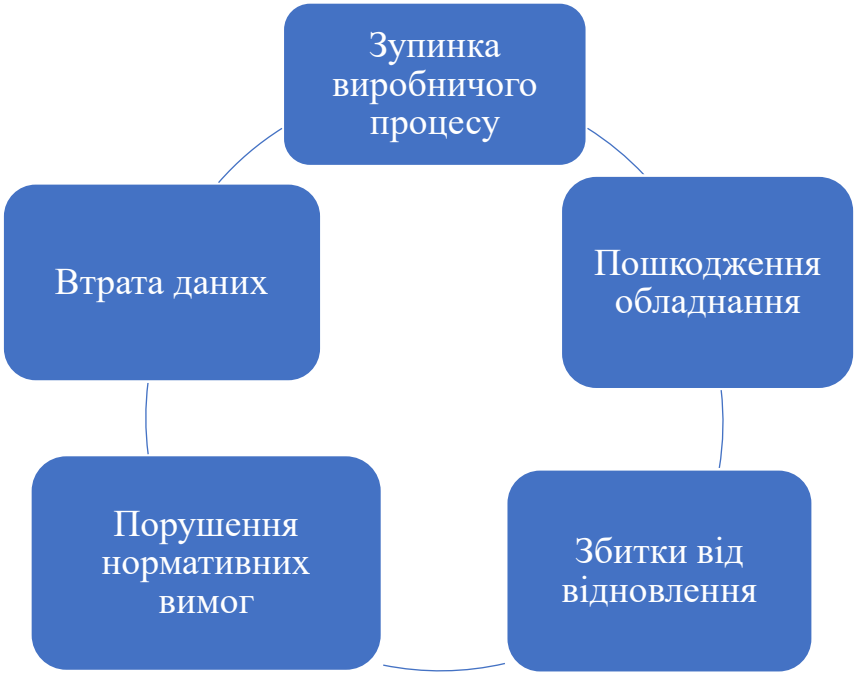

Рис. 3 Можливі наслідки таких кібератак для промислових систем та виробничих процесів

Кібератаки можуть призвести до зупинки або перерви в роботі обладнання та систем контролю, що використовуються у виробничих процесах. Це може призвести до значних фінансових втрат через втрату продуктивності, а також до втрати репутації підприємства через невиконання зобов'язань перед клієнтами та партнерами.

Зупинка виробничого процесу, яка виникає в результаті кібератаки на промислові системи, є серйозною проблемою, яка може мати значний вплив на функціонування підприємства. Цей аспект може бути визначений як втрата продуктивності, що виникає внаслідок призупинення або втрати здатності виробничих систем до нормального функціонування через технічні або програмні втручання. Зупинка виробничого процесу може мати величезні

економічні наслідки через втрату прибутку, невиконання контрактних зобов'язань, збільшення часу виробництва та зниження якості продукції [14].

Ця проблема може виникати з різних причин, включаючи атаки на програмне забезпечення контролю, переривання зв'язку з обладнанням, неправильну роботу систем управління, втручання у мережевий трафік та інші. Вона може впливати на всі аспекти виробничого процесу, включаючи постачання сировини, виробничі лінії, якість продукції та доставку готової продукції.

Зупинка виробничого процесу також може мати важливі наслідки для безпеки працівників та довкілля. Наприклад, вона може призвести до аварій на виробництві, викидів шкідливих речовин у навколишнє середовище або небезпечних умов праці. Тому зупинка виробничого процесу не лише загрожує економічному становищу підприємства, але й може мати серйозний вплив на безпеку та здоров'я людей та навколишнього середовища.

Кібератаки можуть призвести до втрати чутливих даних про виробничі процеси, дизайн продуктів, важливі документи та іншу конфіденційну інформацію. Це може стати причиною фінансових втрат, порушення законодавства про захист персональних даних та інші юридичні проблеми.

Втрата даних - це процес, що характеризується втратою доступу або фізичного видалення цифрової інформації з системи або сховища даних. Цей явище може виникнути внаслідок кібератак, технічних невдач, випадкового видалення або інших факторів. Втрата даних може бути тимчасовою або постійною і може включати в себе втрату важливих документів, файлів, програмного забезпечення, баз даних та іншої цифрової інформації.

Це явище може мати серйозні наслідки для діяльності організацій та індивідів. Зокрема, втрата даних може призвести до порушення робочого процесу, втрати конфіденційної інформації, втрати клієнтів, фінансових втрат та шкоди репутації. Крім того, втрата даних може спричинити порушення вимог законодавства щодо захисту особистих даних та інших правил інформаційної безпеки.

Запобігання втраті даних є критично важливим завданням для організацій та індивідів. Для цього можуть використовуватися різноманітні заходи, такі як регулярні резервні копії даних, використання захисних програм та апаратних засобів, захист мережі та систем, розробка стратегій відновлення даних та навчання персоналу щодо правил безпеки інформації. Такі заходи дозволяють зменшити ризики втрати даних та забезпечити надійний захист цифрової інформації [15].

Деякі види кібератак можуть призвести до пошкодження фізичного обладнання, такого як індустріальні контролери, сенсори, механізми управління та інше. Це може потребувати ремонту або заміни обладнання, що виходить з ладу, та призвести до великих витрат на відновлення працездатності виробничих ліній.

Пошкодження обладнання є серйозною проблемою, яка може виникнути внаслідок кібератак, технічних відмов, недбалості в експлуатації або зовнішніх чинників. Це може включати в себе фізичне пошкодження обладнання, наприклад, його знищення, корозія, перегрів або коротке замикання, а також програмне пошкодження, таке як віруси, шкідливе програмне забезпечення або атаки з використанням вразливостей у програмному забезпеченні.

Пошкодження обладнання може мати серйозні наслідки для функціонування системи та виробничого процесу. Наприклад, воно може призвести до зупинки виробництва, втрати даних, порушення графіку виробництва та втрати продуктивності. Крім того, пошкодження обладнання може призвести до фінансових витрат на ремонт або заміну обладнання, а також до збитків від втрати продукції або невиконання контрактних зобов'язань.

Запобігання пошкодженню обладнання включає в себе ряд заходів та стратегій, таких як регулярне технічне обслуговування та перевірка обладнання, використання захисних програм та апаратних засобів, моніторинг стану обладнання, встановлення заходів безпеки та навчання персоналу щодо безпеки та ефективного використання обладнання. Такі заходи дозволяють зменшити

ризики пошкодження обладнання та забезпечити надійну роботу виробничих систем і пристроїв.

Кібератаки, особливо якщо вони призводять до витоку конфіденційної інформації або порушення стандартів безпеки, можуть мати серйозні наслідки з точки зору регулятивного нагляду. Це може призвести до штрафів, судових позовів та інших санкцій від регулюючих органів [16].

Порушення нормативних вимог у контексті кібербезпеки промислових систем відображає невиконання або недодержання стандартів, правил, законодавства або внутрішніх політик щодо захисту інформації та безпеки даних у промислових середовищах. Це може стосуватися різних аспектів безпеки, таких як захист персональних даних, захист від кібератак, забезпечення надійності та цілісності даних, а також дотримання інших вимог щодо безпеки інформації.

Порушення нормативних вимог може мати серйозні наслідки як для організацій, так і для їх клієнтів та партнерів. Наприклад, воно може призвести до втрати довіри клієнтів, штрафів від регулятивних органів, судових позовів, порушення угод або контрактів та інших юридичних проблем. Крім того, порушення нормативних вимог може також мати негативний вплив на репутацію організації та її можливості залучати нових клієнтів та партнерів.

Для запобігання порушенням нормативних вимог необхідно ретельно дотримуватися вимог законодавства, стандартів та політик безпеки, розробляти та впроваджувати ефективні стратегії та процедури безпеки, забезпечувати навчання персоналу щодо правил та вимог безпеки інформації та проводити аудити безпеки для виявлення та усунення потенційних порушень. Такі заходи допоможуть зберегти надійність, цілісність та конфіденційність даних, а також виконати вимоги щодо безпеки інформації, що ставиться перед підприємствами в сучасному цифровому середовищі.

Відновлення систем після кібератаки може вимагати значних зусиль та витрат. Це включає в себе проведення розслідувань, відновлення даних,

підвищення рівня безпеки та виконання інших заходів для запобігання подібним подіям у майбутньому.

Збитки від відновлення відображають витрати та втрати, пов'язані з процесом відновлення інформаційних систем, програмного забезпечення та інфраструктури після кібератаки або інших подібних подій, що спричинили втрати функціональності або цілісності. Ці збитки можуть включати витрати на відновлення даних, відновлення програмного забезпечення, ремонт або заміну обладнання, а також витрати на проведення розслідувань та вжиття заходів щодо підвищення рівня безпеки.

Витрати на відновлення можуть виявитися значними і можуть включати в себе не лише прямі витрати на придбання та встановлення нового обладнання та програмного забезпечення, але й індиректні витрати на втрату продуктивності, затримки в виробництві, втрату прибутку та негативний вплив на репутацію бізнесу. Крім того, збитки від відновлення можуть включати витрати на оплату консультантів з безпеки, адвокатів, а також витрати на компенсації клієнтам або партнерам у зв'язку з втратою даних або недоступністю послуг.

Для зменшення збитків від відновлення необхідно мати належно розроблені плани відновлення після кібератаки, регулярно виконувати резервне копіювання даних, мати належні заходи безпеки та моніторингу, а також проводити тренування та симуляції для перевірки готовності в разі виникнення інциденту. Тільки за допомогою таких заходів можна ефективно управляти ризиками та зменшити збитки від відновлення після кібератаки.

Кібератаки на промислові системи та виробничі процеси можуть мати серйозні наслідки як для фінансової стійкості підприємства, так і для його репутації та можливостей продовження діяльності. Важливо вживати всі можливі заходи для запобігання таким кібератакам та ефективного реагування в разі їх виникнення.

Дослідження потенційних наслідків кібератак для промислових систем та виробничих процесів підкреслює важливість впровадження ефективних заходів забезпечення безпеки. Зупинка виробничого процесу, втрата даних,

пошкодження обладнання та порушення нормативних вимог можуть призвести до серйозних наслідків для підприємства. Однак, при належній увазі до безпеки та відповідними заходами захисту можна мінімізувати ризики та зберегти стабільність виробничих процесів. Постійне вдосконалення систем безпеки, навчання персоналу та реагування на нові загрози є ключовими аспектами у забезпеченні безпеки промислових систем та виробничих процесів у сучасному цифровому середовищі.

Висновки до розділу 1

Підсумовуючи висвітлені теоретичні аспекти кіберзагроз в промислових системах, можна зробити висновок про їхню загрозливість та потенційний вплив на виробничі процеси та інфраструктуру в цілому. Розглянуті аспекти, такі як шкідливе програмне забезпечення, атаки на мережеві протоколи, соціальна інженерія, використання вразливостей в програмному забезпеченні, фізичні атаки, а також особливості та принципи функціонування промислових систем, підкреслюють складність та різноманітність кіберзагроз у цьому контексті.

Наслідки кібератак для промислових систем, такі як зупинка виробничого процесу, втрата даних, пошкодження обладнання, порушення нормативних вимог та збитки від відновлення, вимагають системного та комплексного підходу до забезпечення кібербезпеки. Необхідно постійно вдосконалювати технічні, організаційні та правові засоби захисту, вдосконалювати системи моніторингу та реагування, а також підвищувати свідомість персоналу щодо потенційних загроз та заходів безпеки.

У світлі постійної еволюції кіберзагроз та їхнього впливу на промислові системи, постійна увага до цього питання та активна реалізація заходів захисту є важливими для забезпечення стійкості та надійності виробничих процесів у сучасному цифровому середовищі.

Розділ 2 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ В ПРОМИСЛОВИХ СИСТЕМАХ

Зростаюча залежність промислових систем від критично важливої інфраструктури та виробничих процесів підвищує важливість надійних заходів кібербезпеки. Сучасні промислові системи часто стають мішенню складних кіберзагроз, які можуть порушити роботу, скомпрометувати конфіденційні дані та завдати значних економічних збитків. Розвиток технологій призвів до розробки інноваційних методів захисту цих систем. Ці методи охоплюють цілу низку стратегій, від сегментації мережі та систем виявлення вторгнень до передових алгоритмів аналізу загроз і машинного навчання. Ці методи захисту, які постійно розвиваються для протидії новим загрозам, мають важливе значення для підтримки цілісності та стійкості промислових систем перед обличчям постійно мінливого ландшафту кіберзагроз.

2.1 Огляд існуючих технологій та рішень для захисту промислових систем.

Для захисту цих систем від кіберзагроз були розроблені різні технології та рішення. Ці рішення включають вдосконалені брандмауери, системи виявлення та запобігання вторгненням, системи управління інформацією та подіями безпеки (SIEM), а також спеціалізовані інструменти промислової кібербезпеки. Промислові послуги формують основу сучасного життя, підтримуючи такі важливі сектори, як електроенергетика, водопостачання, виробництво та ядерна енергетика. Ці послуги значною мірою покладаються на промислові системи управління (ПСУ), які інтегрують різні процеси і прилади, що мають вирішальне значення для промислового виробництва. Захист цих систем має першорядне значення, оскільки збої можуть призвести до катастрофічних наслідків.

TripWire [17] починала як учасник спільноти з відкритим вихідним кодом і з тих пір перетворилася на постачальника передових рішень безпеки, якими

користуються понад 9000 організацій, в тому числі понад 50 відсотків компаній зі списку Fortune 500. Її рішення розроблені для підприємств, що використовують промислові системи управління ("ICS"), пропонуючи безперебійний, надійний захист без необхідності встановлення програмного забезпечення. Цей підхід підвищує ефективність і результативність системи, одночасно спрощуючи управління для операційних команд ICS шляхом надання точних оцінок ризиків відповідним відділам. Ці звіти дають змогу службам безпеки та IT-командам проактивно відстежувати та зменшувати потенційні загрози.

Однією з ключових особливостей TripWire є автоматизовані процеси безпеки, які можна легко налаштувати в режимі реального часу або запланувати відповідно до потреб організації. Така автоматизація підвищує операційну ефективність і забезпечує безперервний захист від кіберзагроз. TripWire також звертає увагу на зростаюче занепокоєння, пов'язане з Інтернетом речей (IoT) в промислових умовах. Згідно з повідомленням у їхньому блозі, 70 відсотків IT-експертів вважають, що їхні організації не готові до загроз, пов'язаних з IoT. Рішення TripWire забезпечують необхідні заходи безпеки для вирішення цих проблем, гарантуючи, що бізнес клієнтів працює безперебійно і безпечно.

Прагнення компанії забезпечити безпроблемний комплексний захист робить її безцінним партнером для підприємств, які покладаються на ICS. Її технології не лише захищають критично важливу інфраструктуру, але й підвищують операційну ефективність завдяки вдосконаленій автоматизації та точній оцінці ризиків. Цей подвійний фокус на безпеці та ефективності позиціонує TripWire як провідного постачальника рішень з кібербезпеки для промислового середовища, допомагаючи організаціям орієнтуватися в складному ландшафті сучасних кіберзагроз.

Запатентовані рішення односпрямованих шлюзів безпеки Waterfall Security [18] вже більше десяти років забезпечують захист промислових підприємств по всьому світу - на комунальних підприємствах, атомних електростанціях, морських платформах, нафтопереробних заводах і виробничих підприємствах.

Ці рішення інтегрують фізичні та цифрові компоненти, щоб забезпечити максимальну безпеку та контроль над потоком даних. На відміну від звичайних брандмауерів, односпрямовані шлюзи Waterfall передають інформацію з робочої мережі, не дозволяючи жодним даним повертатися назад, тим самим усуваючи ризики від зовнішніх кібератак, вірусів або людських помилок.

Програмне забезпечення Waterfall збирає дані в режимі реального часу із захищених мережевих серверів і передає їх у зовнішні мережі, заповнюючи сервери-репліки, щоб забезпечити безперебійну роботу бізнесу та операційних процесів. Цей метод не лише підвищує безпеку, але й забезпечує значну економію коштів у порівнянні з традиційними брандмауерами, зменшуючи витрати, пов'язані з конфігурацією програмного забезпечення, аудитом, навчанням та моніторингом у реальному часі. Технологія Waterfall отримала рекомендації від світових урядів та регуляторних органів, що полегшує дотримання галузевих стандартів.

Таким чином, рішення компанії є надійною та економічно ефективною альтернативою традиційним брандмауерам, забезпечуючи цілісність та безпеку критично важливих промислових мереж, підтримуючи безперебійну роботу.

Symantec [19], провідний постачальник рішень з кібербезпеки, зосереджується на захисті середовищ Інтернету речей у таких галузях, як виробництво, нафтопереробна промисловість та критичні об'єкти інфраструктури. Їхній підхід полягає у впровадженні безпеки безпосередньо в системи для досягнення "кіберстійкості". У своєму звіті "Розумна безпека для виробництва в епоху Індустрії 4.0" компанія Symantec підкреслила, що на виробничий сектор припадає 20% всіх фішингових атак у 2015 році, що на 13% більше, ніж у попередньому році. Уніфікована стратегія безпеки від Symantec пропонує наскрізний огляд бізнес-процесів для виявлення, блокування та усунення наслідків атак. Це комплексне рішення захищає традиційні та новітні кінцеві точки, сервери та мережеві шлюзи, створюючи надійний захист від зовнішніх загроз. Крім того, Symantec інтегрує захист даних та ідентифікаційних даних для захисту особистої та конфіденційної інформації, ще більше знижуючи

ризики для бізнесу та їхніх клієнтів. Рішення Symantec призначені для захисту від атак, які можуть вивести з ладу цілі галузі та завдати значної шкоди, забезпечуючи безперервну та безпечну роботу промислових середовищ.

CyberArk [20] визнає підвищені ризики для промислових систем управління (ПСУ) через поширення адміністративних або привілейованих облікових записів, які надають доступ до критично важливих систем. Їхнє рішення для захисту привілейованих облікових записів покликане зменшити ці ризики, забезпечуючи комплексний моніторинг і контроль над усіма обліковими записами, гарантуючи, що кожен користувач авторизований і облікований. Це рішення інтегровано в єдину платформу, що дозволяє здійснювати безперебійний нагляд і безпечне зберігання жорстко закодованих облікових даних промислових додатків. CyberArk підкреслює важливість безперервного моніторингу для підтримки безпеки організації, значно зменшуючи вікно можливостей для зловмисників і мінімізуючи потенційні збитки завдяки оповіщенням відповідного персоналу в режимі реального часу.

Здатність платформи керувати та контролювати привілейовані облікові записи має вирішальне значення для запобігання несанкціонованому доступу та забезпечення цілісності критично важливих систем. Усуваючи спільні облікові записи, що становлять ризики для безпеки, і дозволяючи детально відстежувати дії користувачів, рішення CyberArk допомагає захиститися від зовнішніх і внутрішніх загроз. Можливості моніторингу та оповіщення в режимі реального часу гарантують, що будь-яка підозріла активність буде негайно виявлена та усунена, тим самим підвищуючи загальний рівень безпеки організації.

Відомі клієнти CyberArk, серед яких BT, PricewaterhouseCoopers, Motorola, Deloitte і Qualcomm, демонструють ефективність і надійність рішень CyberArk для захисту об'єктів критичної інфраструктури. Інтегруючи передові заходи безпеки в єдину платформу, CyberArk забезпечує надійний захист від безлічі загроз, з якими стикається сучасне промислове середовище. Такий проактивний підхід до захисту привілейованих облікових записів має важливе значення для

підтримки безпеки і функціональності активів ICS в умовах все більш складного і загрозливого кібер-ландшафту.

Порівняємо дані рішення за різними характеристика в Табл. 2.1.

Таблиця 2.1.

Порівняльний аналіз розглянутих рішень

	TripWire	**Waterfall Security**	**Symantec**	**CyberArk**
Фокус	Безпека ІКС, оцінка ризиків, захист від загроз IoT	Односпрямовані шлюзи безпеки, замінюють брандмауери	Безпека Інтернету речей, кіберстійкість, захист від фішингу	Безпека привілейованих рахунків, адміністративний контроль
Ключові особливості	Не потребує встановлення програмного забезпечення, автоматизовані процеси безпеки	Поєднує фізичні та цифрові компоненти, передає інформацію в один бік	Наскрізна безпека, захист даних та ідентичності	Повний моніторинг і контроль рахунків, безпечне зберігання облікових даних
Розгортання	Понад 9 000 організацій, включаючи компанії зі списку Fortune 500	Комунальні служби, атомні електростанції, морські платформи, нафтопереробні заводи, виробничі підприємства	Заводи, нафтопереробні заводи, інфраструктури	Відомі клієнти, серед яких BT, PwC, Motorola, Deloitte, Qualcomm, Deloitte, Deloitte, Qualcomm
Інтеграція технологій	Комплексна оцінка ризиків, налаштування в режимі реального часу та за розкладом	Замінює міжмережеві екрани, запобігає зовнішнім кібератакам	Єдина стратегія безпеки, захист традиційних і нових кінцевих точок	Інтегрована платформа для зручного перегляду
Економічна ефективність	Підвищує ефективність системи, зменшує потребу в експертизі з кібербезпеки	Значна економія коштів у порівнянні зі звичайними брандмауерами	Зменшує ризики та перебої в роботі	Зменшує ризики від спільних облікових записів, мінімізує збитки завдяки сповіщенням в режимі реального часу
Моніторинг в режимі реального часу	Так, допомагає службам безпеки та IT-командам відстежувати та	Так, збирає та передає дані в режимі реального часу з операційних серверів	Так, допомагає виявляти та усувати атаки	Так, важливо для мінімізації мережевих ризиків

	запобігати загрозам			
Additional Benefits	Допомагає компаніям почуватися захищеними від загроз, пов'язаних з Інтернетом речей	Рекомендовано урядами та регуляторними органами в усьому світі	Захищає від масштабних атак, забезпечує безперервність роботи	Безперервний моніторинг зменшує вікно для атак

Порівняння рішень з кібербезпеки для промислових систем показує, що TripWire, Waterfall Security, Symantec та CyberArk мають різні фокуси та особливості. TripWire робить акцент на безпеці ІКС з автоматизованими процесами та захистом від загроз Інтернету речей. Waterfall Security пропонує односпрямовані шлюзи безпеки, які замінюють брандмауери для запобігання зовнішнім кібератакам. Symantec націлений на середовища IoT, забезпечуючи наскрізну безпеку та захист від фішингових атак. CyberArk спеціалізується на захисті привілейованих облікових записів, моніторингу та контролі адміністративного доступу для мінімізації мережевих ризиків. Кожне рішення поєднує в собі передові технології та моніторинг в режимі реального часу для підвищення безпеки та операційної ефективності, задовольняючи різні аспекти промислової кібербезпеки.

2.2 Оцінка ефективності різних методів та стратегій захисту.

Забезпечення ефективних засобів кібербезпеки має вирішальне значення для управління IT-діяльністю, захисту даних, систем та мережі від несанкціонованого доступу, зломів та атак. Важливо впроваджувати комплексні заходи безпеки та регулярно їх оновлювати, щоб протистояти загрозам, які постійно змінюються. Постійний моніторинг і своєчасне реагування на інциденти безпеки відіграють життєво важливу роль у збереженні цілісності та конфіденційності критично важливої інформації.

Ключові показники ефективності ("KPI") - це кількісні орієнтири, які дозволяють оцінити ефективність послуг з кібербезпеки [21]. Ці показники узгоджуються з конкретними цілями організації та галузевими стандартами і слугують критично важливими метриками для оцінки ефективності безпеки.

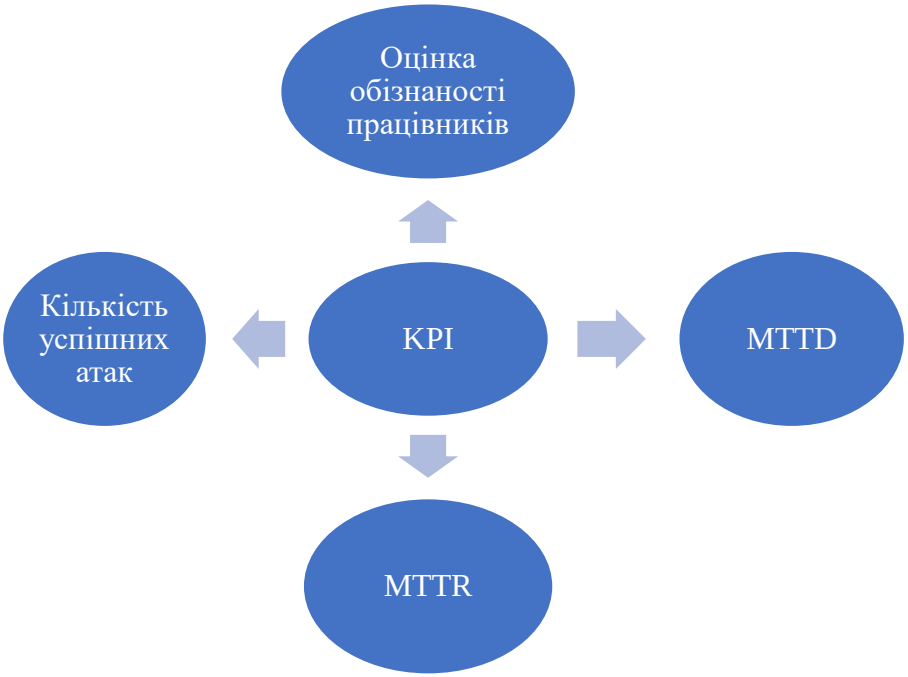

Рис. 2.1. KPI

Середній час виявлення (MTTD) вимірює середній час, необхідний для виявлення інциденту або порушення безпеки. Нижчий показник MTTD вказує на підвищення ефективності виявлення, що свідчить про більш оперативну та проактивну політику безпеки. Впровадження та аналіз таких KPI, як MTTD, дозволяє організаціям постійно оцінювати та вдосконалювати свої заходи кібербезпеки, забезпечуючи надійний захист від нових загроз. Постійно відстежуючи ці показники, організації можуть швидко виявляти вразливості, оптимізувати свої стратегії безпеки та зменшувати потенційні ризики, тим самим зберігаючи цілісність і конфіденційність своїх інформаційних систем.

Середній час реагування (MTTR) є ключовим показником для оцінки ефективності реагування на інциденти в організації. Цей показник вимірює середній час, необхідний для реагування та вирішення інцидентів безпеки, і дає уявлення про ефективність та швидкість процесів реагування. Нижчий показник

MTTR означає більш досконалий механізм реагування на інциденти, що свідчить про те, що організація може швидко зменшити загрози та відновити нормальну роботу. Постійно відстежуючи і прагнучи скоротити MTTR, організації підвищують свою стійкість до кіберзагроз, забезпечуючи мінімальні перебої в роботі і зберігаючи цілісність своїх інформаційних систем. Оптимізований MTTR відображає добре скоординовану стратегію реагування на інциденти, що включає своєчасне виявлення, аналіз та вирішення інцидентів безпеки. Це не лише зменшує потенційну шкоду, але й зміцнює загальну систему кібербезпеки організації [22]. Завдяки ретельному аналізу та вдосконаленню MTTR організації можуть досягти більш надійної та оперативної системи захисту, що має вирішальне значення для захисту критично важливих активів в умовах дедалі складнішого ландшафту загроз.

Показник "Кількість успішних атак" є ключовим в оцінці надійності захисту кібербезпеки організації. Цей показник відстежує частоту порушень безпеки, які успішно обходять захисні заходи протягом певного періоду. Аналізуючи ці дані, організації можуть оцінити ефективність своїх поточних стратегій захисту. Тенденція до зменшення кількості успішних атак свідчить про покращення здатності організації захищати свої системи та дані. Постійний моніторинг цього показника має важливе значення для виявлення вразливостей і вдосконалення протоколів безпеки, що в кінцевому підсумку призводить до створення більш стійкої інфраструктури кібербезпеки. Така пильна оцінка та адаптація гарантує, що захисні заходи розвиватимуться для протидії новим загрозам, підтримуючи цілісність та безпеку активів організації [23].

Оцінка обізнаності працівників у питаннях кібербезпеки за допомогою опитувань або моніторингу рівня завершення тренінгів дає цінну інформацію про ефективність освітніх ініціатив. Цей показник має вирішальне значення для розуміння того, наскільки добре працівники розуміють і дотримуються протоколів безпеки, що є важливим для підтримки надійної системи кібербезпеки. Високий рівень обізнаності та проходження навчання свідчить про те, що працівники добре підготовлені до розпізнавання та реагування на

потенційні загрози, тим самим знижуючи ризик порушень безпеки, спричинених людськими помилками. Постійне оцінювання та вдосконалення цих освітніх програм гарантує, що працівники залишаються пильними та обізнаними щодо еволюції кіберзагроз, що сприяє загальній безпеці організації. Такий проактивний підхід до навчання працівників не лише підвищує індивідуальну відповідальність, але й посилює колективний захист від кібератак.

Впровадження надійної системи моніторингу безпеки має вирішальне значення для організацій, щоб збирати та аналізувати важливі дані, тим самим оцінюючи ефективність своїх заходів з кібербезпеки. Це передбачає безперервне спостереження за мережевим трафіком, файлами журналів, системними сповіщеннями та інцидентами безпеки. Такий комплексний моніторинг дозволяє організаціям виявляти закономірності та ідентифікувати аномалії, що має вирішальне значення для раннього виявлення загроз та проактивного реагування. Постійно аналізуючи ці показники, організації можуть виявити потенційні вразливості, посилити свої протоколи безпеки та підтримувати стійкий захист від нових кіберзагроз. Така постійна пильність є життєво важливою для забезпечення цілісності та безпеки даних і систем організації [24].

Регулярне тестування на проникнення та оцінка вразливостей необхідні для виявлення слабких місць у системах та інфраструктурі організації. Ці оцінки імітують реальні атаки, щоб оцінити ефективність існуючих засобів контролю безпеки та надати дієві рекомендації щодо їх вдосконалення. Крім того, оцінка можливостей реагування на інциденти має вирішальне значення для ефективності служб кібербезпеки. Регулярні випробування, такі як настільні навчання та імітація кібератак, допомагають виявити прогалини в процесах, комунікації та координації. Ці оцінки дають можливість посилити та вдосконалити стратегії реагування, забезпечуючи більш надійну та підготовлену організаційну систему безпеки.

Вимірювання впливу тренінгів з підвищення обізнаності про безпеку має вирішальне значення для підтримки надійної програми кібербезпеки. Організації можуть оцінити ефективність цих ініціатив, спостерігаючи за змінами в

поведінці співробітників, відстежуючи частоту повідомлень про інциденти безпеки та оцінюючи рівень успішності змодельованих фішингових кампаній. Регулярні оцінки гарантують, що навчальні заходи залишатимуться ефективними та відповідатимуть мінливому ландшафту загроз [25]. Крім того, для точної оцінки ефективності програми з кібербезпеки важливо бути в курсі галузевих стандартів і передових практик. Порівнюючи свої показники з галузевими стандартами та аналогічними організаціями, компанії можуть визначити сфери для вдосконалення та поставити реалістичні цілі.

2.3 Аналіз вразливостей та недоліків існуючих систем захисту в промислових системах.

Промислові системи управління (ПСУ) та критичні об'єкти інфраструктури все частіше піддаються кіберзагрозам, що вимагає детального розуміння їхніх вразливостей та недоліків існуючих систем безпеки. Застарілі системи, яким бракує сучасних засобів захисту через їхній вік і конструкцію, становлять значний ризик. Недоліки мережевих протоколів, специфічних для ОТ, ще більше посилюють ці вразливості, оскільки ці протоколи часто не мають надійних заходів безпеки. Інтеграція ІТ- та ОТ-систем створює додаткові складнощі та можливості для атак, а брак знань з кібербезпеки серед персоналу ОТ залишає багато прогалин у впровадженні безпеки [26]. Поширення промислового Інтернету речей (IIoT) створює нові ризики через збільшення кількості підключених пристроїв, які часто не мають належних засобів контролю безпеки. Крім того, роз'єднані практики між ІТ- та ОТ-командами створюють неузгодженість у політиках та заходах безпеки, що призводить до потенційних вразливостей. Недостатній моніторинг ускладнює ці проблеми, оскільки багато середовищ ІКС не мають необхідних інструментів для виявлення загроз і реагування на них у режимі реального часу. Усунення цих вразливостей вимагає комплексного та інтегрованого підходу для підвищення рівня безпеки промислових систем.

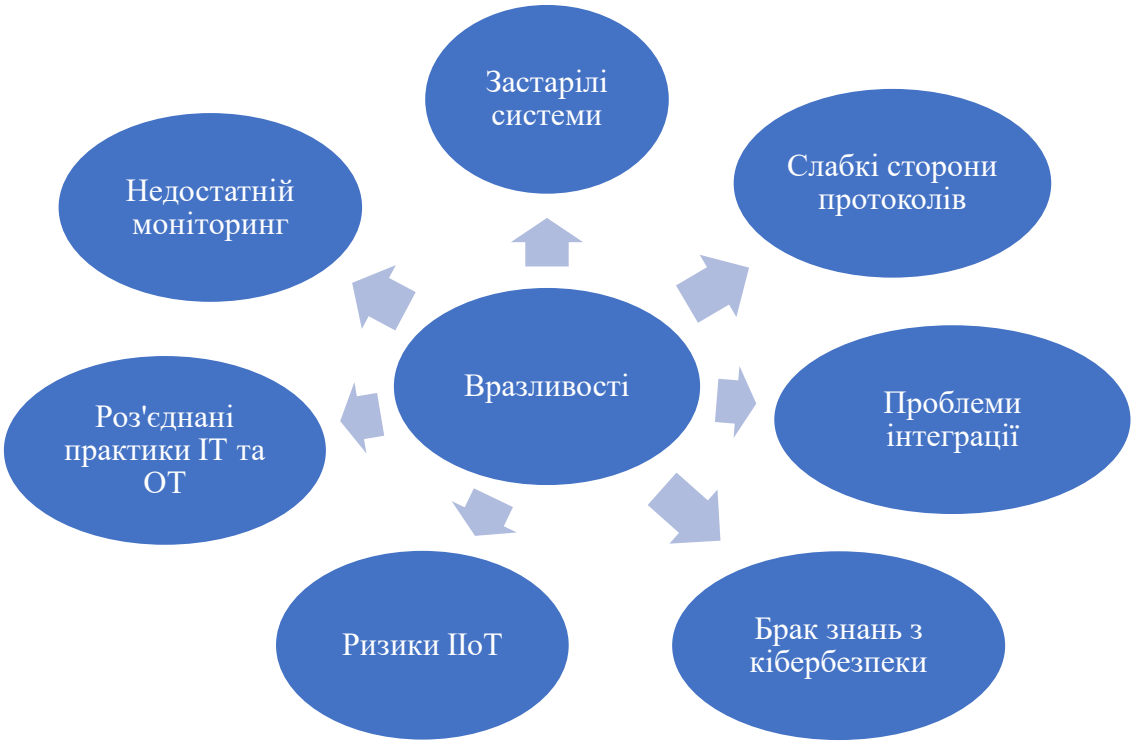

Рис. 2.2. Вразливості існуючих систем захисту в промислових системах.

Застарілі системи в промислових системах управління є особливо вразливими через їхню застарілість та відсутність сучасних засобів захисту. Ці системи були розроблені в першу чергу для надійності та довговічності, часто нехтуючи міркуваннями кібербезпеки. Отже, вони не можуть підтримувати сучасні протоколи та заходи безпеки. Інтеграція цих застарілих систем із сучасною IT-інфраструктурою створює додаткові точки входу для кібератак, посилюючи їхню вразливість. Процес модернізації таких систем є складним і дорогим, тому багато організацій продовжують використовувати застарілі та небезпечні технології. Використання застарілих систем у критичній інфраструктурі створює значні ризики для безпеки, які потребують невідкладної уваги для їх ефективного зменшення [27].

Слабкі місця протоколів у промислових системах управління - це значні вразливості, які виникають через недоліки дизайну та реалізації мережевих протоколів, специфічних для OT. Ці протоколи, часто розроблені десятиліттями тому, не мають властивих їм функцій безпеки, таких як шифрування та автентифікація. Вони були створені для ізольованих і довірених середовищ,

припускаючи, що доступ до них матимуть лише авторизовані суб'єкти. Як наслідок, ці протоколи вразливі до різних атак, включаючи підміну, атаки типу "людина посередині" та несанкціоноване виконання команд. Модернізація цих протоколів з додаванням надійних заходів безпеки є складним завданням через необхідність зворотної сумісності та критичну природу систем, які вони підтримують. Крім того, конвергенція IT- та OT-систем посилює ці недоліки, оскільки створює нові вектори для використання вразливостей цих протоколів. Усунення цих вразливостей вимагає узгоджених зусиль для редизайну протоколів, в яких безпека є основним компонентом, забезпечуючи при цьому мінімальний збій в існуючих операціях.

Проблеми інтеграції в промислових системах управління виникають внаслідок злиття операційних технологій та інформаційних технологій. Ця конвергенція, зумовлена необхідністю підвищення ефективності та зв'язності, розширює сферу атак, піддаючи АСУ ТП вразливостям, притаманним IT-системам. Системи OT, традиційно ізольовані і розроблені для забезпечення стабільності, не здатні впоратися з динамічними викликами безпеки в IT-середовищі. Процес інтеграції часто ігнорує ці відмінності, що призводить до неадекватних заходів безпеки. Це призводить до появи прогалин, якими можуть скористатися кіберзловмисники, що вимагає збалансованого підходу, який би ефективно задовольняв потреби в безпеці як IT, так і OT [28].

Брак знань з кібербезпеки в середовищі промислових систем управління є критичною вразливістю. Операційний технологічний персонал, який часто є експертами в галузі інженерії та промислових процесів, як правило, не має поглибленої підготовки з кібербезпеки. Ця прогалина в знаннях означає, що вони можуть не розпізнати або належним чином протидіяти кіберзагрозам. У міру того, як системи ІКС та IT стають все більш інтегрованими, невідповідність між знаннями персоналу, що займається експлуатацією, і складнощами кібербезпеки стає все більш помітною. Ця невідповідність може призвести до недостатнього впровадження заходів і протоколів безпеки, що збільшує ризик кібератак.

Покращення освіти та підготовки персоналу з питань кібербезпеки є важливим для подолання цього розриву та захисту ПСУ від потенційних загроз.

Промисловий Інтернет речей створює нові ризики для промислових систем управління, значно збільшуючи кількість підключених пристроїв і датчиків в операційних середовищах. Ці пристрої часто не мають надійних засобів захисту, що робить їх вразливими до кібератак. Величезна кількість пристроїв IIoT може створити численні точки входу для зловмисників, кожна з яких потенційно слугує вектором для шкідливого програмного забезпечення або інших зловмисних дій. Крім того, інтеграція IIoT з існуючою інфраструктурою ICS може призвести до проблем сумісності та ускладнити управління безпекою. Забезпечення безпеки пристроїв IIoT вимагає комплексних стратегій, які включають безпечне управління пристроями, регулярні оновлення та суворий контроль доступу. Динамічна природа IIoT також вимагає постійного моніторингу та адаптивних заходів безпеки для ефективного реагування на нові загрози [29].

Роз'єднані практики IT та OT створюють значні проблеми для безпеки промислових систем управління. Інформаційні технології та операційні технології традиційно функціонують окремо, з різними пріоритетами та досвідом. IT фокусується на цілісності даних, конфіденційності та мережевій безпеці, в той час як OT надає пріоритет доступності, надійності та безпеці системи. Такий поділ може призвести до неузгодженості в політиках і практиках безпеки, коли ці сфери зближуються. Відсутність координації та комунікації між командами IT та OT може призвести до прогалин та дублювання заходів безпеки, що робить ІКС вразливою до кіберзагроз. Ефективна інтеграція вимагає узгодження підходів до безпеки як IT, так і OT, сприяння співпраці та забезпечення всебічного навчання в обох сферах для створення цілісної стратегії безпеки, яка відповідає унікальним потребам промислового середовища.

Недостатній моніторинг в промислових системах управління (ПСУ) пов'язаний з відсутністю комплексних механізмів спостереження, необхідних для виявлення та реагування на загрози безпеці в режимі реального часу. Цей

недолік частково пов'язаний з історичною орієнтацією ПСУ на експлуатаційну надійність, а не на безпеку, що призвело до недостатнього інвестування в сучасні інструменти моніторингу. Як наслідок, багато середовищ ПСУ не мають можливості безперервного моніторингу мережевого трафіку, системної активності та потенційних аномалій, які можуть свідчити про кібервторгнення. Відсутність надійних рішень для моніторингу означає, що порушення безпеки можуть залишатися невиявленими протягом тривалого часу, що дозволяє зловмисникам використовувати вразливості без негайного виявлення [30]. Ефективний моніторинг безпеки вимагає розгортання складних інструментів, які надають інформацію в режимі реального часу, сповіщають команди безпеки про підозрілі дії та забезпечують швидке реагування. Розширення можливостей моніторингу має вирішальне значення для покращення загального стану безпеки ПСУ та захисту критичної інфраструктури від кіберзагроз.

Висновок до розділу 2

Сучасні промислові системи все частіше стають мішенню складних кіберзагроз, що може порушити роботу, скомпрометувати конфіденційні дані та завдати значних економічних збитків. Відповідно, розвиток технологій привів до розробки інноваційних методів захисту, які охоплюють сегментацію мережі, системи виявлення вторгнень, передові алгоритми аналізу загроз та машинне навчання.

Дослідження показало, що для захисту промислових систем були розроблені різні технології та рішення, такі як вдосконалені брандмауери, системи виявлення та запобігання вторгненням, системи управління інформацією та подіями безпеки (SIEM), а також спеціалізовані інструменти промислової кібербезпеки. Ці методи захисту мають важливе значення для підтримки цілісності та стійкості промислових систем перед обличчям постійно мінливого ландшафту кіберзагроз.

Аналіз показав, що кожне з розглянутих рішень, таких як TripWire, Waterfall Security, Symantec та CyberArk, має різні фокуси та особливості. TripWire акцентує увагу на безпеці ІКС з автоматизованими процесами та захистом від загроз Інтернету речей. Waterfall Security пропонує односпрямовані шлюзи безпеки, які замінюють брандмауери для запобігання зовнішнім кібератакам. Symantec забезпечує наскрізну безпеку та захист від фішингових атак, зокрема в середовищах IoT. CyberArk спеціалізується на захисті привілейованих облікових записів, моніторингу та контролі адміністративного доступу для мінімізації мережевих ризиків.

Проведений аналіз вразливостей та недоліків існуючих систем захисту в промислових системах виявив, що застарілі системи, слабкі місця протоколів, проблеми інтеграції IT- та OT-систем, брак знань з кібербезпеки серед персоналу OT, а також поширення промислового Інтернету речей (IIoT) створюють нові ризики. Недостатній моніторинг і роз'єднані практики між IT- та OT-командами також сприяють підвищенню вразливостей.

Таким чином, для забезпечення надійного захисту промислових систем необхідно впроваджувати комплексні заходи кібербезпеки, що включають сучасні технології захисту, постійний моніторинг, навчання персоналу та інтеграцію IT- та OT-систем, а також забезпечувати швидке реагування на інциденти безпеки.

Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ ЕФЕКТИВНИХ МЕТОДІВ ЗАХИСТУ ПРОМИСЛОВИХ СИСТЕМ

3.1 Розробка стратегій та методів захисту від кіберзагроз

Промислові системи управління є невід'ємною частиною управління критично важливою інфраструктурою, але стикаються з численними проблемами безпеки. Їх вирішення вимагає спеціальних стратегій, адаптованих до їх унікального середовища. Застарілі системи в ІКС часто не мають сучасних засобів захисту, що робить їх вразливими до кіберзагроз. Слабкість протоколів та складнощі інтеграції між IT- та OT-системами ще більше посилюють ці вразливості. Крім того, значні ризики створюють брак знань з кібербезпеки серед операційного персоналу та збільшення кількості атак через впровадження промислового Інтернету речей. Роз'єднані практики безпеки IT та OT і недостатні можливості моніторингу в режимі реального часу ускладнюють ці проблеми. Щоб зменшити ці вразливості, впровадження передових систем моніторингу та реагування на інциденти має вирішальне значення для виявлення загроз у режимі реального часу та швидкого реагування. Проведення регулярних оцінок та аудитів безпеки забезпечує безперервну оцінку та вдосконалення заходів безпеки. Покращення підготовки персоналу з питань кібербезпеки заповнює прогалини в знаннях, навчаючи їх ефективно протидіяти кіберзагрозам. Забезпечення надійного контролю доступу та механізмів шифрування захищає конфіденційні дані та критичні системи. Інтеграція практик безпеки IT та OT сприяє єдиному підходу до безпеки, що дозволяє знизити ризики більш комплексно. Впровадження процесів постійного вдосконалення заходів безпеки та розробка комплексних планів реагування на інциденти ще більше посилюють систему безпеки, забезпечуючи готовність та стійкість до кіберзагроз [31].

Для успішної розробки стратегій і методів захисту від кіберзагроз необхідно забезпечити надійні заходи контролю доступу, які обмежують

несанкціонований доступ до критично важливих систем і даних, впровадити сучасні інструменти моніторингу для виявлення загроз і оповіщення в режимі реального часу, використовувати механізми шифрування для захисту цілісності та конфіденційності даних, а також розробити комплексні плани реагування на інциденти з детальним описом процедур виявлення, локалізації, усунення та відновлення після порушень безпеки. Крім того, постійна оцінка та вдосконалення заходів безпеки, а також регулярні програми навчання та підвищення обізнаності персоналу мають вирішальне значення для підтримання стійкого захисту від кіберзагроз, що еволюціонують.

До стратегій пов'язаних із захистом промислових систем управління відносяться:

1. Впровадження передових систем моніторингу та реагування на інциденти.

Розгортання сучасних систем моніторингу забезпечує безперервне спостереження за мережевою діяльністю та виявлення загроз у реальному часі. Системи реагування на інциденти дозволяють швидко реагувати на порушення безпеки, мінімізуючи збитки і швидко відновлюючи нормальну роботу. Ці системи надають критично важливу інформацію та сповіщення, сприяючи проактивному управлінню безпекою та підвищуючи загальну стійкість промислових систем управління до кіберзагроз [32].

2. Проведення регулярних оцінок та аудитів безпеки.

Регулярні оцінки та аудити безпеки дозволяють виявити вразливі місця та оцінити ефективність існуючих заходів безпеки. Ці оцінки дають чітке розуміння стану безпеки та вказують на сфери, які потребують вдосконалення. Регулярні оцінки гарантують, що практики безпеки залишаються надійними та сучасними, адаптуючись до нових загроз та підтримуючи відповідність галузевим стандартам та регуляторним вимогам.

3. *Підвищення рівня підготовки персоналу з питань кібербезпеки для операторів наземних ліній електропередач.*

Спеціальні навчальні програми з кібербезпеки для операційного персоналу заповнюють прогалини в знаннях, надаючи їм навички розпізнавання та реагування на кіберзагрози. Ці програми охоплюють такі важливі теми, як ідентифікація загроз, безпечні практики та реагування на інциденти. Безперервне навчання гарантує, що операційний персонал буде в курсі останніх подій у сфері безпеки та найкращих практик, посилюючи захист організації від кібератак.

4. Забезпечення надійних механізмів контролю доступу та шифрування.

Впровадження суворих заходів контролю доступу обмежує несанкціонований доступ до критично важливих систем і даних. Шифрування захищає цілісність і конфіденційність даних шляхом перетворення інформації в захищений код, що робить її недоступною для несанкціонованих користувачів. Разом ці механізми формують критично важливу частину інфраструктури безпеки, захищаючи конфіденційну інформацію та запобігаючи несанкціонованому витоку даних.

5. Інтеграція практик безпеки IT та OT.

Створення єдиної стратегії безпеки передбачає інтеграцію практик безпеки IT та операційної безпеки, сприяючи співпраці між обома командами [33]. Така інтеграція забезпечує узгодженість політик і заходів безпеки, що стосуються як безпеки даних, так і надійності системи. Узгоджуючи свої підходи, організації можуть ефективніше зменшувати ризики та створювати цілісний захист від кіберзагроз на всіх операційних рівнях.

6. Впровадження процесів безперервного вдосконалення заходів безпеки.

Процеси безперервного вдосконалення передбачають регулярний перегляд та оновлення заходів безпеки для усунення нових вразливостей та загроз, що виникають. Цей проактивний підхід гарантує, що практики безпеки розвиваються разом з ландшафтом загроз, підтримуючи надійний захист. Безперервне вдосконалення сприяє розвитку культури пильності та адаптації, що є важливим для підтримки довгострокової ефективності безпеки.

7. Розробка комплексних планів реагування на інциденти.

Комплексні плани реагування на інциденти визначають процедури реагування на порушення безпеки, включаючи виявлення, локалізацію, ліквідацію та відновлення. Ці плани забезпечують структуроване та ефективне реагування на інциденти, мінімізуючи збої в роботі та збитки. Регулярне тестування та оновлення планів реагування підвищує їхню ефективність, готуючи організацію до швидкого та ефективного реагування на потенційні інциденти безпеки.

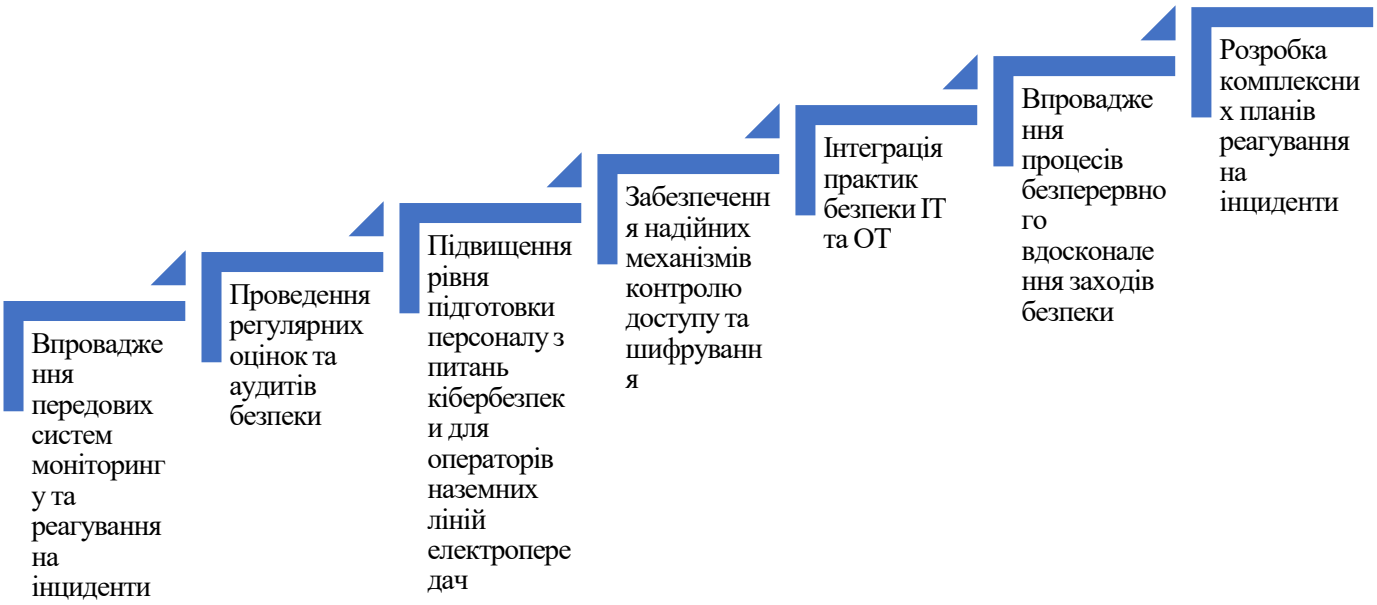

Рис. 3.1. Стратегії захисту ПСУ

Ключові компоненти контролю, необхідні для захисту промислових систем управління (ПСУ), включають надійні заходи контролю доступу, які обмежують несанкціонований доступ до критично важливих систем і даних. Удосконалені інструменти моніторингу надають інформацію в режимі реального часу та сповіщають про підозрілі дії, покращуючи можливості виявлення загроз. Механізми шифрування забезпечують цілісність і конфіденційність даних, перетворюючи інформацію в захищений код [34]. Комплексні плани реагування на інциденти детально описують процедури реагування на порушення безпеки, включаючи виявлення, локалізацію, усунення та відновлення, забезпечуючи

структуроване та ефективне реагування на інциденти. Ці компоненти разом захищають конфіденційну інформацію та запобігають несанкціонованому витоку даних, формуючи життєво важливу частину інфраструктури безпеки. Ключові компоненти промислової системи управління, включаючи контур управління, людино-машинний інтерфейс (HMI), а також утиліти для дистанційної діагностики та обслуговування, показані на рисунку 3.2.

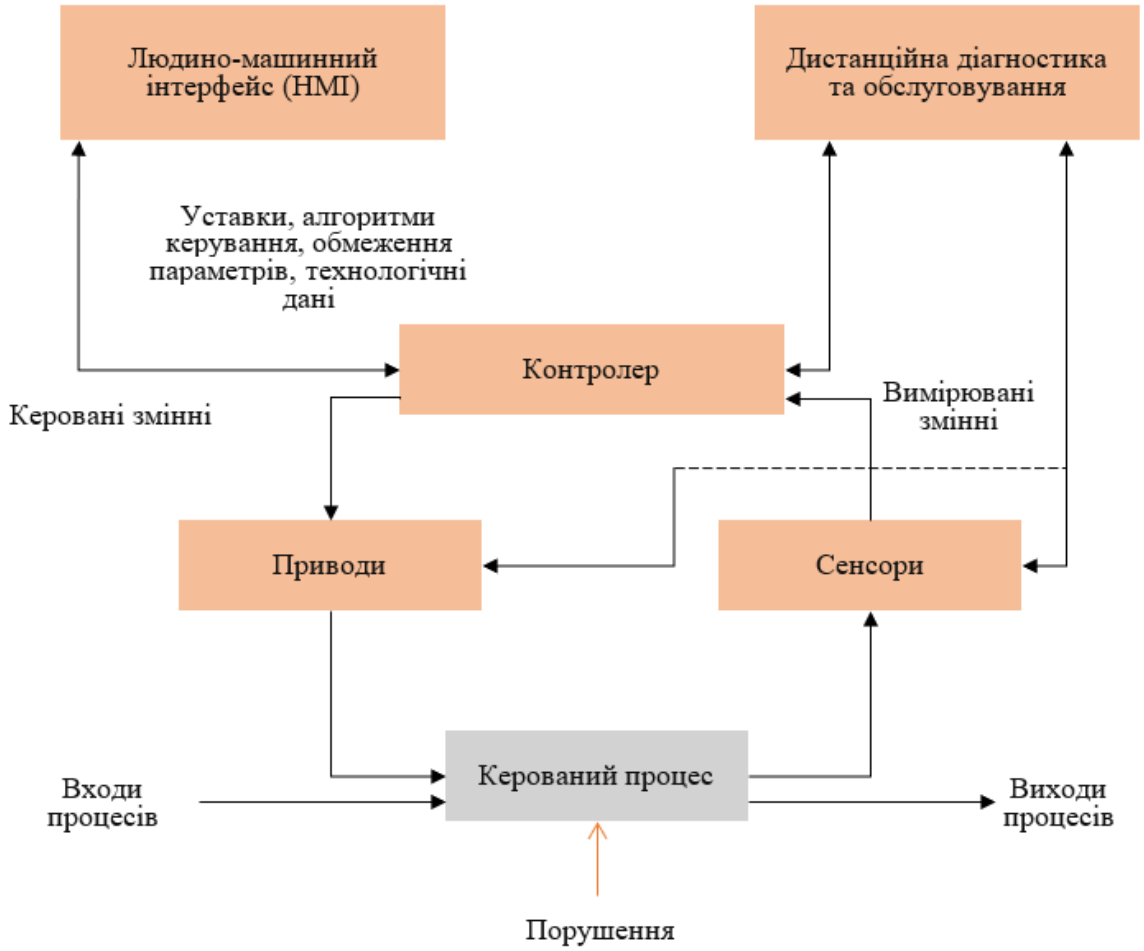

Рис. 3.2. Ключові компоненти управління [35]

Контур керування складається з датчиків для вимірювання, апаратних засобів керування, технологічних виконавчих механізмів і засобів передачі вимірювальних величин. Змінні вимірювання передаються до контролера від датчиків процесу. Контролер інтерпретує сигнали і генерує відповідні керуючі сигнали, які передаються на виконавчі механізми. Людино-машинний інтерфейс дозволяє інженеру з управління або оператору конфігурувати задані значення,

алгоритми управління і параметри в контролері, а при зміні процесу - нові сигнали датчиків, що визначають стан процесу. HMI також забезпечує відображення інформації про стан процесу, включаючи аварійні сигнали та інші засоби сповіщення оператора про несправності. Інструменти діагностики та технічного обслуговування, часто доступні через модем і інтерфейс з підтримкою Інтернету, дозволяють інженерам з управління, операторам і постачальникам контролювати і змінювати властивості контролера, виконавчих механізмів і датчиків з віддалених місць [36]. Типова промислова система містить велику кількість контурів керування, HMI та засобів дистанційної діагностики та обслуговування, побудованих на основі набору мережевих протоколів. Контури рівня керування та контури нижчих рівнів працюють безперервно протягом усього технологічного процесу з тривалістю циклу від хвилин до мілісекунд.

3.2 Впровадження новітніх технологій та інструментів для захисту промислових систем.

Стрімкий розвиток технологій у промисловості спричинив трансформаційні зміни в різних секторах, а штучний інтелект (ШІ) став ключовим фактором посилення кібербезпеки. ШІ пропонує низку можливостей, які значно покращують виявлення, запобігання та реагування на кіберзагрози, що робить його стратегічною необхідністю, оскільки кіберзагрози стають все більш витонченими. Удосконалене виявлення загроз за допомогою штучного інтелекту перевершує традиційні заходи безпеки, які часто покладаються на статичні правила. Натомість ШІ виконує швидкий аналіз великих масивів даних, виявляючи закономірності, які вказують на потенційні загрози. Машинне навчання, підмножина ШІ, ще більше підвищує операційну ефективність, аналізуючи набори даних для виявлення аномалій [37].

В основі ШІ лежить структура нейрона, яка імітує нейронну поведінку людини, що дає змогу застосовувати його в різних галузях інженерії, зокрема в

кібербезпеці. Нейронні мережі, що є частиною машинного навчання, обробляють дані на декількох рівнях, застосовуючи правила навчання до тих пір, поки вихідні дані не будуть відповідати бажаному результату. Після навчання ці мережі працюють в режимі пам'яті або виконання. Машинне навчання використовує дані та алгоритми для постійного вдосконалення моделей на основі досвіду, натхненного людським навчанням.

Одне з основних застосувань ШІ в кібербезпеці - це вдосконалене виявлення загроз. ШІ аналізує величезні масиви даних, щоб виявити закономірності, які вказують на порушення безпеки. Ця здатність дозволяє швидко виявляти загрози і реагувати на них, посилюючи заходи безпеки. Іншими важливими аспектами є предиктивний аналіз і оцінка ризиків, де ШІ використовує дані і тенденції для прогнозування потенційних майбутніх загроз, що дає змогу проактивно реагувати на вразливості. Можливості аналізу та реагування в режимі реального часу є життєво важливими, оскільки системи ШІ миттєво аналізують мережевий трафік, поведінку користувачів і системні операції. Це дозволяє миттєво виявляти та пом'якшувати наслідки інцидентів безпеки, часто без втручання людини [38].

Поведінкова аналітика в ШІ виявляє незвичайні моделі поведінки користувачів, визначаючи відхилення, які можуть свідчити про внутрішні загрози або несанкціонований доступ. Безперервне навчання на основі поведінки користувачів покращує здатність ШІ виявляти аномалії, сприяючи більш комплексному захисту. Функції автоматизованого реагування на інциденти ШІ аналізують атаки, визначають уражені системи та вживають заздалегідь визначених заходів для стримування загроз, що дозволяє командам кібербезпеки зосередитися на складних стратегічних завданнях.

Однак впровадження ШІ та МН у кібербезпеку також пов'язане з певними проблемами, зокрема, з конфіденційністю даних та необхідністю використання великих масивів даних для навчання алгоритмів. Вирішення цих проблем вимагає співпраці між командами ІТ та операційних відділів, аналітиками даних та експертами з кібербезпеки, що забезпечить надійність та стійкість систем

штучного інтелекту. Тематичні дослідження, такі як розгортання ШІ в електромережах, демонструють значне скорочення кіберінцидентів завдяки виявленню аномалій у режимі реального часу та автоматизованому реагуванню на них [39].

Нові тенденції свідчать про те, що ШІ відіграватиме дедалі більшу роль у прогнозуванні технічного обслуговування та оптимізації роботи, що сприятиме подальшій інтеграції кібербезпеки з промисловими процесами. Оскільки організації інвестують в технології штучного інтелекту, розуміння рентабельності інвестицій (ROI) має вирішальне значення. Рішення з кібербезпеки на основі ШІ можуть скоротити час простою, запобігти витоку даних і заощадити витрати, пов'язані з кіберінцидентами, що виправдовує початкові інвестиції [40].

Необхідно також враховувати етичні міркування, такі як прозорість автоматизованого прийняття рішень і захист від ворожих атак на системи ШІ. Програми безперервного навчання та підвищення обізнаності співробітників доповнюють технології ШІ, сприяючи формуванню комплексної культури безпеки в організаціях. Інтеграція ШІ та МН з існуючими системами вимагає ретельного планування, щоб звести до мінімуму збої і максимально підвищити рівень безпеки, забезпечуючи безперебійне поліпшення стану кібербезпеки. Впровадження ШІ в кібербезпеку не лише вирішує поточні проблеми, але й готує організації до майбутніх загроз, підвищуючи загальну стійкість і операційну ефективність.

3.3 Організація навчання та підготовки персоналу з питань кібербезпеки промислових систем.

Стрімкий розвиток технологій у промисловості спричинив трансформаційні зміни в різних секторах, а штучний інтелект (ШІ) став ключовим фактором посилення кібербезпеки. ШІ пропонує низку можливостей, які значно покращують виявлення, запобігання та реагування на кіберзагрози,

що робить його стратегічною необхідністю, оскільки кіберзагрози стають все більш витонченими. Удосконалене виявлення загроз за допомогою штучного інтелекту перевершує традиційні заходи безпеки, які часто покладаються на статичні правила. Натомість ШІ виконує швидкий аналіз великих масивів даних, виявляючи закономірності, які вказують на потенційні загрози. Машинне навчання, підмножина ШІ, ще більше підвищує операційну ефективність, аналізуючи набори даних для виявлення аномалій [41].

В основі ШІ лежить структура нейрона, яка імітує нейронну поведінку людини, що дає змогу застосовувати його в різних галузях інженерії, зокрема в кібербезпеці. Нейронні мережі, що є частиною машинного навчання, обробляють дані на декількох рівнях, застосовуючи правила навчання до тих пір, поки вихідні дані не будуть відповідати бажаному результату. Після навчання ці мережі працюють в режимі пам'яті або виконання. Машинне навчання використовує дані та алгоритми для постійного вдосконалення моделей на основі досвіду, натхненного людським навчанням. Одне з основних застосувань ШІ в кібербезпеці - це вдосконалене виявлення загроз. ШІ аналізує величезні масиви даних, щоб виявити закономірності, які вказують на порушення безпеки. Ця здатність дозволяє швидко виявляти загрози і реагувати на них, посилюючи заходи безпеки. Іншими важливими аспектами є предиктивний аналіз і оцінка ризиків, де ШІ використовує дані і тенденції для прогнозування потенційних майбутніх загроз, що дає змогу проактивно реагувати на вразливості. Можливості аналізу та реагування в режимі реального часу є життєво важливими, оскільки системи ШІ миттєво аналізують мережевий трафік, поведінку користувачів і системні операції. Це дозволяє миттєво виявляти та пом'якшувати наслідки інцидентів безпеки, часто без втручання людини.

Поведінкова аналітика в ШІ виявляє незвичайні моделі поведінки користувачів, визначаючи відхилення, які можуть свідчити про внутрішні загрози або несанкціонований доступ. Безперервне навчання на основі поведінки користувачів покращує здатність ШІ виявляти аномалії, сприяючи більш комплексному захисту [42]. Функції автоматизованого реагування на інциденти

ШІ аналізують атаки, визначають уражені системи та вживають заздалегідь визначених заходів для стримування загроз, що дозволяє командам кібербезпеки зосередитися на складних стратегічних завданнях. Однак впровадження ШІ та ML у кібербезпеку також пов'язане з певними проблемами, зокрема, з конфіденційністю даних та необхідністю використання великих масивів даних для навчання алгоритмів. Вирішення цих проблем вимагає співпраці між командами IT та операційних відділів, аналітиками даних та експертами з кібербезпеки, що забезпечить надійність та стійкість систем штучного інтелекту. Тематичні дослідження, такі як розгортання ШІ в електромережах, демонструють значне скорочення кіберінцидентів завдяки виявленню аномалій у режимі реального часу та автоматизованому реагуванню на них [43].

Нові тенденції свідчать про те, що ШІ відіграватиме дедалі більшу роль у прогнозуванні технічного обслуговування та оптимізації роботи, що сприятиме подальшій інтеграції кібербезпеки з промисловими процесами. Оскільки організації інвестують в технології штучного інтелекту, розуміння рентабельності інвестицій (ROI) має вирішальне значення. Рішення з кібербезпеки на основі ШІ можуть скоротити час простою, запобігти витоку даних і заощадити витрати, пов'язані з кіберінцидентами, що виправдовує початкові інвестиції. Необхідно також враховувати етичні міркування, такі як прозорість автоматизованого прийняття рішень і захист від ворожих атак на системи ШІ. Програми безперервного навчання та підвищення обізнаності співробітників доповнюють технології ШІ, сприяючи формуванню комплексної культури безпеки в організаціях. Інтеграція ШІ та ML з існуючими системами вимагає ретельного планування, щоб звести до мінімуму збої і максимально підвищити рівень безпеки, забезпечуючи безперебійне поліпшення стану кібербезпеки. Впровадження штучного інтелекту в кібербезпеку не лише вирішує поточні проблеми, а й готує організації до майбутніх загроз, підвищуючи загальну стійкість та операційну ефективність.

Висновки до розділу 3

Для захисту промислових систем управління від кіберзагроз необхідно впроваджувати спеціальні стратегії та методи, адаптовані до їх унікального середовища. Застарілі системи, слабкість протоколів, складнощі інтеграції між IT- та OT-системами, а також брак знань з кібербезпеки серед операційного персоналу створюють значні ризики для безпеки промислових систем.

Дослідження показало, що для зменшення цих вразливостей необхідно впроваджувати передові системи моніторингу та реагування на інциденти, проводити регулярні оцінки та аудити безпеки, покращувати підготовку персоналу з питань кібербезпеки, забезпечувати надійний контроль доступу та шифрування, інтегрувати практики безпеки IT та OT, впроваджувати процеси безперервного вдосконалення заходів безпеки та розробляти комплексні плани реагування на інциденти.

Аналіз показав, що штучний інтелект (ШІ) значно покращує виявлення, запобігання та реагування на кіберзагрози в промислових системах. ШІ здатний швидко аналізувати великі масиви даних, виявляючи закономірності, що вказують на потенційні загрози, а також здійснювати предиктивний аналіз і оцінку ризиків. Поведінкова аналітика в ШІ допомагає виявляти незвичайні моделі поведінки користувачів, визначаючи відхилення, які можуть свідчити про внутрішні загрози або несанкціонований доступ. Функції автоматизованого реагування на інциденти ШІ дозволяють швидко та ефективно реагувати на загрози, мінімізуючи збої в роботі та збитки.

Отже, впровадження передових технологій та інструментів, таких як ШІ, у кібербезпеку промислових систем забезпечує надійний захист від кіберзагроз, підвищує операційну ефективність та готовність до майбутніх загроз, забезпечуючи стійкість та безперебійну роботу критично важливої інфраструктури.

ВИСНОВКИ

У результаті дослідження, присвяченого аналізу кіберзагроз в промислових системах та розробленню способів захисту, було зроблено кілька важливих висновків.

У першому розділі, присвяченому теоретичним основам кіберзагроз в промислових системах, було виявлено різноманітність кіберзагроз та їх потенційний вплив на виробничі процеси та інфраструктуру. Зокрема, було підкреслено складність і масштабність проблеми кібербезпеки у промислових системах, а також необхідність постійного вдосконалення заходів з кібербезпеки. Особлива увага приділялася таким загрозам, як шкідливе програмне забезпечення, атаки на мережеві протоколи, соціальна інженерія, використання вразливостей в програмному забезпеченні та фізичні атаки.

У другому розділі, що стосується аналізу сучасних методів захисту від кіберзагроз в промислових системах, було з'ясовано, що для зменшення вразливостей необхідно впроваджувати передові системи моніторингу та реагування на інциденти, проводити регулярні оцінки та аудити безпеки, покращувати підготовку персоналу з питань кібербезпеки, забезпечувати надійний контроль доступу та шифрування, а також інтегрувати практики безпеки IT та OT.

У третьому розділі, що описує рекомендації щодо розроблення та впровадження ефективних методів захисту промислових систем, було виявлено, що впровадження передових технологій та інструментів, таких як штучний інтелект (ШІ), значно покращує виявлення, запобігання та реагування на кіберзагрози в промислових системах. Також наголошено на важливості постійного вдосконалення систем безпеки, навчання персоналу та реагування на нові загрози.

Загалом, розробка та впровадження ефективних методів захисту промислових систем є складним, але надзвичайно важливим завданням. Вона вимагає системного та комплексного підходу, що включає постійне

вдосконалення технічних, організаційних та правових засобів захисту, вдосконалення систем моніторингу та реагування, а також підвищення свідомості персоналу щодо потенційних загроз та заходів безпеки. Тільки такий підхід дозволить ефективно захищати промислові системи від сучасних кіберзагроз і забезпечити їх надійність та стійкість у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Buchwald P., Anus A. Industrial Internet of Things Systems for Tracking and Traceability of Production Business Processes. *Multidisciplinary Aspects of Production Engineering*. 2020. Vol. 3, no. 1. P. 464–476. URL: https://doi.org/10.2478/mape-2020-0039

2. Chen H. Theoretical Foundations for Cyber-Physical Systems: A Literature Review. *Journal of Industrial Integration and Management*. 2017. Vol. 02, no. 03. P. 1750013. URL: https://doi.org/10.1142/s2424862217500130

3. Classification of Cloud Systems Cyber-security Threats and Solutions Directives / H. Bennasar et al. *Application and Theory of Computer Technology*. 2017. Vol. 2, no. 3. P. 1. URL: https://doi.org/10.22496/atct20170227147

4. Countermeasures against Cyber Threats to Aviation Systems / I. K. Lim et al. *Crisis and Emergency Management: Theory and Praxis*. 2022. Vol. 18, no. 3. P. 21–31. URL: https://doi.org/10.14251/crisisonomy.2022.18.3.21

5. Dhirani L. L., Armstrong E., Newe T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*. 2021. Vol. 21, no. 11. P. 3901. URL: https://doi.org/10.3390/s21113901

6. Hammoudeh M., Epiphaniou G., Pinto P. Cyber-Physical Systems: Security Threats and Countermeasures. *Journal of Sensor and Actuator Networks*. 2023. Vol. 12, no. 1. P. 18. URL: https://doi.org/10.3390/jsan12010018

7. Internet of Things-based Decision Support Systems, Industrial Big Data Analytics, and Autonomous Production Processes in Sustainable Smart Manufacturing. *Journal of Self-Governance and Management Economics*. 2021. Vol. 9, no. 4. P. 21. URL: https://doi.org/10.22381/jsme9420212

8. Kazarin O. V., Sharyapov R. A., Yashchenko V. V. MULTIFACTORIAL CLASSIFICATION OF THREATS TO INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS. *RSUH/RGGU Bulletin. Series Information Science. Information Security. Mathematics*. 2018. No. 1. P. 39–55. URL: https://doi.org/10.28995/2686-679x-2018-1-39-55

9. Kuznetsov D. I., Riabchyna L. S. Internet of things systems information security. *Jornal of Kryvyi Rih National University*. 2019. No. 49. P. 80–84. URL: https://doi.org/10.31721/2306-5451-2019-1-49-80-84

10. Mitigating Cyber Security Threats of Industrial Control Systems (Scada & Dcs) / A. Lamba et al. *SSRN Electronic Journal*. 2017. URL: https://doi.org/10.2139/ssrn.3492685

11. Nankya M., Chataut R., Akl R. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. *Sensors*. 2023. Vol. 23, no. 21. P. 8840. URL: https://doi.org/10.3390/s23218840

12. Salun M., Palyanychka Y. Features and principles of monitoring of industrial enterprise competitiveness. *Economics of Development*. 2018. Vol. 17, no. 3. P. 74–82. URL: https://doi.org/10.21511/ed.17(3).2018.07

13. Schoepf M., Weibelzahl M., Nowka L. The Impact of Substituting Production Technologies on the Economic Demand Response Potential in Industrial Processes. *Energies*. 2018. Vol. 11, no. 9. P. 2217. URL: https://doi.org/10.3390/en11092217

14. Shirinkina E. V. Features of functioning of industrial enterprises in the digital economy. *Economy in the industry*. 2018. Vol. 11, no. 2. P. 143–150. URL: https://doi.org/10.17073/2072-1633-2018-2-143-150

15. Tleuberdin S. T., Seitkulov Y. N. Classification of cyber threats for internet of things. *Bulletin of the National Engineering Academy of the Republic of Kazakhstan*. 2023. Vol. 90, no. 4. P. 115–125. URL: https://doi.org/10.47533/2023.1606-146x.40

16. Zhang C., Xu X., Chen H. Theoretical foundations and applications of cyber-physical systems: a literature review. *Library Hi Tech*. 2019. Vol. 38, no. 1. P. 95–104. URL: https://doi.org/10.1108/lht-11-2017-0230

17. Open Source Tripwire. *Sourceforge*. URL: https://sourceforge.net/projects/tripwire/

18. Waterfall. *Waterfall-security*. URL: https://waterfall-security.com

19. Symantec. *Broadcom*. URL: https://www.broadcom.com/products/cybersecurity/endpoint

20. Cyberark. *Cyberark*. URL: https://www.cyberark.com

21. A logic-based framework for the security analysis of Industrial Control Systems / L. Lemaire et al. *Automatic Control and Computer Sciences*. 2017. Vol. 51, no. 2. P. 114–123. URL: https://doi.org/10.3103/s0146411617020055

22. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis / H. Abdo et al. *Computers & Security*. 2018. Vol. 72. P. 175–195. URL: https://doi.org/10.1016/j.cose.2017.09.004

23. A survey of static analysis methods for identifying security vulnerabilities in software systems / M. Pistoia et al. *IBM Systems Journal*. 2007. Vol. 46, no. 2. P. 265–288. URL: https://doi.org/10.1147/sj.462.0265

24. Bansal A., Khosla T., Saini V. K. Security Challenges and various methods for Increasing Security in E-Commerce Applications. *International Journal for Research in Applied Science and Engineering Technology*. 2023. Vol. 11, no. 1. P. 311–316. URL: https://doi.org/10.22214/ijraset.2023.48475

25. Bansal A., Khosla T., Saini V. K. Security Challenges and various methods for Increasing Security in E-Commerce Applications. *International Journal for Research in Applied Science and Engineering Technology*. 2023. Vol. 11, no. 1. P. 311–316. URL: https://doi.org/10.22214/ijraset.2023.48475

26. BATUR DİNLER Ö. Deceptive Patch Solutions for Protecting Industrial Control Systems Based on Discovered Vulnerabilities. *Türk Doğa ve Fen Dergisi*. 2024. URL: https://doi.org/10.46810/tdfd.1273507

27. Baumung W., Fomin V. V. Optimization Model to Extend Existing Production Planning and Control Systems for the Use of Additive Manufacturing Technologies in the Industrial Production. *Procedia Manufacturing*. 2018. Vol. 24. P. 222–228. URL: https://doi.org/10.1016/j.promfg.2018.06.035

28. Erbel M., Kopniak P. Assessment of the web application security effectiveness against various methods of network attacks. *Journal of Computer Sciences Institute*. 2018. Vol. 9. P. 340–344. URL: https://doi.org/10.35784/jcsi.707

29. Evaluation of filtration effectiveness of various types of facemasks following with different sterilization methods / A. Kumar et al. *Journal of Industrial Textiles*. 2021. P. 152808372110287. URL: https://doi.org/10.1177/15280837211028794

30. Martyshkin A. I., Kuzina V. V. Overview of existing solutions for the organization of reconfigurable computing systems. *Contemporary information technologies*. 2021. No. 34. URL: https://doi.org/10.46548/cit-2021-0034-0001

31. Military and offshore technologies provide slip ring solutions for industrial vision systems. *Sensor Review*. 2002. Vol. 22, no. 4. URL: https://doi.org/10.1108/sr.2002.08722daf.003

32. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game / X. Liu et al. *Computers & Security*. 2021. Vol. 102. P. 102138. URL: https://doi.org/10.1016/j.cose.2020.102138

33. Rohith Vallabhaneni, Abhilash Maroju, Sravanthi Dontu S. A. V. Analysis on Security Vulnerabilities of the Modern Internet of Things (IOT) Systems. *International Journal on Recent and Innovation Trends in Computing and Communication*. 2023. Vol. 11, no. 9s. P. 801–808. URL: https://doi.org/10.17762/ijritcc.v11i9s.9487

34. Ruiz-Puente C. Proposal of a Conceptual Model to Represent Urban-Industrial Systems from the Analysis of Existing Worldwide Experiences. *Sustainability*. 2021. Vol. 13, no. 16. P. 9292. URL: https://doi.org/10.3390/su13169292

35. Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective / M. M. Aslam et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3394848

36. Swindle S., Baker S. S., Auld G. W. Operation Frontline: Assessment of Longer-term Curriculum Effectiveness, Evaluation Strategies, and Follow-up Methods. *Journal of Nutrition Education and Behavior*. 2007. Vol. 39, no. 4. P. 205–213. URL: https://doi.org/10.1016/j.jneb.2007.03.003

37. raceability in Systems Engineering – Review of industrial practices, state-of-the-art technologies and new research solutions / S. F. Königs et al. *Advanced Engineering Informatics*. 2012. Vol. 26, no. 4. P. 924–940. URL: https://doi.org/10.1016/j.aei.2012.08.002

38. Abzaldinova E. V., Sungatullin R. G., Baturin V. A. INNOVATIVE METHODS OF PROTECTION AGAINST CYBER THREATS: REVIEW OF MODERN APPROACHES. *EKONOMIKA I UPRAVLENIE: PROBLEMY, RESHENIYA*. 2024. Vol. 3/8, no. 144. P. 45–49. URL: https://doi.org/10.36871/ek.up.p.r.2024.03.08.007

39. Artificial Intelligence-based Internet of Manufacturing Things Systems, Digital Twin Data Modeling and Visualization Tools, and Multi-Sensory Extended Reality and Geospatial Mapping Technologies in the Immersive Industrial Metaverse. *Economics, Management, and Financial Markets*. 2023. Vol. 18, no. 1. P. 41. URL: https://doi.org/10.22381/emfm18120233

40. Baric R. Developing broadly protective strategies to protect against future pandemic threats. *Vaccine Insights*. 2022. Vol. 1, no. 1. P. 59–65. URL: https://doi.org/10.18609/vac.2022.010

41. Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks / T. Sendjaja et al. *International Journal of Science and Society*. 2024. Vol. 6, no. 1. P. 1008–1019. URL: https://doi.org/10.54783/ijsoc.v6i1.1098

42. Kopytkov V. V., Dorzhsuren C., Tairbergenov Y. A. Research and implementation of innovative technologies for the use of composite polymer materials to protect the root systems of seedlings from desiccation and increase their establishment. *BIO Web of Conferences*. 2021. Vol. 36. P. 04006. URL: https://doi.org/10.1051/bioconf/20213604006

43. Yeboah-Ofori A. Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*. 2018. Vol. 7, no. 1. P. 87–98. URL: https://doi.org/10.17781/p002378